

Ваш цифровий слід



Коли ви підключаєтеся до Інтернету,
зробіть паузу й поставтеся до цього
відповідально

Освітній проєкт із цифрового
громадянства та запобігання
кіберзлочинності

Профілактика кіберзлочинності:

посібник для
вчителів та
батьків



United Nations
Office on Drugs and Crime



GLOBAL PROGRAMME ON
CYBERCRIME

Canada 



Pantallas Amigas



United Nations
Office on Drugs and Crime

Подяки

Ця публікація була розроблена Управлінням Організації Об'єднаних Націй з наркотиків і злочинності (UNODC) в рамках Глобальної програми з кіберзлочинності за щедрої підтримки уряду Канади.

Публікація була підготовлена Хорхе Флоресом Фернандесом за суттєвої підтримки таких співробітників UNODC: Берти Наеллі Лоя Марін, Жорді Мартіна Домінго та Ренати Дельгадо-Шенк.

UNODC також висловлює вдячність численним експертам, які надали підтримку у розробці цього посібника.



Глобальна програма протидії кіберзлочинності

Місія глобальних заходів з протидії та запобігання кіберзлочинам (як залежним від кіберпростору, так і здійсненим за допомогою кіберпростору) за допомогою інноваційних, інтегрованих та індивідуалізованих рішень. Глобальна програма діє на глобальному рівні з використанням місцевих та регіональних підходів. Наразі вона має консультативні групи, що працюють у трьох регіонах: Центральній та Південній Америці, Західній та Центральній Африці, а також Південно-Східній Азії та Тихоокеанському регіоні. Глобальна програма має три напрямки діяльності: розбудова потенціалу, нормативна допомога та співпраця як на міжвідомчому, так і на міжнародному рівнях.

Глобальна програма протидії кіберзлочинності сприяє довгостроковим, стійким заходам з нарощування потенціалу для запобігання та протидії кіберзлочинності шляхом підтримки національних структур з виявлення, повідомлення, розслідування, судового переслідування та винесення вироків або покарань за кіберзлочини. Крім того, UNODC використовує свою спеціалізовану експертизу щодо реагування систем кримінального правосуддя для надання технічної допомоги в таких сферах: (i) нарощування потенціалу, (ii) нормативна допомога, (iii) запобігання та підвищення обізнаності, (iv) співпраця та (v) дослідження та аналіз явища кіберзлочинності та її тенденцій.



UNODC вжило розумних запобіжних заходів для перевірки інформації, що міститься в цій публікації. Читачі несуть відповідальність за тлумачення та використання цього матеріалу.

Цей посібник підготовлено з урахуванням принципів використання інклюзивної мови відповідно до Гендерної стратегії UNODC із забезпечення гендерної рівності та розширення прав і можливостей жінок (2022–2026).

Повне або часткове відтворення цього матеріалу дозволяється за умови посилання на UNODC як джерело та за умови, що це не пов'язано з будь-яким комерційним використанням. Будь-які зміни змісту цього посібника заборонені.

ISBN: 978-84-17774-81-3

Автор: Хорхе Флорес Фернандес (PantallasAmigas)

© Управління Організації Об'єднаних Націй з наркотиків і злочинності, листопад 2022 року. Всі права захищені.



Передмова

Управління Організації Об'єднаних Націй з наркотиків і злочинності (UNODC) є провідною агенцією ООН, яка надає технічну підтримку державам-членам у запобіганні та боротьбі зі злочинністю, незаконним обігом наркотиків, організованою злочинністю, корупцією та тероризмом, а також надає технічні консультації та проводить навчання для подолання викликів, пов'язаних із цими явищами. У цьому контексті Глобальна програма з кіберзлочинності спеціалізується на задоволенні потреб держав-членів у сфері запобігання та боротьби з кіберзлочинністю, як у відношенні до злочинності, що здійснюється за допомогою кібертехнологій, так і до злочинності, що залежить від кібертехнологій.

У глобалізованому контексті, де злочинність діє в безмежному середовищі кіберпростору, запобігання кіберзлочинності є необхідним доповненням до будь-яких заходів та відповідних дій, спрямованих на ефективну боротьбу з цим видом злочинності.

При цьому UNODC через свою Глобальну програму з боротьби з кіберзлочинністю тісно співпрацює з системами кримінального правосуддя по всьому світу, включаючи правоохоронців, прокурорів, суддів, судових експертів, рятувальників, вчителів, освітян та урядовців (зокрема, у сферах освіти, безпеки та правосуддя), а також громадянським суспільством та приватним сектором з метою посилення стратегій, політик та загальних заходів, спрямованих на зменшення та управління ризиками, що виникають внаслідок зловживання інформаційно-комунікаційними технологіями.

Цей посібник розроблено як допоміжний матеріал для педагогічних заходів, що проводяться вчителями, репетиторами, матерями, батьками, опікунами та законними представниками, зацікавленими у поглибленні знань дітей та молоді та наданні їм рекомендацій щодо безпечного користування Інтернетом.

UNODC висловлює вдячність уряду Канади за щедрий внесок у розробку цього посібника, який було використано для інформування понад мільйона людей.

14

Кібербезпека



Вступ

Чому безпека в Інтернеті є важливою?

Які небезпеки існують?

Пам'ятайте

Шкідливе програмне забезпечення

Визначення

Загальні особливості

Типи шкідливих програм

Загальні рекомендації щодо запобігання

Виявлення та дії

Незахищені з'єднання

Фальшиві посилання

Як вони працюють?

Профілактичні заходи

Несанкціонований доступ до пристроїв

Безпечні паролі

Безпечний пароль у восьми кроках

Рекомендації щодо захисту від загроз вашій кібербезпеці

23

Приватність



Вступ

Чому приватність є важливою?

Які можливі негативні наслідки?

Пам'ятайте

Приватність як право та фактор захисту

Приватність як право

Приватність як фактор захисту

Виховання культури конфіденційності

Приватність під загрозою зникнення

Традиційна освіта з питань конфіденційності в Інтернеті

Спільна приватність

Кібербезпека та приватність

Ідентичність і цифровий слід

Соціальні мережі, тегування та геолокація

Управління приватністю в соціальних мережах

Теги фотографій

Геолокалізація

Захист вашої конфіденційності на смартфоні

Десять правил захисту приватності вашого мобільного телефону

Ключі до збереження вашого приватного життя та даних



31

Кібербулінг



Вступ

Пам'ятайте

Визначення та опис кібербулінгу

Які ознаки цього?

Відмінності між булінгом та кібербулінгом

Фактори, що сприяють кібербулінгу серед однолітків

Актуальність життєвих навичок

Деякі ключові навички для кіберспівіснування

Кіберспівіснування як свідомий, постійний і колективний виклик

Десять правил для позитивного цифрового співіснування

Профілактична робота

Заохочення до захисту приватності та кібербезпеки

Розповсюдження інформації про правові межі та відповідальність

Просування концепції цифрового громадянства та мережевої етики

Заклик до дії для різних типів аудиторій

Додаткова цінність до гарної атмосфери в просторах для цифрових відносин

Втручання. Що робити у випадку кібербулінгу?

Десять правил для жертв кібербулінгу

40

Грумінг



Вступ

Пам'ятайте

Інтернет-грумінг: що це таке і як це відбувається?

Хто є жертвами грумінгу?

Умови, необхідні для грумінгу

Фактори ризику, яких слід уникати

Як поводитися у випадку грумінгу?

Десять порад щодо боротьби з грумінгом

44

Секстинг



Вступ

Що таке секстинг?

Які можливі ризики для тих, хто займається секстингом?

Пам'ятайте

Запобігання необдуманому, неусвідомленому або здійсненому під тиском секстингу

Подумайте перед тим як зробити секстинг. 10 причин не робити секстинг. Ви вирішите!

Десять правил захисту приватного життя

Що робити у разі виникнення проблеми?

48

Сексторція



Вступ

Що таке сексторція?
Які наслідки?

Пам'ятайте

Як запобігти сексторції

Як запобігти тому, що зображення потрапило в
«неправильні» руки
Розуміння мотивів сексторції
Особиста та соціальна профілактика

Десять правил для жертв сексторції



53



Сексуальність та споживання порнографії в Інтернеті

Вступ

Пам'ятайте

Визначення та особливості

Джерела, доступ та споживання порнографічного контенту
Вигадка з реалістичним виглядом та реальними наслідками
Насильство щодо жінок
Відносини домінування-підкорення та об'єктивізація жінок
Негативні психологічні та соціальні наслідки
Секс без кохання
Ризиковані практики
Проблемне використання

Стратегії профілактики споживання порнографічного контенту

Підвищення інформованості громадськості
Афективно-сексуальна освіта, адаптована до нових реальностей
Обмеження доступу
Просування критичного соціального позиціонування

Десять рекомендацій щодо безпечного усвідомленого ставлення до онлайн-контенту

60



Дезінформація та місінформація в Інтернеті

Вступ

Пам'ятайте

Визначення, поняття та особливості

Дезінформація і місінформація
Медіа- та інформаційна грамотність
Критичне мислення, навички та ставлення
Цифрове життя дітей і критичне мислення
Упередження, емоції та їхнє значення в дезінформації
Фільтр-бульбашка та ехо-камери

Що можна зробити для запобігання та боротьби з дезінформацією?

Зупинитися, щоб подумати, і розглянути варіант не ділитися
Усвідомлення наслідків та власної відповідальності
Стимулювання критичного мислення в широкому сенсі
Знання, щоб уникнути впливу упереджень та емоцій
Знання своїх стратегій: яка мета, і як працює дезінформація
Знання та використання інструментів для перевірки інформації

Десять правил боротьби з дезінформацією

Джерело
Зміст
Намірність



69

Кібернасильство проти жінок та дівчат

Вступ

Ключові моменти, про які слід пам'ятати

Визначення та особливості

Грумінг
Кіберхарасмент та кіберсталкінг щодо феміністичних активісток
Сексистський або ґендерно-зумовлений кібербулінг
Сексуальний кібербулінг
Контролююче кібернасильство
Сексуальне кібернасильство

Що можна зробити для запобігання та боротьби з цим?

Освіта в галузі рівності
Формування емпатії та видимості насильства
Розповсюдження інформації про правові наслідки
Просування кібербезпеки та приватності
Колективна участь
Кіберактивізм

Визначення десяти форм контролюючого кібернасильства

Десять ознак контролюючого кібернасильства

75



Цифровий слід, репутація та цифрова ідентичність

Вступ

Пам'ятайте

Визначення та особливості

Цифровий слід

Цифрова ідентичність

Елементи, що складають цифрову ідентичність

Особливості цифрової ідентичності

Цифрова репутація

Що можна зробити, щоб запобігти цьому та вжити відповідних заходів?

Усвідомлення елементів, що входять у це, та їхніх
взаємовідносин

Які проблеми можуть бути пов'язані з цифровим
слідом?

Як зменшити цифровий слід

Які проблеми можуть бути пов'язані з негативною
репутацією та цифровим слідом?

Як створити гарну цифрову ідентичність та
репутацію

Десять рекомендацій для позитивної цифрової репутації або ідентичності



81

Як ідентифікувати жертву

Вступ

Розширення Інтернету та комунікаційних технологій, а разом із цим зростання рівня підключення та кількості користувачів, попри численні переваги, також призвели до глобального зростання рівня кіберзлочинності. Сьогодні існує більше як жертв кіберзлочинів, так і осіб, які їх вчиняють. Цю ситуацію ще більше загострила пандемія COVID-19.

У 2021 році держави-члени на Кіотському конгресі з питань злочинності висловили глибоку стурбованість зростаючою тенденцією до використання Інтернету злочинцями та організованою злочинністю в незаконних цілях, що створює безпрецедентні виклики у сфері запобігання та боротьби з існуючими злочинами, а також призводить до появи нових форм злочинності, включаючи як кіберзалежні, так і кіберпідтримувані злочини. Неконтрольовані ризики та вразливість у сфері кіберзлочинності є каталізатором транснаціональної організованої злочинності та прямою загрозою соціально-економічному розвитку, а також національній і міжнародній безпеці.

Тому запобігання кіберзлочинності є надзвичайно важливим для боротьби із зловживанням інформаційно-комунікаційними технологіями в злочинних цілях, особливо стосовно дівчат, хлопців, молодих жінок і чоловіків, які щодня наражаються на ризики кіберзлочинності, особливо в контексті зростання рівня підключення до Інтернету та переходу до цифровізації в суспільстві та освіті.

У цій ситуації як державний, так і приватний сектори несуть відповідальність і зобов'язання розробляти та впроваджувати ефективні заходи для зменшення та управління поточними та зростаючими ризиками.

У контексті Порядку денного ООН у сфері сталого розвитку до 2030 року (Цілі № 4, 5, 7, 16 та 17) та Стратегії UNODC на 2021–2025 роки Управління ООН з наркотиків і злочинності (UNODC) взяло на себе зобов'язання очолювати та підтримувати держави-члени, громадянське суспільство й приватний сектор у розробленні заходів із запобігання кіберзлочинності з метою посилення захисту всіх осіб, а особливо тих, хто є більш вразливими до неї.

Посібник містить базовий матеріал для отримання знань про кіберзлочинність у закладах освіти та/або вдома. Він складається з десяти тематичних розділів, в яких взаємопов'язані кіберзлочинність, кібербезпека та права людини. Всі три теми базуються на основних принципах прав дитини: (i) право на життя та недискримінацію дітей; (ii) право на розвиток своїх здібностей до максимального

потенціалу; (iii) право висловлювати свою думку та бути почутими; та (iv) врахування найкращих інтересів дитини в усіх заходах, що безпосередньо або опосередковано впливають на неї. Слід нагадати, що як хлопчики, так і дівчатка є повноцінними особистостями, які здатні робити вибір і сприяти зменшенню ризиків кіберзлочинності, що впливають на них. У цьому сенсі їх не тільки слід захищати від кіберзлочинності, але й надавати їм можливість брати участь у пошуку рішень для запобігання їхній вктимізації.

Водночас не можна заперечувати, що діти можуть бути як жертвами, так і агресорами певних форм кіберзлочинності. У зв'язку з цим частина матеріалів з профілактики також спрямована на те, щоб усі (дорослі та діти) усвідомлювали, що є злочином, а що ні, як запобігати йому та що робити у випадках, коли ми підозрюємо, що хтось став жертвою кіберзлочинності. У цьому посібнику читачі знайдуть не тільки базові знання з кожної теми, але й цільові поради щодо того, як управляти цими складними ситуаціями в освітньому середовищі.

Розвиток інформаційно-комунікаційних технологій (ІКТ) є нестримним. Завдяки ІКТ наше життя стало простішим і швидшим, і ми маємо багато позитивних можливостей, що сприяють нашій соціалізації та обміну знаннями. Водночас це середовище створило багато ризиків, якими необхідно управляти.

Цей посібник розроблено як допоміжний матеріал для розробки педагогічних заходів вчителями, вихователями, батьками, опікунами, доглядачами, членами сім'ї, організаціями громадянського суспільства та іншими особами, які бажають підтримувати та направляти дітей і молодих жінок та чоловіків у запобіганні кіберзлочинам та безпечному використанні Інтернету та цифрових технологій. У контексті зростання рівня підключення до Інтернету та переходу до віртуальних освітніх інструментів це завдання зараз є важливішим ніж будь-коли.

Майбутнє нашого суспільства залежить від сьогоднішніх дітей. Наша спільна відповідальність - надати їм інструменти та знання, необхідні для прийняття відповідальних і правильних рішень, які дозволять їм безпечно пересуватися як в офлайн, так і в онлайн-просторі. Якщо ми навчаємо дітей, як безпечно пересуватися у фізичному світі, чи не повинні ми робити те саме щодо їхніх дій і досвіду в кіберпросторі?



Кібербезпека

Вступ

У цьому розділі розглядаються деякі загрози безпеці в Інтернеті, пов'язані з певними пристроями та процесами. Тема кібербезпеки є настільки широкою та динамічною, що її важко висвітлити в посібнику такого характеру, крім основних аспектів. Водночас в Інтернеті можна знайти вичерпну та детальну інформацію про більш технічні аспекти, яку можна вивчати разом із учнями. Кіберзлочинність є дуже прибутковим бізнесом, який набирає обертів і постійно розвивається. Тому надзвичайно важливо мати детальну інформацію та розвивати необхідні профілактичні навички з раннього віку. Ми повинні пам'ятати, що наша особиста безпека залежить від безпеки наших пристроїв.

ЧОМУ БЕЗПЕКА В ІНТЕРНЕТІ Є ВАЖЛИВОЮ?

У світі, де все пов'язано між собою, ми знаходимося в зоні досяжності кіберзлочинців та інших осіб, які прагнуть скористатися нашими помилками або неправильними діями.

Шкідливе програмне забезпечення є повсюди в Інтернеті і може спричинити як незначні незручності, так і серйозні особисті проблеми. Воно може проникнути в наші підключені пристрої в разі атак, або ми можемо ненавмисно занести його самі. Кіберзлочинність також використовує обман і намагається скористатися нашими помилками, коли ми надаємо конфіденційну інформацію в неправильному місці або вважаємо неправдиву інформацію справжньою. Інколи, наприклад, використання слабкого пароля полегшує його викрадення, і тому інші можуть отримати контроль над нашими пристроями та додатками, а отже, і над нашим цифровим життям та інформацією.

Пам'ятайте

- Мобільні телефони, планшети та комп'ютери - це пристрої, які при підключенні до Інтернету стають вразливими цілями.
- Існує багато типів комп'ютерних загроз (шкідливого програмного забезпечення), які можуть дістатися до нас через різні канали в Інтернеті і мати різні негативні наслідки.
- Коли ваші пристрої заражені або атаковані, навіть якщо ви про це не знаєте, саме ви можете зазнати серйозних особистих наслідків.
- Захист власної кібербезпеки - це щоденне особисте завдання, яке потрібно адаптувати до нових обставин і додатків.
- Також дуже важливо звертати увагу на інших людей і підтримувати їх. Якщо вони захищені, ви будете в більшій безпеці, адже ми всі взаємопов'язані.
- Для забезпечення безпеки необхідно мати програму безпеки або антивірус на всіх ваших пристроях (мобільних телефонах, планшетах або комп'ютерах) та безпечні паролі для доступу до ваших послуг, профілів та додатків в Інтернеті.

ЯКІ НЕБЕЗПЕКИ ІСНУЮТЬ?

Коли існують вразливі місця в системі безпеки або ми стаємо об'єктом атаки, це може мати кілька наслідків:

- Використання обладнання в інших цілях. Пристрій жертви використовується анонімно для таких дій, як збір даних про перегляди, відображення реклами або додавання його до ботнету (мережі ботів або «зомбі»), що використовується для вчинення інших кіберзлочинів. Інфекція прагне залишитися непоміченою, і часто жертва про неї не знає.
- Викрадення пристрою за допомогою програм-вимагачів. Вони блокують доступ до частини пристрою і вимагають виконання умови, зазвичай оплати, для його звільнення.
- Доступ до конфіденційних даних або особистої інформації. Крадіжка особистої інформації (паролів, фотографій, банківських реквізитів, документів, що посвідчують особу, тощо) може мати різні цілі і, як правило, вимагає подальшого втручання зловмисника. Деякі з найбільш шкідливих наслідків варіюються від сексуального шантажу або крадіжки особистих даних до кібербулінгу або шпигунства шляхом активації камери або мікрофона.
- Обман і шахрайство. Після обману жертва піддається ризику крадіжки грошей або іншого цифрового майна і може навіть стати учасником кіберзлочину.



Шкідливе програмне забезпечення

ВИЗНАЧЕННЯ

Загальне визначення шкідливого програмного забезпечення - це комп'ютерний код або програмне забезпечення, яке впроваджується в комп'ютери та комп'ютерні системи різними способами і може мати незручні, шкідливі або навіть руйнівні чи непоправні наслідки.

Хоча спочатку це шкідливе програмне забезпечення мало чітку мету - заподіяти різного ступеня шкоди пристрою (видалення інформації, відображення дратівливого вікна, показ або пошук помилок у програмуванні тощо), сьогодні його присутність є навмисно прихованою і, дуже часто, пов'язаною з кримінальною діяльністю з метою отримання прибутку. Воно може співіснувати з інфікованими користувачами та їхніми пристроями в повній, непомітній і зовні видимій гармонії.

ЗАГАЛЬНІ ОСОБЛИВОСТІ

В основному, і саме звідси походить його оригінальна загальна назва, комп'ютерний «вірус» можна порівняти з його аналогом у галузі біології: він заражає інші організми, поширюється різними способами, має різний склад і зовнішній вигляд, виявляє різні симптоми, і не всі з них викликають захворювання.

Шкідливе програмне забезпечення може потрапити на наш пристрій різними способами. Деякі з них вимагають втручання або певних дій з боку користувача, таких як натискання на «підроблене» посилання, завантаження, відкриття або встановлення файлу чи програми, в які вбудовано шкідливий код, тощо. Інші типи шкідливого програмного забезпечення «впроваджуються» іншими особами внаслідок бездіяльності, необережності або дезінформації користувача. Вони використовують, наприклад, незміну попередньо встановлених паролів на пристроях, щоб проникнути всередину, використовуючи пароль, який легко зламати, тощо.

Операційні системи та програмне забезпечення, які ми встановлюємо на наших пристроях, оскільки вони є комп'ютерним кодом, можуть містити програмні помилки, а також залишати відкритими двері для проникнення інших осіб.

Методи поширення є різноманітними і включають, серед іншого, USB-накопичувачі, електронну пошту з вкладеннями, завантаження з Інтернету, передавання файлів через FTP (протокол передавання файлів), мережі P2P (обмін файлами між рівноправними користувачами) тощо.

Оскільки шкідливе програмне забезпечення також є програмним кодом, воно може впливати на всі типи пристроїв, на яких воно запускається (настільні комп'ютери, ноутбуки, планшети, смартфони, маршрутизатори тощо), тому при впровадженні заходів безпеки бажано враховувати всі ці пристрої.

Не слід забувати, що за створенням і поширенням цього шкідливого коду стоять люди, і тому важко визначити їхні цілі. Деякі шкідливі програми, наприклад трояни, могли бути запрограмовані групою студентів як жарт або експеримент без наміру заподіяти серйозної шкоди або як спосіб довести вразливість програмного забезпечення або пристроїв легально створених компаній. Однак немає сумнівів, що на сьогоднішній день на цьому побудовано великий бізнес, і є люди, які самостійно або в складі команд, з метою отримання фінансової вигоди, не вагаються вчиняти злочини.

Наші дані, дані інших людей, а також дані установ, у яких ми навчаємося або працюємо, які ми використовуємо та зберігаємо в повсякденному житті, можуть містити цінну інформацію. У разі потрапляння до чужих рук така інформація може бути використана проти нас (крадіжка, викрадення особистих даних, продаж конфіденційної інформації третім сторонам тощо) або, якщо її буде знищено чи зроблено непридатною для використання, може завдати нам серйозної шкоди (наприклад, шифрування даних і пов'язана з цим неможливість отримати доступ до певної інформації).

Нині найнебезпечніші та найскладніші загрози є гібридними. Вони поєднують різні характеристики та функціональні можливості, а також використовують техніки повторного встановлення після видалення та перезавантаження пристрою, що ускладнює їх аналіз компаніями, які розробляють програмне забезпечення для захисту (зазвичай відоме як антивірусне програмне забезпечення).

ТИПИ ШКІДЛИВИХ ПРОГРАМ

Існує кілька типів шкідливого програмного забезпечення, класифікація яких зазвичай ґрунтується на способах їх поширення, хоча також застосовується класифікація за рівнем небезпеки, яку вони становлять. Нижче наведено ті типи, що мають найпоширеніші або найбільш загальні методи поширення.

Віруси та черв'яки (інфекційне шкідливе програмне забезпечення)

- Вони заражають інші файли та програми, модифікуючи їх для створення копій себе на зараженому пристрої.
- Вони також можуть бути запрограмовані на виконання інших дій, таких як видалення файлів або відображення реклами.
- Для поширення вірусів необхідне втручання користувача.
- Черв'яки самостійно розмножуються, поширюючись з однієї машини на іншу.

Троянські програми (приховане шкідливе програмне забезпечення)

- Маскуючись під «нешкідливі» програми, вони спонукують користувача запустити їх, створюючи шлюз для інших шкідливих програм.

- Вони не здатні самовідтворюватися і не можуть поширюватися самостійно, тому необхідне втручання користувача.
- Вони виконують свої дії непомітно.
- Вони збирають інформацію або дистанційно контролюють хост, ставлячи під загрозу конфіденційність і безпеку користувачів або перешкоджаючи їхній роботі.

Шпигунське програмне забезпечення (зловмисне програмне забезпечення для збору даних)

- Воно збирає інформацію з пристрою, на якому встановлено, і передає її особі, яка його встановила.
- Воно може шпигувати за поведінкою користувача в Інтернеті, даними, контактами, звичками використання, відвіданими сторінками, запущеними програмами, деталями підключення, переліком програм, встановлених на пристрої, тощо.
- Його кінцеві наслідки можуть бути серйозними, оскільки воно може сприяти крадіжці банківських даних та крадіжці особистих даних.

Інші відповідні типи шкідливого програмного забезпечення:

- **Незаконне програмне забезпечення:** зазвичай воно завантажується та встановлюється непомітно з Інтернету і, вводячи користувача в оману щодо того, що його пристрій заражений, пропонує безкоштовно встановити пробну версію антивірусної програми та платну версію для видалення нібито інфекції.
- **Програми-вимагачі** (криптовіруси, хакери): це програми, які шифрують (кодують) важливі для користувача файли, роблячи їх недоступними, а потім вимагають сплатити великий «викуп», щоб отримати пароль для відновлення доступу до «заблокованої» або «зашифрованої» інформації.

ЗАГАЛЬНІ РЕКОМЕНДАЦІЇ ЩОДО ЗАПОБІГАННЯ

Так само, як ми заохочуємо до основних заходів безпеки, щоб уникнути певних небезпек, які загрожують молодим людям у наш час, ми повинні пропагувати серед дітей захист їхніх пристроїв, враховуючи, що ми всі маємо при собі велику кількість конфіденційної інформації та даних, не тільки своїх, але й інших людей. Нижче наведено деякі загальні рекомендації для дітей:

- Перш за все, будьте обережні, критично мисліть і керуйтеся здоровим глуздом під час будь-якого спілкування або взаємодії в Інтернеті, особливо щодо несподіваних повідомлень та електронних листів від друзів, невідомих осіб або організацій.
- Ми повинні пам'ятати, що завантаження програмного забезпечення з ненадійних веб-сайтів або обмін файлами P2P (Peer-to-Peer, від одного комп'ютера до іншого) є ризикованим, тому доцільніше користуватися послугами завантаження від легально зареєстрованих

компаній з надійною репутацією. У разі сумнівів завжди краще не відкривати та не запускати файли, а перевірити іншими засобами надійність та безпечність того, що завантажується, відкривається або виконується.

- Знання своїх пристроїв, розуміння того, як вони працюють і поведуться в «нормальному» режимі, може допомогти виявити наявність шкідливого коду. Незвичайна або дивна поведінка може вказувати на зараження, і бажано звернути на це особливу увагу, якщо ви нещодавно встановили нову програму або переглядали сумнівні веб-сайти.
- Важливо, щоб на всіх пристроях завжди було встановлено «антивірусне» програмне забезпечення, яке забезпечує захист у режимі реального часу від потенційних атак, незалежно від використовуваної операційної системи. Воно не тільки постійно виявляє загрози, що виникають під час взаємодії з Інтернетом, але й може виявляти їх на флеш-накопичувачах, зовнішніх жорстких дисках або інших типах обладнання, підключених до ваших пристроїв. Крім того, ми повинні пам'ятати про необхідність регулярно проводити повне сканування комп'ютера і мати на увазі, що антивіруси мають обмеження і не є бездоганними, тому ми не повинні повністю покладатися на них для нашого захисту.
- Не менш важливо регулярно оновлювати програмне забезпечення (операційну систему, браузер, додатки тощо), оскільки виявлені в коді помилки зазвичай виправляються в цих оновленнях і запобігають доступу інших осіб до наших пристроїв з використанням цих помилок або вразливостей.
- Налаштування пристроїв та операційних систем, програм, додатків і служб у найбільш «закритому» або обмеженому режимі, навіть до початку їх використання, є рекомендованою стратегією для запобігання будь-яким вторгненням. Функції, такі як Bluetooth або служба визначення місцезнаходження, які наражають на ризик пристрої та їхніх користувачів, слід вмикати лише за потреби, а за замовчуванням залишати вимкненими.
- Дуже часто для входу в пристрої, мережі та інші сервіси використовуються прості та легкі для злому або виявлення паролі чи шаблони. Використання складних або надійних паролів є настільки ж важливим, як і тип замка, який ви маєте вдома. Створення паролів за допомогою впізнаваних комбінацій (рекомендується поєднувати літери, цифри та символи довжиною 8 або більше символів) або використання сервісів для генерації паролів допоможе скласти ключ, який, навіть якщо його і можна зламати, принаймні ускладнить це завдання для інших людей.

Мнемонічні правила або використання захищеного паролем або зашифрованого єдиного файлу, що містить усі ваші ключі, можуть допомогти без проблем їх запам'ятати. У будь-якому випадку, сьогодні майже всі сервіси надають дуже просту опцію відновлення пароля, якщо ви його забули.

- Нарешті, ми рідко замислюємося над надзвичайною важливістю регулярного створення резервних копій наших файлів (особливо тих, втрата яких може завдати серйозної шкоди). Таким чином, якщо наші файли або пристрої з будь-якої причини стануть недоступними, наслідки їх втрати будуть мінімізовані.

Майже так само важливим, як і профілактика, є раннє виявлення загрози, яка змогла подолати наші запобіжні заходи, та подальші коригувальні дії.



Виявлення та дії

Окрім застосування запобіжних заходів, діти повинні усвідомлювати необхідність вміти виявляти потенційні проблеми кібербезпеки, а також знати, принаймні на базовому рівні, що робити в таких випадках.

Після того, як шкідливе програмне забезпечення потрапило в нашу систему, його не завжди легко виявити. Однак ми можемо зіткнутися з проблемами, якщо виявимо деякі з таких симптомів у наших пристроях:

- Він надто нагрівається.
- Використовує занадто багато заряду батареї.
- Під час перегляду веб-сторінок без видимих причин з'являються спливаючі вікна.
- Наш браузер перенаправляє нас на небажані веб-сайти.
- Файли та програми зникають або виходять з ладу без видимих причин і без будь-яких незвичайних дій з нашого боку.

Залежно від серйозності зараження та наявності у нас достатніх знань, можна вжити таких заходів:

- Виконайте глибоке сканування та очищення за допомогою антивірусного/антишпигунського програмного забезпечення. Якщо у вас не встановлено антивірусне програмне забезпечення, існує кілька компаній, які пропонують безкоштовні інструменти для швидкого онлайн-сканування ваших пристроїв, або пробні чи спрощені версії, які можна встановити для більш ретельного пошуку. Якщо спочатку нічого не виявлено, може бути доцільним виконати додаткове сканування за допомогою іншого антивірусу, оскільки вони використовують різні інструменти виявлення.
- Очистіть використовуваний інтернет-браузер (файли cookie, плагіни, які могли бути встановлені тощо).
- Видаліть програми, плагіни або додатки, особливо якщо ви почали виявляти проблеми з пристроєм після їх встановлення.
- Зверніться за допомогою до спеціалістів.
- Відформатуйте пристрій (після створення резервної копії даних, налаштувань та відповідної інформації, оскільки ця дія призведе до видалення всього вмісту пристрою).



Незахищені з'єднання

Використання Інтернету в дорозі, за допомогою мобільних телефонів і планшетів, стає все більш поширеним. Це означає, що досить часто, особливо маленькі діти, шукають мережу, як правило Wi-Fi, щоб підключитися до неї. Дітей слід попередити, що ці точки підключення також можуть становити загрозу.

Підключаючись до Інтернету з будь-якого місця за допомогою кабелю, Wi-Fi, радіо тощо, ви отримуєте доступ і приєднуєтеся до мережі з мільйонами взаємопов'язаних пристроїв. Ці пристрої, як правило, мають вбудовані заходи безпеки, подібні до тих, що є на вашому власному пристрої, щоб мати доступ і переглядати тільки «відкритий» контент. Однак ці заходи безпеки можуть бути неправильно налаштовані або взагалі не налаштовані, або бути настільки привабливими, що їх можна спробувати зламати, і інші люди можуть, крім перехоплення наших повідомлень, отримати доступ до наших пристроїв через з'єднання з усіма пов'язаними з цим небезпеками. Аналогічно, мережі пристроїв, навіть без підключення до Інтернету, мають подібні особливості та ризики.

Ми повинні пам'ятати, що, незважаючи на те, що ми можемо контролювати конфігурацію власних пристроїв і підключень у себе вдома або школі,

ми, як правило, не знаємо, які заходи безпеки можуть бути вжиті в громадських або приватних місцях, де користувачам дозволено отримувати доступ до їхніх мереж, з підключенням до Інтернету або без нього.

Багато людей, особливо молодь, зазвичай економлять на використанні даних (які їхні інтернет-провайдери надають у певних межах), встановлюють програмне забезпечення для пошуку відкритих або легко зламуваних Wi-Fi-з'єднань, вважаючи, що вони «крадуть» Wi-Fi. Роблячи це, вони не усвідомлюють пов'язаних з цим ризиків і наражаються на небезпеку потрапити в пастку, влаштовану іншими людьми, які «відкривають» своє з'єднання, щоб встановити зв'язок між пристроями і, як результат, отримати доступ до тих, що підключені.

Так само безкоштовні або відкриті з'єднання можуть приховувати шахрайські наміри. Головне, чого слід уникати, — це підключення до відкритої публічної мережі Wi-Fi (без пароля), оскільки це може бути пасткою, коли безкоштовна мережа надається кіберзлочинцем, який пропонує її поблизу під назвою, що помилково наводить вас на думку, що це саме та мережа, яку ви шукали.

Фальшиві посилання

Поширеною загрозою, яка регулярно приносить багато результатів, є надання фальшивих посилань, під невинним і часом невігядливим виглядом, що приводить користувачів до справжніх обманних ситуацій, починаючи з того, що користувачі надають конфіденційні дані. Хоча діти зазвичай не є об'єктом кіберзлочинів з фінансових причин, саме тому, що вони не мають власних грошей або коштів, важливо, щоб вони були ознайомлені з цими техніками, оскільки вони можуть застосовуватися до платіжних систем, пов'язаних з їхньою діяльністю, таких як онлайн-покупки або відеоігри.

ЯК ВОНИ ПРАЦЮЮТЬ?

Вони надходять безпосередньо (через електронну пошту, WhatsApp, форуми або мережі) або опосередковано (банери, реклама, завантаження прихованого шкідливого програмного забезпечення тощо) і при активації перенаправляють, як правило, на веб-сторінки, ідентичні справжнім, де користувачеві пропонується заповнити форму. Коли користувач заповнює форму, надаючи запитовані дані, вони потрапляють під контроль кіберзлочинців. Деякі з цих повідомлень апелюють до наших почуттів співчуття або солідарності (труднощі з отриманням спадщини, оскільки вони живуть у далекій країні),

цікавості («дізнайтеся, хто видалив вас зі своєї групи друзів»), наївності («ви виграли автомобіль»), або попередження чи погрози («підтвердження даних, необхідних для встановлення оновлень системи»). Серед мільйонів повідомлень, що надсилаються автоматично, багатьом з них вдається обдурити велику кількість людей.

Однією з найприбутковіших технік шахрайства для кіберзлочинців є фішинг, який працює наступним чином:

- Зображення банку замінюється іншим, щоб отримати номери рахунків, паролі та інші конфіденційні дані.
- Вони можуть відображати логотип банку, але зазвичай не персоналізовані, оскільки розсилаються масово і часто містять граматичні та орфографічні помилки.
- Посилання перенаправляють користувачів з електронних листів на сторінки, які не починаються з «https», і значок замка не відображається (це означає, що вони не мають цифрового сертифіката).
- Сторінка, на яку вони перенаправляють, дуже схожа на оригінальну сторінку банку.



ПРОФІЛАКТИЧНІ ЗАХОДИ

Щоб зменшити ймовірність потрапляння на шахрайське посилання, рекомендується:

- Вводити URL-адресу або адресу веб-сторінки в браузері, а не натискати на посилання, надані в електронних листах, повідомленнях або на веб-сайтах.
- Переконайтеся, що сторінка використовує протокол «https» (з літерою «s» наприкінці) і що на ній відображається символ замка, пов'язаний із цифровим сертифікатом. Цей символ або піктограма зазвичай з'являється внизу рядка стану або вгорі адресного рядка веб-браузера. При натисканні на нього з'явиться вікно з описом цифрового

сертифіката, який, коротко кажучи, є сертифікатом, підписаним певним органом, що надає інформацію про власника веб-сайту, до якого здійснюється доступ.

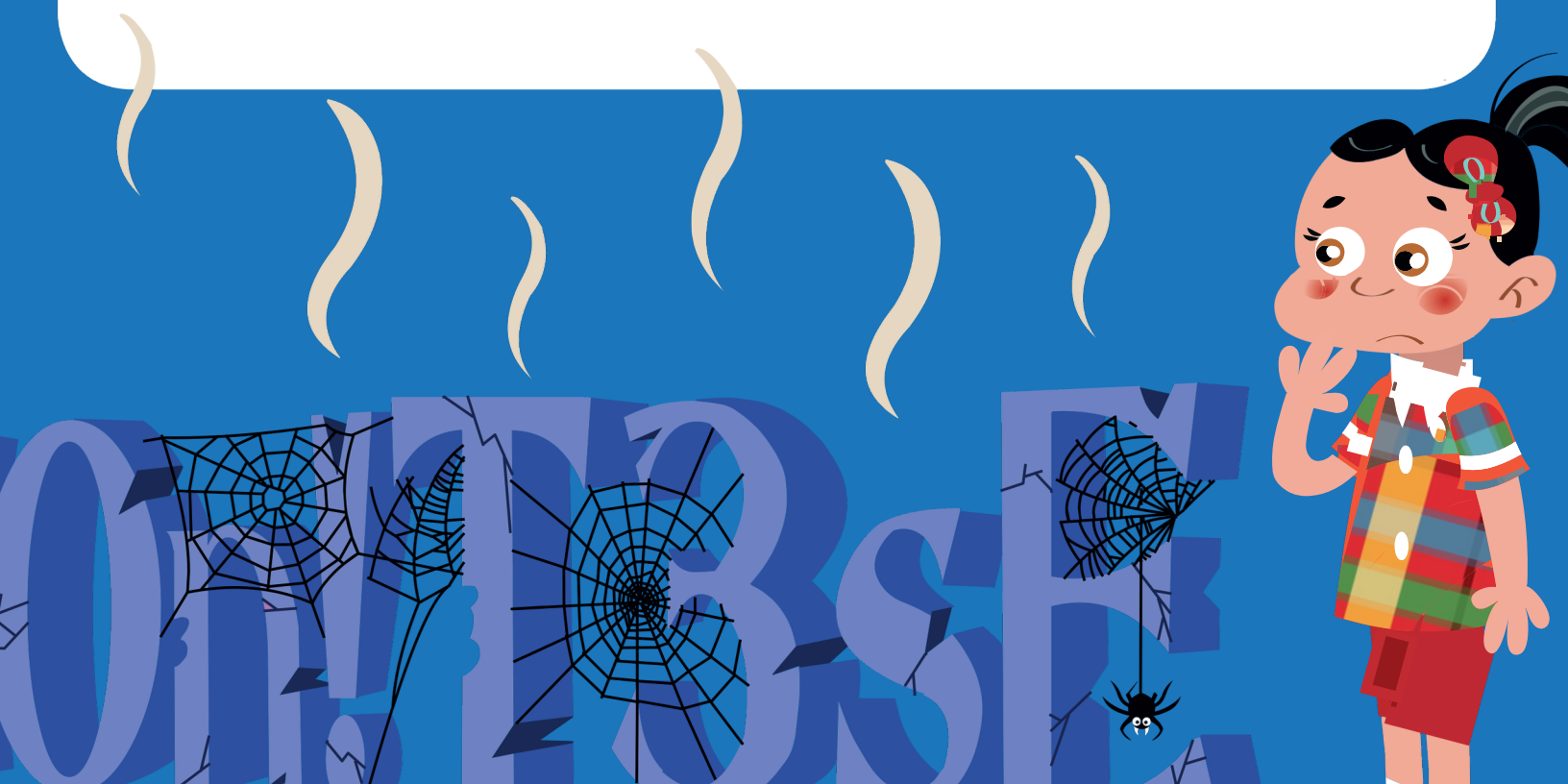
- Пам'ятайте, що банки або компанії ніколи не запитують особисті дані електронною поштою.
- Уникайте введення конфіденційних даних і, якщо ви маєте сумніви, зверніться безпосередньо до компанії.
- Дотримуйтесь здорового глузду, який підказує, що ніхто не віддає щось просто так.

Несанкціонований доступ до пристроїв

Мобільний телефон – це портативний пристрій, яким ми користуємося постійно, і який, як такий, можна забути, загубити або навіть вкрати. Він також може потрапити до рук невідомих небажаних осіб, якщо його залишити без нагляду. Важливо заохочувати дітей замислитися над цим і мати це на увазі також з точки зору конфіденційності. У цьому випадку слід розглянути кілька запобіжних заходів, таких як:

- Встановіть пароль, графічний ключ або PIN-код та/або цифровий доступ до пристрою, щоб тільки його законний власник міг користуватися вмістом, що на ньому зберігається.
- Заблокуйте додатки, браузери та програми від збереження паролів у пам'яті пристрою, щоб інші люди, які можуть отримати доступ до мобільного телефону, не могли автоматично отримати доступ до них або робити щось під чужим ім'ям.

- Запишіть і зберігайте в безпечному місці IMEI мобільного телефону. Це унікальний код, який ідентифікує пристрій і, в разі крадіжки або втрати, допомагає повідомити про це. Це дозволяє, наприклад, заблокувати будь-які дзвінки, зроблені з цього пристрою. Зазвичай, щоб отримати цей код, можна ввести в додатку, який використовується для здійснення телефонних дзвінків, наступні символи: *#06# (зірочка, решітка, нуль, шість, решітка).
- Існують додатки, програми та сервіси, які використовуються для пошуку та відстеження пристроїв, мобільних телефонів і ноутбуків, і якщо їх встановити до крадіжки або втрати, вони допоможуть їх знайти.
- Існують інші програми, які дозволяють дистанційно видалити інформацію, що зберігається на пристрої (відновити заводські налаштування), знайти особу, яка його тримає (зробивши фотографію особи, яка його вмикає, ідентифікувавши номер SIM-карти, що використовується тощо).



Безпечні паролі

Паролі є першою лінією захисту від несанкціонованого доступу до даних (розмов, зображень, контактів тощо) та особистих послуг, які можуть бути використані для заподіяння нам шкоди. Паролі є першою перешкодою в кібербезпеці, воротами до нашого цифрового життя, і тому вони повинні бути надійними. Їх вибір є важливим рішенням, яке доводиться приймати часто.

Паролі дорівнюють приватності, оскільки вони відкривають доступ до особистої інформації. Однак вони також пов'язані з безпекою власника, оскільки доступ до певних даних може бути використаний для заподіяння серйозної шкоди різними способами, такими як крадіжка особистих даних або шантаж. Загалом, паролі є воротами до цифрового життя, і тому вони повинні бути надійними. Хлопчики та дівчатка повинні знати, як створити ці бар'єри надійним чином.

Рекомендації щодо захисту від загроз вашій кібербезпеці

Як бачимо, існує кілька аспектів кібербезпеки, які повинні враховувати всі: діти, а також дорослі. Їх можна узагальнити у восьми рекомендаціях, які можна легко донести до дітей:

- Використовуйте антивірусне програмне забезпечення на всіх пристроях (комп'ютері, мобільному телефоні або планшеті), які ви використовуєте для підключення до Інтернету. Існує багато безкоштовних програм, сумісних з усіма операційними системами.
- Оновлюйте операційну систему та програми, оскільки вони містять виправлення безпеки.
- Завантажуйте програми з офіційних магазинів. Не довіряйте програмному забезпеченню сумнівної легальності або походження, оскільки воно може містити шкідливе програмне забезпечення.
- Уникайте відкриття посилань або несподіваних файлів від невідомих осіб або джерел. Не завантажуйте їх автоматично.
- Звертайте особливу увагу на те, де ви вводите свої паролі і хто їх запитує. Якщо адреса веб-сторінки починається з «https», це означає, що вона є безпечною і надійною.

БЕЗПЕЧНИЙ ПАРОЛЬ У ВОСЬМИ КРОКАХ

1. Він має містити щонайменше 8 символів.
2. Він не має бути легким для вгадування (ім'я, дата народження тощо).
3. Він має містити великі та малі літери.
4. Він має містити цифри та літери.
5. Він не має зберігатися на жодному пристрої. Його слід вводити вручну кожного разу, коли це потрібно.
6. Це секрет, яким не слід ділитися ні з ким, хто не є членом сім'ї.
7. Його слід регулярно змінювати.
8. Він має бути різним для кожної служби, соціальної мережі або програми.

- Підключення до відкритих громадських мереж Wi-Fi є ризикованим. Намагайтеся не робити нічого важливого, оскільки ваші комунікації можуть бути прослухані.
- Вмикай служби для обміну інформацією з вашого мобільного телефону, такі як Bluetooth, тільки тоді, коли ви збираєтеся ними користуватися.
- Будьте пильні та перевіряйте інформацію про людей, з якими ви спілкуєтеся, та послуги, якими ви користуєтеся. Пошук інформації або відгуків в Інтернеті для їх перевірки може допомогти виявити шахрайство та афери.



Приватність

Вступ

Про конфіденційність вже багато сказано. Конфіденційність є постійною темою, з якої ми виділимо лише два основні аспекти: з одного боку, концепція конфіденційності змінюється; з іншого боку, все більше поширюється думка, що її захист є дуже складним завданням, якщо не просто неможливим.

ЧОМУ ПРИВАТНІСТЬ Є ВАЖЛИВОЮ?

Є дві основні причини:

- Це фундаментальний елемент безпеки.

Інформація про те, хто ви, як виглядаєте, хто ваші друзі та родичи, де ви знаходитесь, що вам подобається, чим займаєтесь тощо, є найкращим джерелом інформації для тих, хто хоче вам нашкодити.

- Це впливає на ваш імідж, ідентичність та цифровий слід.

Можливо, зараз ви не вважаєте це важливим.

Можливо, ви вважаєте, що те, що ви публікуєте або що про вас говорять, важливо лише тут і зараз та лише для людей, про яких ви думаєте. Однак слід, залишений інформацією про вас в Інтернеті, може негативно вплинути на вас у недалекому майбутньому. Цей слід може бути глибоким, широким і майже неможливим для видалення.

ЯКІ МОЖЛИВІ НЕГАТИВНІ НАСЛІДКИ?

Якщо ви не дбаєте про свою приватність, не відбираючи та не керуючи тим, що ви хочете опублікувати, і тим, хто може про це дізнатися, ви можете створити певні ризики:

- Ви стаєте більш вразливими до різних небезпек: сексуальних кіберхижаків, кібербулінгу, сексторції, крадіжки особистих даних тощо.
- Вашу ідентичність і цифрову репутацію стає дедалі складніше контролювати або змінювати.
- Ви можете засмутити інших або піддати їх ризику, публікуючи моменти свого життя, якими ви ділилися з ними.

Пам'ятайте

- Якщо хтось хоче вам нашкодити, він може зробити це різними способами, і чим більше він знає про вас, тим легше йому це буде.
- Приватність і кібербезпека йдуть рука в руку. Якщо ваші пристрої вразливі або ваші паролі не є безпечними, ваша приватна інформація буде під загрозою.
- Те, що відомо про вас, також залежатиме від дій інших людей: так само, як ви відповідальні за їхню конфіденційність.
- Якщо ви хочете зберегти свою конфіденційність, ви повинні взяти запобіжних заходів. Повідомте людям, з якими ви спілкуєтесь, яку інформацію про вас вони можуть і не можуть поширювати, і яким чином.
- Ви маєте право вирішувати, як використовувати ваші особисті дані, включаючи ваше зображення.
- Онлайн-сервіси та додатки, якими ви користуєтесь, є ще одним способом розкриття вашого особистого життя, навіть якщо ви цього не усвідомлюєте.



Приватність як право та фактор захисту

Приватність вже не є опцією. Приватність настільки важлива, що стала однією з ключових проблем в Інтернеті. Насправді, це постійне поле битви між великими інтернет-компаніями та державними установами, які прагнуть захистити дані та права своїх громадян. Це також є предметом суперечок між окремими особами, оскільки в Інтернеті нас постійно запрошують, а іноді й спонукають ділитися інформацією, навіть інформацією про інших. Приватність вислизає з наших рук, як пісок.

ПРИВАТНІСТЬ ЯК ПРАВО

Наприкінці 2013 року Генеральна Асамблея Організації Об'єднаних Націй прийняла резолюцію, в якій закріпила право на приватність і закликала держави-члени припинити діяльність, що порушує «принцип демократичного суспільства». Резолюція містила прохання до Верховного комісара ООН з прав людини подати звіт про захист і просування права на приватність у контексті внутрішнього та екстериторіального спостереження. Стаття 12 Загальної декларації прав людини вже встановила, що право на приватність є правом людини. Ця стаття також включає право на самозахист у цифрову епоху, коли в ній зазначається, що «Ніхто не може бути підданий довільному втручанню в його приватне життя, сім'ю, житло або листування, а також нападкам на його честь і репутацію. Кожен має право на захист закону від такого втручання або нападів».

З іншого боку, в рамках цього права передбачені спеціальні заходи захисту дітей та осіб з інвалідністю, які перебувають у особливо вразливому становищі. Нарешті, відповідно до Конвенції про права дитини (КПД) «найкращі інтереси дитини» повинні розглядатися як право, принцип законодавчого та процесуального правила, згідно з яким благополуччя та права хлопчиків та дівчаток мають пріоритет у разі конфлікту з іншими інтересами.

Приватність дітей в Інтернеті є надзвичайно важливим питанням і потребує особливої уваги. У Європейському Союзі Загальний регламент про захист даних (GDPR), чинний з 25 травня 2018 року, встановив як загальне правило вік 16 років (і в будь-якому разі не нижче 13 років у разі застосування винятків) як мінімальний вік, з якого особа може мати повну автономію для надання згоди на обробку своїх персональних даних у послугах інформаційного суспільства, зокрема в соціальних мережах.

ПРИВАТНІСТЬ ЯК ФАКТОР ЗАХИСТУ

Безсумнівно, чим більше інформації відомо про людину, тим вразливішою вона стає. У цифровому контексті це має критичне значення, оскільки заподіяти людині біль надто легко, швидко і часто безкарно. Нерівність сил між жертвою та агресором в Інтернеті посилюється фактором конфіденційності, який майже завжди схиляється на користь того, хто завдає шкоди. Агресори можуть вдаватися до анонімності, підробки особи або самозванства, щоб приховати свою ідентичність, а жертви – ні. Вони все одно мусять жити своїм життям в Інтернеті під своїм ім'ям і, на жаль, без повного контролю над тим, що про них відомо.

Завдати шкоди людині в Інтернеті надзвичайно легко (погрозові повідомлення, наклеп і дифамація, містифікації, зневага тощо), і що більше інформації відомо про жертву, то інтенсивнішою та прихованішою може бути ця шкода. Отже, робота над створенням безпечнішого Інтернету також потребує зменшення ймовірності віктимізації та масштабу можливої шкоди. Усе це безпосередньо пов'язано з ефективним і свідомим управлінням конфіденційністю та персональними даними.



Виховання культури конфіденційності

Втрату приватності громадян можна аналізувати з багатьох різних точок зору. Оскільки це досить широка тема, що охоплює контроль, об'єднання та обмін інформацією між державними органами або великими компаніями, а також Інтернет речей (IoT), доцільно зосередитися на повсякденних і звичних питаннях.

ПРИВАТНІСТЬ ПІД ЗАГРОЗОЮ ЗНИКНЕННЯ

Чому наша приватність так сильно зменшилася? Простіше кажучи, можна сказати, що це залежить від особистої інформації, яка була створена, збережена, збагачена (а отже, отримала додаткову цінність і більше значення) та передана або опублікована.

- Більше інформації, що генерується: Генерування особистої інформації відбувається постійно і, як правило, несвідомо. Ми можемо думати як про особисте зображення, яке було опубліковано і позначено тегами (наприклад, у геолокалізації, яку наш мобільний телефон може постійно реєструвати), так і про електронну покупку продукту або послуги. Цікаво, що ми всі носимо з собою фото- та відеокамеру, вбудовану в наш смартфон.
- Більше інформації, що зберігається: зберігання цифрової інформації зазнало постійної революції завдяки зниженню цін на пристрої для зберігання даних та широкому спектру технологій і пристроїв, які стали більш універсальними. За кілька років ми перейшли від носіння друкованої фотографії родича в гаманці до носіння в мобільному телефоні десятків зображень і відео людей, яких ми знаємо, і навіть людей, яких ми не знаємо.
- Більш збагачена інформація: в інформаційному менеджменті взаємопов'язані дані збільшують свою цінність. Сучасні технології дозволяють нам використовувати інформацію, яка завдяки зв'язкам, доказам або припущенням дає нову похідну інформацію з високою доданою вартістю, що перевищує просте додавання агрегованих даних.
- Більше інформації передається/публікується: незалежно від того, що можуть робити великі корпорації або державні служби (в межах законодавства та практики саморегулювання), очевидно, що саме ми, люди, в більшості випадків ділимося цією інформацією. Це стає все легшим, зручнішим, швидшим і дешевшим, і ми переборщуємо, приділяючи занадто багато уваги комерційним інтересам, які закликають нас «ділитися своїм життям».

Чи загрожує приватність зникненню? Очевидно, що приватність сьогодні не є такою ж, як до появи мобільних телефонів. Тому приватність нашого часу не можна порівняти з тією, що існувала до появи Інтернету в наших домівках.

Соціальні мережі, з іншого боку, ставлячи користувачів у роль творців і споживачів особистої інформації, стали поворотним моментом у питанні конфіденційності. Це стало ще більш очевидним із поширенням смартфонів, які полегшують наше життя і цифровізують його, буквально на кожному кроці.

ТРАДИЦІЙНА ОСВІТА З ПИТАНЬ ПРИВАТНОСТІ В ІНТЕРНЕТІ

З метою підвищення обізнаності населення, особливо дітей, зазвичай проводяться кампанії з захисту персональних даних, що зосереджуються на двох аспектах. З одного боку, це налаштування наших параметрів конфіденційності в соціальних мережах, а з іншого - ідентичність та цифрова репутація. В обох випадках основна увага приділяється обмеженню поширення персональної інформації та аналізу її наслідків у довгостроковій перспективі. Крім того, останнім часом ведуться розмови про захист мобільних телефонів за допомогою паролів та підвищення обізнаності про те, що публікується про інших людей, коли це може їм зашкодити. Певним чином здається, що тягар конфіденційності лягає на нас самих і що це є єдиною основою для дій.

СПІЛЬНА ПРИВАТНІСТЬ

Розгляд приватності виключно як особистої проблеми дедалі більше віддаляється від нашого сучасного повсякденного життя. Ми живемо у взаємопов'язаному суспільстві з гіперпідключеними людьми, де типовою поведінкою, імпульсом, є обмін інформацією. Діти часто сприймають це як імітаційну гру, жарт або хобі. Діти, а дедалі частіше й молоді люди та дорослі, роблять це необдуманно, постійно й компульсивно.

Це явище іноді називають «екстимністю» (публічним розкриттям інтимності), «надмірним поширенням» (oversharing) або «шерентингом» (коли батьки поширюють зображення своїх дітей). Однак досить часто те, чим люди діляться, також зачіпає приватність інших. У наш час ділитися своїм життям офлайн неминуче означає ділитися ним і онлайн, і від цього моменту приватність стає надзвичайно делікатним викликом.

Саме тому приватність перестала належати лише нам і перебувати під нашим виключним контролем. Навпаки, вона перетворилася на колективно керовану цінність, тобто спільну приватність (coprivacy). Просування цінності та культури приватності й інтимності має ґрунтуватися на цій концепції спільної приватності — як узгодженої, усвідомленої та відповідальної практики щодо власної приватності, приватності інших людей і спільної приватності, а не лише як індивідуальної практики.

Звичайно, важливо знати, що про нас публікується, як і де; однак, без сумніву, джерело цього виходить за межі наших можливостей прийняття рішень, оскільки воно залежить також від інших людей. У цьому контексті приватність стає практикою щодо прав і обов'язків цифрового громадянства.

КІБЕРБЕЗПЕКА ТА ПРИВАТНІСТЬ

Взаємозв'язок між конфіденційністю та кібербезпекою легше зрозуміти, якщо розглядати його як колективну проблему. З одного боку, конфіденційність та кібербезпека є взаємопов'язаними поняттями, оскільки жодна інформація не може бути гарантовано конфіденційною, якщо немає впевненості в її безпеці та захищеності. З іншого боку, кібербезпека є проблемою, яку необхідно вирішувати та підтримувати в рамках спільнот: чим безпечніше середовище, тим безпечніші його компоненти. Оскільки ми живемо у взаємопов'язаному світі, високий рівень кібербезпеки можна досягти лише за умови наявності зв'язків, що відповідають вищезазначеним основним принципам.

ІДЕНТИЧНІСТЬ ТА ЦИФРОВИЙ СЛІД

Наша ідентичність та цифровий слід є аспектами, які тісно пов'язані з приватністю та мають велике значення, оскільки вони можуть впливати на соціалізацію та життя дітей як зараз, так і в майбутньому. Можна сказати, що наша цифрова ідентичність - це те, як нас бачить Інтернет, або, іншими словами, те, що про нас формують пошукові системи (передусім Google) та, меншою мірою, інші інтернет-гіганти, такі як Meta/Facebook, Instagram чи Twitter, і що змушує людей думати, ким ми є. Вона складається з того, що ми говоримо (пишемо) і робимо, з того, що інші люди говорять (відображають, показують або пишуть) про нас і їх взаємодії, а також з того, як ця інформація показується іншим через додатки або інтернет-сервіси. Навіть такі помітні відсутності, як відсутність у дитини акаунта в Instagram, формують цифрову ідентичність.

Наш цифровий слід - це онлайн-слід, який кожен з нас залишає після себе, і він пов'язаний з нашою цифровою ідентичністю, зокрема з діями, які мали значний вплив на Інтернет протягом нашого життя. Діти мають усвідомлювати важливість цих двох понять і те, як вони на них впливають. Хоча це не завжди так і не завжди справедливо, цифрова складова їхньої ідентичності з кожним днем стає дедалі актуальнішою. Невідповідна репутація в Інтернеті або свідчення минулих проступків можуть мати негативні наслідки для людей, які навіть не усвідомлюють цього й не можуть цього уникнути.



Соціальні мережі, тегування та геолокація

Окрім соціальних та культурних змін, два елементи стали ключовими для руйнування конфіденційності: соціальні мережі, які соціалізують інформацію, та мобільні телефони, які автоматично реєструють дані, серед яких інформація про геолокацію. Щоб діяти відповідально та проактивно в контексті цього виклику, діти повинні усвідомлювати це з самого раннього віку.

УПРАВЛІННЯ ПРИВАТНІСТЮ В СОЦІАЛЬНИХ МЕРЕЖАХ

Якщо обмежити питання управління конфіденційністю сферою соціальних мереж, то конфіденційність залежить від трьох факторів:

- те, що ми публікуємо самі, і як ми це робимо (обмежено, публічно тощо);
- спосіб, у який платформа, на якій ми публікуємо, обробляє цю інформацію;
- і, зокрема, інші люди.

Дуже наочним прикладом є теги зображень у соціальних мережах. Незалежно від того, хто опублікував зображення, якщо хтось додає теги, пов'язуючи кожну особу, яка з'являється на фотографії, з ідентифікатором у соціальній мережі, це має мультиплікативний ефект: соціальна платформа бере на себе обов'язок інформувати спільноту про те, що існує зображення, на якому з'являються певні користувачі, а також уся інформація, що міститься в ній.

Це може бути більш-менш явно. Отже, з трьох факторів, що впливають на конфіденційність (що публікується і як, як поведуться з цією інформацією та іншими людьми), можна зробити висновок, що найважливішими є ті, якими ми не можемо керувати. Можна подумати, що ми маємо можливість вибирати, на якій платформі публікувати інформацію, і знати, як вона керує цією інформацією на різних рівнях, мікро- та макро. Але реальність є зовсім іншою. Ми не можемо ні вибирати, ні гарантувати певним і постійним чином, що ми знаємо наслідки зміни правил конфіденційності соціальних мереж. Теги на зображеннях у соціальних мережах є яскравим прикладом цього. Тому варто підняти таку поширену тему серед дітей.

ТЕГИ ФОТОГРАФІЙ

Завантаження зображень в Інтернет стає з кожним днем все простішим і поширенішим. У соціальних мережах також є можливість додавати теги, тобто пов'язувати людей із цими зображеннями. Чи замислювалися діти над наслідками цієї функції? Ми повинні допомогти їм це з'ясувати.

Тегування в соціальних мережах може становити пряме й явне порушення права на приватність, оскільки платформа повинна отримати попередню та чітко виражену згоду особи, яку тегують, перш ніж оприлюднювати її зображення та робити його публічним.



Яке право має хтось ідентифікувати вас на зображенні - з урахуванням наслідків у контексті та додаткових даних - фактично пов'язуючи вашу особу з набором світлих точок або пікселів? І на яких етичних підставах соціальна мережа дозволяє, заохочує та поширює таку практику?

Публікація зображення в соціальній мережі є майже щоденною дією для дітей. Дуже часто ці зображення доповнюються тегами. Якщо завантаження зображення в Інтернет може в деяких випадках бути порушенням конфіденційності людей на зображенні, то який ефект може мати використання тегів? Давайте розглянемо це в загальних рисах, відкинувши операційні та конфігураційні відмінності між різними соціальними мережами. Простіше кажучи, можна сказати, що тег на зображенні - це позначка або знак, який пов'язує зображення, а конкретно - його прямокутну область, з конкретною особою. Ця позначка зазвичай пов'язана з областю на зображенні, де знаходиться ця особа. Що відбувається, коли вас тежують? Є два ефекти:

- **Ефект асоціації:** якщо вас позначили, ви пов'язані з цим зображенням, а саме з ділянкою цього зображення, на якій зазвичай перебуваєте. Однак немає можливості гарантувати цю асоціацію, оскільки соціальна мережа дозволяє позначити графічну ділянку, набір пікселів, який вона не може інтерпретувати.
- **Ефект поширення:** коли вас позначили, ваші «друзі» в соціальній мережі отримають повідомлення про те, що вас позначили на новому зображенні і що їм потрібно лише натиснути, щоб його переглянути. Ефект привабливості та поширення цієї функції, пов'язаної із зображеннями, що пропонуються соціальними мережами, настільки сильний, що навіть користувачі користуються нею для інших цілей, наприклад, для ідентифікації особи на зображенні, і обидві ці функції далекі від початкової мети.

Коротко кажучи, це означає, що інші люди отримають повідомлення про те, що ви пов'язані з зображенням, і вони зможуть побачити його ще до того, як ви дізнаєтеся про його публікацію. Якщо вам пощастить, ви можете знати про існування цього зображення і про те, що ви є його частиною. Ви навіть можете припустити, що хтось завантажив його в Інтернет, незалежно від того, подобається вам це чи ні. Однак тег є сигналом тривоги, адже він публічно поширює інформацію про ваше життя, часто без вашого контролю, за участю інших людей і соціальних мереж. Раптом багато ваших «друзів» дізнаються, що можуть побачити кадр з вашого життя, і дуже часто діляться ним з іншими людьми. На більш практичному рівні, незалежно від того, що встановлено відповідним законодавством про особисті дані, ми можемо визначити конкретні ситуації, в яких теги спричиняють проблеми з

конфіденційністю, які дуже часто є причиною та/або наслідком поганого цифрового співіснування. Деякі з них можуть бути спричинені випадково або навмисно:

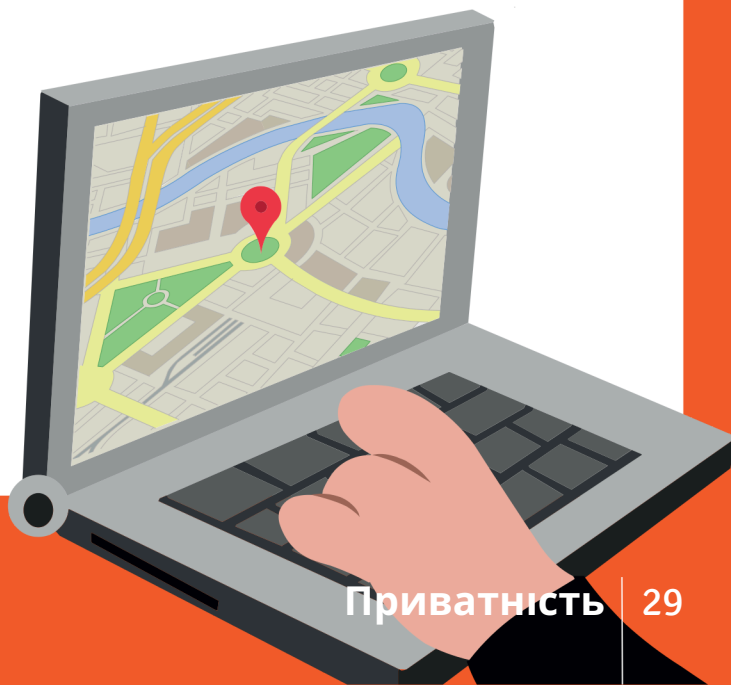
- тегування в контексті, який є недоречним через поведінку, місце, час або компанію;
- тегування, що показує фізичну зовнішність людини, зображену в соціальній мережі без зображення або з аватаром;
- образи, публічні зловживання та погрози, наприклад, пов'язані з особою, позначеною тегом на фотографії, що шкодить її особистому іміджу або є загрозливою.

Обман полягає в тому, що зображення, яке може бути образливим або неприємним, стає доступним для перегляду особи, яку позначили, у відповідь на сповіщення про тег, пов'язаний із нею.

ГЕОЛОКАЛІЗАЦІЯ

Завдяки можливості геолокалізації або геореференціювання, доступній у смартфонах, тобто визначенню місця, де вони знаходяться, ми можемо отримати більше переваг. Разом з функціональністю телефонів, що працюють як карти та компаси, ці функції надають інші важливі дані, такі, як хто може бути поруч або яка інформація може бути кориснішою в цьому конкретному місці та часі. Це надає велику додаткову цінність користувачам, які, можливо, платять за це ціною своєї приватності.

Якщо дозволи встановлені у відкритому режимі, будь-яка дія, виконана за допомогою нашого мобільного телефону та його додатків, може містити додаткову інформацію (у вигляді метаданих, непомітних на перший погляд або у більш явній формі) про місце, де вона була отримана, а отже, і про місцезнаходження особи, яка в цей момент користується терміналом. Не завжди легко це контролювати. Ці дані можуть становити загрозу безпеці, оскільки можуть розкривати точне місцезнаходження, включаючи географічні координати, особи або місце, де було зроблено фотографію.



Необхідно підвищувати обізнаність щодо цього питання. Установлені додатки зазвичай за замовчуванням мають увімкнений режим визначення місцезнаходження. Саме програмне забезпечення телефону постійно - і за першої ж нагоди - пропонує нам надати доступ до даних про місцезнаходження пристрою. На цьому слід особливо наголошувати дітям, які можуть навіть не усвідомлюючи наражати себе на серйозні небезпеки, зокрема викрадення.

Захист вашої конфіденційності на смартфоні

Ваш смартфон містить велику кількість інформації та особистих даних. Ваші контакти, доступ до програм, якими ви зазвичай користуєтеся, таких як Instagram або WhatsApp, фотографії тощо, – все це знаходиться у вашому мобільному телефоні, де також можна знайти решту ваших даних. Існує й інша інформація, про яку ви, можливо, не знаєте, але яка також зберігається: мережі Wi-Fi, до яких ви підключаєтеся, або місця, де ви бували.

Тому дітям необхідно бути повністю обізнаними з цією проблемою та вживати всіх заходів, які є в їхньому розпорядженні, щоб використання мобільного телефону не становило загрози в цьому плані. Нижче наведено десять рекомендацій, які слід знати, розуміти та приймати.

Ключі до збереження вашого приватного життя та даних

Говорячи про приватність, ми говоримо про кібербезпеку, а отже, про здоров'я та благополуччя дітей. Надзвичайно важливо допомогти їм стати компетентними, свідомими та критично мислячими учасниками в цьому питанні й надати їм такі базові рекомендації:

- Дбайте про безпеку своїх пристроїв та інтернет-з'єднань. Використовуйте надійні паролі.
- Закривайте камеру комп'ютера, коли не використовуєте її.
- Пам'ятайте, що все, що з'являється на екрані, може бути зафіксовано: розмови, зображення, відео... З цього моменту ви назавжди втрачаєте над ними контроль.
- Звертайте увагу на метадані (додаткові приховані дані), такі як геолокація. Вони можуть розкрити про вас інформацію, про яку ви навіть не здогадуєтеся.
- Звертайте особливу увагу на налаштування конфіденційності на ваших пристроях, в

ДЕСЯТЬ ПРАВИЛ ЗАХИСТУ ПРИВАТНОСТІ ВАШОГО МОБІЛЬНОГО ТЕЛЕФОНУ

1. Встановіть програмне забезпечення для захисту (антивірус) для боротьби зі шкідливим програмним забезпеченням на вашому мобільному телефоні.
2. Оновлюйте операційну систему мобільного телефону, щоб підвищити рівень безпеки.
3. Заблокуйте свій пристрій надійним паролем (цифри та літери) або графічним ключем.
4. Уникайте зберігання пароля в додатках, які є для вас найбільш важливими.
5. Увімкніть службу визначення місцезнаходження мобільного телефону на випадок його втрати.
6. Дізнайтеся, як дистанційно заблокувати та видалити дані з мобільного телефону на випадок його втрати або крадіжки.
7. Увімкніть геолокацію на пристрої та в окремих додатках тільки тоді, коли це необхідно, і з розумінням наслідків.
8. Перевіряйте дозволи, які запитує кожна програма під час її встановлення, і переконайтеся, що вони не є зловживанням.
9. Встановлюйте додатки з офіційних магазинів, щоб уникнути шкідливого програмного забезпечення.
10. Будьте особливо обережні перед відкриттям невідомих посилань, файлів або невідомих мереж Wi-Fi.

додатках та соціальних мережах:

- Дізнайтеся, де знаходяться відповідні опції.
- Переконайтеся, що ви розумієте їх значення та наслідки.
- Увімкніть їх відповідно до своїх уподобань та потреб.
- Будьте пильні перед будь-якими змінами в них.

- Будьте обережні з людьми, які погано управляють своєю конфіденційністю або не вживають основних заходів кібербезпеки, оскільки це може мати негативні наслідки для вас. Допмагаючи їм, ви допомагаєте собі.
- Уникайте тегування зображень у соціальних мережах, оскільки зображення, пов'язані з людьми, можуть надавати занадто багато інформації.



Кібербулінг

Вступ

Онлайн-переслідування серед однолітків, яке зазвичай називають кібербулінгом (через схожість із терміном «булінг», що застосовується до переслідування в шкільному середовищі), без сумніву, є серйозною проблемою в класі. Це дуже специфічна форма цифрового насильства серед дітей яка постійно зростає і має наслідки, що виходять за межі шкільного контексту.

Страждання жертви булінгу є надзвичайно інтенсивними. Вони можуть проявлятися у вигляді смутку, ізоляції, відсутності впевненості та самоповаги, порушень сну та харчування, виникнення психосоматичних розладів тощо. Це залишає глибокі та тривалі шрами у тих, хто страждає від цього.

Пам'ятайте

- Кібербулінг є найактуальнішою проблемою, з якою стикаються діти в Інтернеті: він завдає серйозної шкоди, трапляється досить регулярно і його надзвичайно важко запобігти та зупинити.
- Важливо усвідомлювати, що відсутність фізичної агресії не означає відсутність жертв або заподіяної шкоди.
- Оскільки Інтернет є дуже потужним інструментом, коли його використовують для заподіяння шкоди, його наслідки можуть бути руйнівними. Існує значний дисбаланс сил між жертвами та агресорами.
- Цей тип цифрового насильства серед однолітків має три переваги: його легко здійснювати, він має негайні наслідки і завжди доступний.
- Люди, які страждають від кібербулінгу, мають схильність до ізоляції, іноді вони відчують провину за свою ситуацію. Зазвичай вони не просять про допомогу на ранніх стадіях.

Визначення та опис кібербулінгу

Кібербулінг – це умисне, повторюване і тривале переслідування через Інтернет (соціальні мережі, відеоігри, миттєві повідомлення, веб-сторінки тощо) однієї або декількох осіб щодо жертви, яка є однолітком і пов'язана з ними в шкільному контексті, над якою вони мають або встановлюють позицію переваги чи то через безкарність, чи то через нав'язування свого контролю. Зазвичай шкільний булінг і кібербулінг йдуть рука в руку, але не завжди. Це може набувати різних форм: поширення неправдивих чуток, зображень, що висміюють або знущаються, виключення з групи обміну повідомленнями, крадіжка пароля в соціальній мережі з метою образи інших, видаючи себе за іншу особу, тощо. Повторні агресивні дії не завжди здійснюються однією і тією ж особою; це можуть бути кілька різних осіб, які беруть участь у цьому, просто натискаючи «Like» або поширюючи образливу інформацію.

ЯКІ ОЗНАКИ ЦЬОГО?

Правда полягає в тому, що способи образи хлопчиків та дівчаток за допомогою Інтернету можуть бути настільки різноманітними, наскільки дозволяє уява. Той факт, що Інтернет є одночасно середовищем соціалізації та елементом, що перетинає інші контексти, дозволяє ширше розмаїття. Найпоширенішими ознаками кібербулінгу є:

- Флеймінг: надсилання образливих повідомлень на форум без будь-якої конструктивної мети.
- Навмисне повідомлення адміністраторам онлайн-сервісів, таких як Meta/Facebook. Соціальні мережі мають політику використання, яку необхідно прийняти під час реєстрації. Ця політика забороняє певні види поведінки, такі як образи або публікація інтимних зображень. Одночасно вони просять допомогу у спільноті користувачів у повідомленні про такі порушення, використовуючи для цього спеціальний канал



або форму. Користувачі можуть повідомляти про інших, імітуючи або створюючи ситуацію шахрайським способом, в якій порушуються умови використання, навіть домагаючись заборони або закриття профілю, про який було повідомлено.

- Переслідування та домагання за допомогою образливих та принизливих повідомлень, які можуть надсилатися до груп, що заохочують анонімність осіб, які ними користуються. Наприклад, групи або додатки WhatsApp, такі як ThisCrush (інтернет-сайт, де можна ділитися коментарями про думки чи почуття щодо іншої особи, використовуючи справжнє ім'я або анонімно).
- Крадіжка паролів з метою видати себе за іншу особу або завадити їй використовувати свою особу для образливих або компрометуючих дій перед іншими людьми.
- Сексуальне переслідування з єдиною метою – бути неприємним, наприклад, шляхом надсилання порнографічних зображень.
- Залякування за допомогою погроз. Вони можуть складатися зі слів, мемів або простого посилання на відео, де показано фізичне насильство.
- Приниження, створення сторінок з насмішками або поширення неправдивої інформації чи новин, які можуть змусити іншу особу або групи осіб повірити, що щось неправдиве є правдою, що шкодить репутації та дружнім стосункам.
- Розкриття конфіденційної або приватної інформації, як це часто буває у випадку гомосексуальних жертв, які, можливо, не бажали оприлюднювати свою сексуальну орієнтацію.
- Навмисне виключення когось з онлайн-активності, наприклад, не включаючи цю особу до групи миттєвих повідомлень у класі (наприклад, WhatsApp).

Для нас важливо знати, як можна виявити цю проблему у хлопчиків та дівчаток у шкільному середовищі:

- Прогули школи, наприклад, з недостатньо обґрунтованими пропусками.
- Зниження концентрації уваги.
- Раптові зміни настрою.
- Моменти смутку, апатії або байдужості.
- Миттєві спалахи агресивності.
- Відсутність друзів або соціальних стосунків.
- Мінімальне спілкування або ізоляція в класі.

ВІДМІННОСТІ МІЖ БУЛІНГОМ ТА КІБЕРБУЛІНГОМ

Щоб ефективно розпізнавати перші симптоми кібербулінгу та його фактори ризику, вчителі повинні знати різницю між різними видами кібербулінгу серед однолітків.

Незважаючи на те, що страждання жертви є загальним кінцевим результатом, існують деякі дуже важливі особливості кібербулінгу серед однолітків порівняно з традиційним булінгом.

- Жертва завжди знаходиться в зоні досяжності агресії, в будь-який час і в будь-якому місці. Навіть якщо вона не підключена до мережі, на її профіль у соціальних мережах можуть надходити образливі повідомлення. Це може відбуватися одночасно з нанесенням шкоди її ідентичності або цифровій репутації негативними коментарями на форумах, у групах обміну повідомленнями або під зображеннями в соціальних мережах.
- У випадках булінгу зазвичай простежується певна ієрархія ролей, де ключову роль відіграє ініціатор агресії. Водночас в онлайн-середовищі до агресивної поведінки може долучатися значно ширше коло людей. Інтернет створює можливість долучатися до цькування користувачам незалежно від місця їхнього перебування, віку чи належності до певної спільноти. Крім того, як і багато інших форм онлайн-взаємодії, такі дії можуть відбуватися спільно або колективно.
- Агресія сприймається більшою кількістю людей і триває довше. Однак вона менш помітна для родин та освітньої спільноти. Наприклад, створення та поширення фейкового профілю у Facebook, в якому видаєш себе за учня, що зазнає булінгу, і публікуєш образливі, неприємні або загрозливі фотографії, вимагає мінімум зусиль і має величезний вплив.
- Сприйняття заподіяної шкоди є меншим, оскільки страждання людини, яка зазнає переслідувань, часто не є безпосередньо помітними. Розвивати емпатію нелегко, коли між людьми є екрани, відстань і навіть час. Погроза, написана як жарт, може здатися її адресату в певний момент і в певному контексті найсуворішим вироком.
- Профілі агресорів і жертв дуже різноманітні. Немає чітких закономірностей. Будь-хто може заподіяти шкоду. Часто трапляються люди, які і самі страждали від кібербулінгу, і самі його чинили або навіть очолювали.

Ці різні характери є результатом диференціюючих факторів, які Інтернет пропонує як канал і контекст соціалізації для дітей.

ФАКТОРИ, ЩО СПРИЯЮТЬ КІБЕРБУЛІНГУ МІЖ ОДНОЛІТКАМИ

Інтернет та цифрове життя мають певні особливості, які сприяють легкому вчиненню насильства серед дітей. Набагато легше здійснювати кібербулінг, ніж його зупинити. Кібербулінг набуває дуже різних форм і, як правило, залишається безкарним, на відміну від інших видів протиправної поведінки. Наступні каталітичні фактори можна визначити як «привабливі» для вчинення кібербулінгу:

Анонімність (нерозкриття своєї особи), видавання себе за іншу особу (прикидання кимось іншим) та самозванство (прийняття вигаданої особи) в Інтернеті відкривають цілий ряд можливостей і дають більшу впевненість у безкарності.

- Незнання чинного законодавства. Ігноруючи той факт, що закон є однаковим як в Інтернеті, так і в реальному житті, багато хто легко втягується у вчинення серйозних злочинів, таких як погрози смертю.
- Миттєвість, якість, потужність та ціна доступу і виробництва онлайн-контенту, а також доступність і низька вартість пристроїв надають будь-якому потенційному кривднику цінний арсенал зарядженої зброї. Мем можна відредагувати і розповсюдити з будь-якого комп'ютера або мобільного телефону.
- Позитивне ставлення до технологічних досягнень у групі однолітків може спонукати деяких привернути до себе увагу, демонструючи свої навички шляхом знущань над однокласниками.
- Постійна поява нових додатків і сервісів, які створюють нові можливості для переслідування та додаткових превентивних заходів. З появою нових соціальних додатків можуть з'являтися нові форми булінгу.
- Складність доведення факту кіберзалежності, оскільки воно набуває мінливих і різноманітних форм, які дуже важко розслідувати і притягнути до кримінальної відповідальності. У такому мінливому середовищі важко встановити довгострокові стандартні протоколи для виявлення знущальників і отримання доказів їхніх дій.
- Інвестиції, зроблені в онлайн-ігри для створення віртуальних спільнот, без будь-якої турботи про збереження конфіденційності та гарної атмосфери співіснування. Це розважальні середовища, які в деяких випадках, здається, не мають внутрішніх структур відповідальності та регулювання.

- Відсутність особистого контакту з жертвою (іноді вони навіть не знайомі) або необхідність бути психічно чи фізично сильнішим. Це означає, що можливі комбінації профілів жертв і кривдників з часом стають дедалі різноманітнішими.
- Легке «об'єднання» хуліганів. В Інтернеті неважко знайти людей, готових боротися за реальну чи уявну справу, будь то їхня власна чи чужа, або просто бути частиною групи хуліганів.
- Неусвідомлення наслідків різних дій. Можливо, все почалося як жарт або через роздратування, але фотографія, на якій жертва висміюється, може поширитися ширше, ніж очікувалося. Це також може збігтися з делікатним моментом у настрої жертви (з іншими особистими проблемами, низькою самооцінкою тощо). Таким чином, хтось може заподіяти більше шкоди, ніж передбачалося або ніж уявлялося.
- Виправдання на кшталт «всі так роблять», «я не мав наміру» або «це був не тільки я». Це прості способи спробувати уникнути відповідальності.
- Прийняття ролі, за яку вони несуть відповідальність за свої дії. Коли хтось приймає на себе роль і представляє себе в Інтернеті як іншу людину, він може по-різному сприймати свою відповідальність і совість по обидва боки екрану.
- Зростаюче значення онлайн-життя. Це означає, що будь-які дії з кібербулінгу мають великий потенціал впливу і дуже мало можливостей або способів уникнути їх. Якщо в минулому підключення до Інтернету було чимось випадковим, то в майбутньому відключення від мережі стане все більш рідкісним явищем. Перебування в Інтернеті збільшує шанси страждати і зазнавати булінгу.

Коротко кажучи, на жаль, кібербулінг є легким, дешевим, завжди доступним і дуже часто залишається безкарним.

АКТУАЛЬНІСТЬ ЖИТТЄВИХ НАВИЧОК

У 1993 році відділ психічного здоров'я Всесвітньої організації охорони здоров'я (ВООЗ) започаткував міжнародну ініціативу з навчання життєвих навичок у школах.

Метою цієї ініціативи було поширення навчальних програм у всьому світі, спрямованих на розвиток набору навичок, які вважаються важливими для формування психосоціальних компетентностей дітей, зокрема соціальних, когнітивних та емоційно-регулятивних навичок. Освіта, заснована на розвитку життєвих навичок, зосереджується на наданні навчання навичкам, необхідним для подолання вимог і викликів повсякденного життя. Освіта, заснована на життєвих навичках, має на меті поліпшити здатність людей жити здоровішим і щасливішим життям, впливати на фактори, що визначають здоров'я та добробут, та брати активну участь у побудові більш справедливого, більш підтримуючого та рівноправного суспільства. Хоча існують різні способи класифікації цих навичок, ініціатива ВООЗ була широко визнана та прийнята як стандарт завдяки своїй великій гнучкості та застосовності. У ній можна виділити десять основних життєвих навичок:

- Самосвідомість.
- Емпатія.
- Асертивна комунікація.
- Міжособистісні стосунки.
- Прийняття рішень.
- Управління проблемами та конфліктами.
- Творче мислення.
- Критичне мислення.
- Управління емоціями та почуттями.
- Управління напругою та стресом.

Усі вони є необхідними, хоча їхня роль залежить від ситуації. З іншого боку, вони мають різний рівень актуальності в цифровому житті. У цьому контексті ми можемо заохочувати розвиток деяких із них у класі (особливо в разі кібербулінгу). Багато з них можуть слугувати протиотрутою від певних шкідливих форм поведінки.

ДЕЯКІ КЛЮЧОВІ НАВИЧКИ ДЛЯ КІБЕРСПІВІСНУВАННЯ

Кібербулінг ставить великі виклики перед усіма, хто до нього причетний: жертвою, агресором та свідком/очевидцем. Залежно від моменту та ролі в ситуації кібербулінгу, життєві навички можуть допомогти як запобігти йому, так і впоратися з ним. Серед них найважливішими життєвими навичками можуть бути:

- Емпатія: це дуже важливо, коли йдеться про міжособистісні стосунки. Якщо ми не відчуваємо, що вони страждають, ми не можемо співчувати. Екрани та відстань ускладнюють сприйняття шкоди.
- Самооцінка: низька самооцінка часто є типовою для агресорів, навіть якщо може здаватися інакше. Висока самооцінка зазвичай є навичкою, яку повинні розвивати ті, хто піддається булінгу.

- Критичне мислення: крім інших навичок і цінностей, які потрібно задіяти, першим кроком для виходу з ситуації кібербулінгу є припинення сприйняття його як «нормального». Денормалізація є ключовою для залучення сторонніх спостерігачів (свідків) до активних дій.
- Асертивність: Свідки повинні мати можливість відмовитися від участі в речах, які їм не до вподоби, навіть якщо це непопулярний вибір.

КІБЕРСПІВІСНУВАННЯ ЯК СВІДОМИЙ, ПОСТІЙНИЙ І КОЛЕКТИВНИЙ ВИКЛИК

Особливості Інтернету роблять агресію легшою та зручнішою як у класі, так і поза ним. З цієї причини необхідно щодня створювати атмосферу гармонійного співіснування серед усіх користувачів Інтернету. Ми повинні усвідомити це разом. Для цього ключовим є розуміння концепції відповідального цифрового громадянства. Це означає завжди зважати на інших людей в Інтернеті: навіть проактивно намагатися запобігати будь-яким конфліктам, які можуть призвести до булінгу. Нижче наведено десять порад для вчителів щодо поліпшення атмосфери кіберспівіснування серед дітей і, як наслідок, їхнього цифрового благополуччя.

ДЕСЯТЬ ПРАВИЛ ДЛЯ ПОЗИТИВНОГО ЦИФРОВОГО СПІВІСНУВАННЯ

1. **Користуйтеся Інтернетом етично та ввічливо: дотримуйтесь мережевого етикету.**

Дотримуйтесь мережевого етикету! Мережевий етикет — це набір рекомендацій, які допомагають нам підтримувати добрі стосунки в Інтернеті. Дотримання цих рекомендацій покращує цифрове співіснування.

2. **Уникайте використання виразів, які можуть образити інших людей у публічних місцях.**

Те, що говориться в Інтернеті, дуже часто поширюється несподівано і може бути неприємним або незручним для когось.

3. **Захищайте себе від шкідливого програмного забезпечення. Блокуйте свій смартфон і захищайте свої паролі.**

Важливо запобігати небажаному доступу до вашої інформації або інформації інших людей. Захист пристроїв і паролів запобігає крадіжці особистих даних.

4. **Пам'ятайте, що перебування по цей бік екрану не захищає вас.**

Нерозумно думати, що ви можете уникнути певних ситуацій, просто відключившись від мережі. Інтернет має дуже широкий охоплення.

5. **Захищайте свої особисті дані та приватність, щоб підвищити рівень захисту.**

Чим більше інформації ви маєте про людину, тим більша ймовірність заподіяння шкоди.

6. **Не робіть в Інтернеті того, чого ви не зробили б при особистій зустрічі.**

Іноді людина по той бік екрану є ближчою, ніж ви можете собі уявити. Мова, вік, інтереси та культура допомагають у цьому.

7. **Тримайтеся подалі від агресивних або незручних людей і будьте обережні з новими знайомими.**

В Інтернеті деякі люди просто прагнуть провокувати та завдавати шкоди. Важливо уникати їх, особливо у своїх соціальних мережах.

8. **Уникайте припущень. Ви можете помилятися.**

Образливі дії іноді бувають ненавмисними, неправильно витлумаченими або спрямованими на когось іншого. Вони також можуть приховувати навмисний обман.

9. **Ігноруйте провокації. Порахуйте до десяти і подумайте про щось інше, перш ніж відповідати.**

Відповідь на образливу поведінку не допомагає уникнути конфлікту і може призвести до кібербулінгу. Людина з поганими намірами та доступом до Інтернету може завдати серйозної шкоди.

10. **Якщо вас переслідують в Інтернеті, зверніться за допомогою до адміністратора сайту або служби.**

Багато онлайн-сервісів, таких як соціальні мережі та ігри, мають правила користування, які забороняють образливу поведінку своїх користувачів.

Профілактична робота

Кібербулінг – це, по суті, питання цінностей. Однак ці цінності можуть бути обумовлені або, у будь-якому випадку, інтенсивністю, з якою може проявлятися їх відсутність. Існує кілька напрямків дій, які, на додаток до розвитку життєвих навичок, можуть допомогти зменшити кібербулінг.

ЗАОХОЧЕННЯ ДО ЗАХИСТУ ПРИВАТНОСТІ ТА КІБЕРБЕЗПЕКИ

Приватність і кібербезпека йдуть рука в руку, а разом з ними – і безпека окремих осіб. Хлопчик або дівчинка, які дотримуються належних практик безпеки та приватного життя, будуть менш схильні до кібербулінгу, або ж цей кібербулінг буде менш інтенсивним і матиме менші наслідки.

РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ ПРО ПРАВОВІ МЕЖІ ТА ВІДПОВІДАЛЬНІСТЬ

Дуже важливо підвищувати обізнаність про те, що є поза законом, та про наслідки для тих, хто бере участь у таких діях.

Погрози, образи, розкриття таємниць та крадіжка особистих даних є діями, що підпадають під визначення кібербулінгу та караються законом. Дитина, яка усвідомлює цю ситуацію, може вирішити не брати участь у кібербулінгу або, якщо вона уже бере участь, припинити або пом'якшити свою поведінку. З іншого боку, якщо жертва усвідомлює, що закон на її боці, вона може зберегти докази або свідчення образливих дій і, за необхідності, вжити правових заходів.

ПРОСУВАННЯ КОНЦЕПЦІЇ ЦИФРОВОГО ГРОМАДЯНСТВА ТА МЕРЕЖЕВОЇ ЕТИКИ

Ми повинні донести до дітей, що Інтернет – це не просто щось, чим ми користуємося, а місце, де ми живемо та співищуємо. З цієї причини ми повинні відігравати активну роль у цьому новому контексті, де ми діємо як цифрові громадяни, беручи активну участь у здійсненні наших прав та обов'язків, що дозволяють нам насолоджуватися цим чудовим середовищем соціалізації. Інтернет – це те, що ми з нього



робимо, і саме тому ми повинні сприяти спільній відповідальності. У цьому контексті ми можемо включити поняття «нетикет», як сукупність правил, встановлених певною групою з метою поліпшення умов для насолоди та співіснування в конкретному цифровому контексті. Аналогічно, створення динаміки, в якій старші діти беруть на себе відповідальність за навчання молодших здоровому використанню та позитивному співіснуванню в Інтернеті, має надзвичайний ефект на атмосферу в школі. Cybermanagers, програма PantallasAmigas, була піонером у цій галузі і успішно працює з 2010 року.

ЗАКЛИК ДО ДІЇ ДЛЯ РІЗНИХ ТИПІВ АУДИТОРІЇ

Існують різні типи людей, яких зазвичай визначають як спостерігачів або свідків булінгу чи кібербулінгу. Проте є спосіб залучити їх усіх до вирішення проблеми: спонукати їх вийти з пасивності, перестати бути співучасниками булінгу. Наприклад, першим кроком може бути запрошення їх перестати бути спостерігачами; другим кроком може бути прояв підтримки жертви в приватному порядку; третім кроком, що вимагає більшої залученості, може бути прийняття активної та публічної позиції проти ситуації з онлайн-булінгом.

ДОДАТКОВА ЦІННІСТЬ ДЛЯ ГАРНОЇ АТМОСФЕРИ У ПРОСТОРАХ ДЛЯ ЦИФРОВИХ ВІДНОСИН

Рівень насильства в Інтернеті настільки високий, що йому необхідно протидіяти безпосередньо, щоб воно не стало нормою або не сприймалося як звичайна риса Інтернету. Необхідно підкреслювати цю різницю, і для цього немає нічого кращого, ніж висвітлювати позитивні аспекти доброї атмосфери в Інтернеті та основних цінностей, таких як повага і толерантність до різноманітності у всіх її проявах, шляхом підвищення обізнаності серед однолітків. Позитивне сприйняття доброї атмосфери співіснування, без сумніву, призводить до більшої відданості їй і до відмови від дій, що її руйнують.

Втручання. Що робити у випадку кібербулінгу?

Вжиття заходів у разі наявності доказів або виявлення ознак кібербулінгу може залежати від кількох факторів (шкільного та соціального контексту, ступеня і тривалості булінгу, особливостей учасників ситуації тощо). Навіть якщо органи управління освітою або заклад освіти мають визначені наказами та алгоритмами реагування процедури, у кожному випадку важливо діяти обережно, розсудливо та ухвалювати обґрунтовані рішення. Встановлення обставин ситуації та визначення відповідних заходів реагування можуть бути складним процесом, що потребує ретельного аналізу фактів. Водночас слід враховувати, що особи, які вчиняють агресивні дії, також можуть потребувати допомоги. Під час реагування необхідно дотримуватися прав усіх учасників ситуації, зокрема права на приватність та принципу презумпції невинуватості.

ДЕСЯТЬ ПРАВИЛ ДЛЯ ЖЕРТВ КІБЕРБУЛІНГУ

Всі жертви кібербулінгу знаходяться в одному кліщі від своїх кривдників. Ключовим є вжиття негайних заходів у відповідний спосіб. Іноді ініціатива виходить від самої жертви, наприклад, тому що вона не може знайти допомогу або не хоче про неї просити. Незалежно від того, хто ініціює дії, ключовим є її співпраця. Тому, хоча вчителі повинні намагатися надати безпосередню допомогу, вони також повинні дати жертві можливість допомогти собі самостійно.



Ці десять правил можуть бути процедурними рекомендаціями, які слід донести до дітей, щоб обмежити або зупинити шкоду:

1. Попросіть про допомогу. Зверніться до батька, матері або, якщо це неможливо, до дорослого, якому довіряєте. Переконайтеся, що ця людина знає і розуміє ці вказівки, щоб ви могли діяти в одному напрямку і щоб вона не збільшила шкоду, намагаючись захистити вас.

2. Ніколи не реагуйте на провокації або образи. Це ніяк не допоможе вам. Навпаки, це може підбадьорити і дати перевагу тим, хто вас знущується. Зберігайте спокій і ніколи не дійте імпульсивно або перебільшено.

3. Не робіть припущень. Ні обставини, ні люди, які беруть участь у ситуації, можуть бути не такими, якими здаються. Залишайте місце для розумних сумнівів, оскільки дії на основі неправильних припущень можуть погіршити ситуацію та створити нові проблеми.

4. Намагайтеся якомога більше уникати місць, де вас цькують, доки ситуація не проясниться. Якщо це відбувається в соціальних мережах або онлайн-спільнотах, вам це не складе труднощів.

5. Чим більше інші знають про вас, тим вразливішими ви є і тим різноманітнішою та інтенсивнішою може бути шкода, яку вони можуть вам заподіяти. Чи можете ви уявити собі брехню, яка висміює вас, засновану на реальних приватних даних і легко помітну? Що сталося б, якби хтось, видаючи себе за вас, ображав ваших друзів? Тому настав час закрити двері до вашого приватного життя в Інтернеті для людей, яким ви не довіряєте повністю. Ви можете це зробити таким чином:

а) Уникати зловмисників. Для цього ви повинні виконати наступні кроки в точності в зазначеному порядку:

а.1. Проведіть ретельну перевірку своїх пристроїв, щоб переконатися, що на них немає шкідливого програмного забезпечення (троянів, зловмисного програмного забезпечення...), яке

може дати перевагу людині, яка вас переслідує. Це важливо.

а.2. Змініть паролі до онлайн-сервісів, якими ви користуєтеся, але ніколи не робіть цього, не виконавши попередній крок. Пам'ятайте, що вони повинні бути складними для вгадування та поєднувати цифри та літери.

б) Очистіть список контактів. Перегляньте та скоротіть список контактів, які ви додали до своїх соціальних мереж або інших онлайн-соціальних середовищ.

с) Переналаштуйте параметри конфіденційності ваших соціальних мереж або подібних сайтів, якими ви користуєтеся, та посилюйте їх. Переконайтеся, що ви повністю розумієте, як працюють ці опції та які вони мають наслідки.

д) Перевірте, що люди пишуть про вас у соціальних мережах. Шукайте інформацію про вас, опубліковану іншими людьми, і спробуйте її видалити, якщо вважаєте, що вона може бути використана проти вас.

е) Переглядайте інформацію, яку ви публікуєте, перевіряйте, хто може її бачити, та за потреби обмежуйте її доступність.

ф) Повідомте своїм контактам, що ви не хочете, щоб вони поширювали вашу інформацію або фотографії в колективних групах.

г) Здійснюйте своє право на захист персональних даних. Ви вирішуєте, як вони можуть бути використані, включаючи ваше зображення.

6. Завжди зберігайте докази знущань, незалежно від їхньої форми. Це може бути вам дуже корисно. Спробуйте також дізнатися або встановити особу авторів, але не порушуючи прав інших осіб.

7. Скажіть своїм кривдникам, що їхні дії вас турбують, і попросіть їх припинити, не проявляючи агресії та не погрожуючи їм. Пам'ятайте, що ви не повинні сприймати факти або людей у вашому спілкуванні як належне, тому будьте дуже обережні у своїх діях, не вказуючи пальцем на людей привселюдно, але водночас намагаючись переконатися, що особа або особи, яких це стосується, зрозуміли ваше повідомлення.

8. Спробуйте дати їм зрозуміти, що їхні дії караються законом, якщо вони продовжуватимуть свої переслідування. Ви можете запропонувати їм перевірити в Інтернеті новини про подібні випадки або вироки, щоб вони могли переконатися в цьому самі.

9. Дайте чітко зрозуміти, що ви готові повідомити про це, якщо, незважаючи на ваше попереднє попередження, вони продовжують знущатися. Заявіть, що ви зібрали достатньо доказів з самого початку і знаєте, як і куди про це повідомити. Ви повинні заявити, що, якщо кіберзнущання продовжуватимуться, у вас не буде іншого вибору, як звернутися до поліції.

10. Якщо на цьому етапі знущання все ще тривають, вживіть наступних заходів: повідомляйте про випадки кібернасильства у поліцію за телефоном 102 або подайте електронне звернення до кіберполіції за посиланням <https://ticket.cyberpolice.gov.ua>.

Щоб реалізувати ці рекомендації на практиці, важливо врахувати наступні моменти:

Хоча це в основному рекомендації, що застосовуються до дорослих і поза шкільним контекстом, повідомлення слід адаптувати, коли воно передається дітям.

- Кожен випадок і кожна людина є унікальними. Тому ці поради призначені для допомоги, повністю або частково, в найпоширеніших випадках.
- Порядок дій є важливим. Однак серйозність подій у деяких випадках може вимагати прискорення виконання певних кроків, скорочення часу між ними або їх повного пропускання.
- У крайніх випадках слід негайно звернутися за допомогою до поліції.

Нарешті, стосовно оточення жертви, слід дотримуватися трьох основних принципів:

1. Захистіть і підтримайте постраждалу особу. Це найважливіше. Вона має відчувати підтримку, розуміння та супровід.
2. Відмовтеся від будь-яких припущень, оскільки обман є одним із найпоширеніших інструментів, якими користуються кривдники, а в Інтернеті досить часто трапляється видавання себе за іншу особу.
3. Дійте спокійно та виважено, співпрацюючи з усіма залученими сторонами. Посилення вже наявного насильства або його поширення не сприятиме швидкому розв'язанню ситуації.



Грумінг

Вступ

Сексуальне домагання до хлопчиків і дівчаток є дедалі більшою проблемою в Інтернеті. Поява Інтернету призвела до зростання цього виду ризику для дітей з різних причин, зокрема таких:

Педофіли та особи, які вчиняють розбещення дітей, більше не є ізольованими особами, які ховаються. Вони можуть спілкуватися в Інтернеті з подібними до себе людьми й фактично знаходити онлайн-простори, які безкарно пропагують «любов до дітей». Це робить їх сильнішими, оскільки зменшує будь-які потенційні почуття провини, а також надає їм підтримку завдяки знаходженню спільноти однодумців.

Зображення сексуального насильства та експлуатації дітей (які юридично і, можливо, справедливо називаються дитячою порнографією) є частиною незаконного бізнесу, що розвивається завдяки Інтернету, і, як такі, приносять великі гроші від відвідування чатів та обміну файлами.

Особливості Даркнету (Dark Web) можуть сприяти безкарності цього виду кіберзлочинності, оскільки

робить її майже невиявленою. Згідно з дослідженням Університету Портсмута, 80% трафіку, що генерується в цьому шарі Інтернету, пов'язаний з поширенням інтимних зображень та сексуальним насильством над дітьми.

У цьому випадку дисбаланс сил між жертвою та агресором ще більше посилюється. Хижакі можуть охопити більшу кількість жертв будь-якого віку та в будь-якій країні, навіть одночасно, тому можливості запобігати та переслідувати ці злочини дуже обмежені.

Сьогодні суспільство стикається із серйозним викликом, до вирішення якого вчителі мають можливість зробити ефективний внесок. Кібербулінг може призвести до шкідливої поведінки, включаючи самогубство. Незважаючи на це, саме цей вид насильства над неповнолітніми зріс найбільше і, не доходячи до крайніх ситуацій, може бути пов'язаний із сексуальним насильством, експлуатацією та торгівлею людьми, а в будь-якому випадку також залишає глибокий слід у жертв.

Пам'ятайте

- Грумінг становить серйозну загрозу для сексуального здоров'я та особистої цілісності дітей. Оскільки їхнє цифрове життя пов'язане з дедалі більш раннім віком, вони опиняються в межах досяжності сексуальних хижаків з усього світу, щодо яких вони знаходяться в явно невідповідному становищі через вік, досвід та технологічні навички.
- Це більше стосується дівчат, ніж хлопців. В екстремальних випадках це може призвести до фізичних зустрічей з агресором, викрадення, зґвалтування, сексуальної експлуатації або торгівлі людьми.
- Канали та контексти, що дозволяють постійне, безперервне та приватне спілкування без суворого контролю ідентичності, є найбільш сприятливими для такого виду переслідування: соціальні мережі, програми для обміну миттєвими повідомленнями, багатокористувацькі онлайн-ігри тощо.
- Найскладнішим завданням у боротьбі з сексуальним кібербулінгом дітей, окрім профілактики та раннього виявлення, безсумнівно, є створення умов, за яких жертви можуть звернутися по допомогу. Для цього сім'ї, суспільство та установи повинні працювати пліч-о-пліч.

Інтернет-грумінг: що це таке і як це відбувається?

Грумінг — це стратегія сексуального кіберпереслідування, що здійснюється дорослим щодо неповнолітнього. Сексуальний хижак, завоювавши довіру жертви за допомогою емпатії, уваги або лестощів, прагне отримати від дитини сексуальні вигоди (зображення, відео або навіть особисті зустрічі), зазвичай використовуючи погрози та шантаж. Це також відомо як «грумінг дітей», «інтернет-грумінг» або «сексуальне кіберпереслідування неповнолітніх».

Грумер часто використовує соціальні мережі, чати, онлайн-ігри або форуми, щоб зв'язатися зі своїми жертвами та подружитися з ними. Він або вона отримує їхню увагу, використовуючи

привабливий профіль, який робить їх надійними, демонструє ті самі інтереси (вподобання) та емоції в їхніх розмовах і використовує ті самі вирази, мову та смайлики, що й діти, щоб завоювати симпатію своїх жертв. Вони зображують себе як ідеальних дівчат, хлопців або друзів.

Однак існують певні складності у використанні терміну «грумінг». Наприклад, виникає плутанина між грумінгом і кібербулінгом. Обидва поняття мають певну схожість у своїх цілях і наслідках. Проте сексуальний кібербулінг є видом онлайн-насильства, який не передбачає встановлення дружнього контакту з неповнолітніми, а здійснюється прямо і примусово: іноді таку поведінку також називають

«грумінгом». Подібна ситуація спостерігається і щодо сексторції, яка зазвичай є одним із фінальних етапів грумінгу. У цьому сенсі термін «сексторція» також нерідко вживається замість «грумінгу».

ХТО Є ЖЕРТВАМИ ГРУМІНГУ?

Жертвою може стати будь-яка особа віком до 18 років. Однак дівчата стають жертвами частіше, ніж хлопці. Кіберхижаки розвинули свою техніку і вдосконалюють її з кожним новим нападом. Першим кроком зазвичай є вивчення «жертви» та факторів її вразливості. Від цього моменту ступінь складності або опору, який чинить жертва, а також поріг ризику, на який може піти сексуальний хижак, визначатимуть, чи буде стратегія грумінгу успішною. На жаль, відстань грає на користь злочинців, оскільки сексуальне насильство над неповнолітніми може здійснюватися з іншої країни або континенту, що дуже ускладнює активацію правових механізмів для розслідування та притягнення до відповідальності.

УМОВИ, НЕОБХІДНІ ДЛЯ ГРУМІНГУ

Є два ключові аспекти або моменти в грумінгу:

- **Хижак отримує контроль над ситуацією**, здобуваючи матеріал, який може використати для шантажу жертви або незаконного впливу на її волю: отримання інтимного зображення жертви, захоплення її профілю в соціальній мережі, дізнання про таємницю, яку не можна розголошувати, тощо. Іноді саме дитина добровільно передає контроль над таким матеріалом. В інших випадках засоби контролю здобуваються шляхом примусу або обману, без можливості для жертви цього запобігти.

- **Нездатність жертви звернутися за допомогою та підтримкою**. Це зумовлено двома факторами. По-перше, сильним тиском, який може чинити зловмисник за допомогою маніпуляцій та погроз.

Як поводитися у випадку грумінгу?

У разі виявлення серед дітей потенційного випадку грумінгу найважливішим завданням є забезпечити припинення насильства або його наслідків і не допустити їх продовження, надаючи підтримку постраждалій особі.

Ситуації сексуальних домагань рідко завершуються самі собою. Булінг зазвичай має повторюваний характер. Для того щоб сприяти припиненню грумінгу, необхідно поінформувати сім'ю, аби вони могли ефективно співпрацювати з відповідними органами влади, зокрема з поліцією. Вкрай важливо зберігати пильність і прагнути довести ситуацію до

По-друге, відчуттям жертви, що вона вчинила щось неналежне або непристойне.

Без однієї з цих двох ситуацій віктимізація може не відбутися.

Елементом, який традиційно сприяє догляду за зовнішністю, є камера на комп'ютерах і мобільних телефонах. Хоча очевидно, що існує багато інших засобів створення та надсилання зображення іншій особі, доступність, простота та готовність, з якою це можна зробити за допомогою будь-якої доступної камери, є визначальним фактором. Хижаки намагаються змусити свою жертву показати, в нібито приватному контексті, компрометуюче зображення, яке вони зможуть зафіксувати, а потім використовувати для шантажу жертви за допомогою сексторції.

ФАКТОРИ РИЗИКУ, ЯКИХ СЛІД УНИКАТИ

З огляду на те, як розвивається ця все більш поширена форма віктимізації, можна виділити чотири конкретні обставини, що підвищують ризик грумінгу:

- Низька самооцінка змушує жертв більше цінувати компліменти та нові дружні стосунки, прагнути подальшого схвалення, не бажаючи не виправдати очікування або прохання цієї людини.
- Надмірне проведення часу в Інтернеті може призвести до знайомства з невідповідними людьми або місцями.
- Ризикована або «непристойна» поведінка, яка може бути використана іншими для шантажу.
- Відсутність єдності та довіри в сім'ї часто означає відсутність належного нагляду та додаткові труднощі для жертви у пошуку допомоги.

повного врегулювання. Саме тому, якщо учня ідентифіковано як такого, що потенційно зазнає грумінгу, сім'ю необхідно поінформувати та надати їй такі рекомендації:

1. Оцініть, які правопорушення міг скоїти булер і які з них можна довести. Можливо, не вдасться



довести, що булер має певні зображення чи інформацію або що він чи вона оприлюднили їх. Також може бути неможливо довести, що ці зображення були отримані під примусом чи обманом, або навіть що були отримані погрози. Тому доцільно знати, які правопорушення скоїв або скоює хижак, оскільки це дає змогу вжити правових заходів.

2. Пошук і збір доказів злочинної діяльності: скріншоти, розмови, повідомлення тощо, все, що може слугувати доказом дій зловмисника або надати підказки про його місцезнаходження чи методи, буде дуже корисним як для розслідування, так і для збору доказів. При дотриманні цього шляху загальним правилом має бути постійне дотримання закону.

3. Подання скарги. Про інцидент слід повідомити в поліцію, надавши відповідний аналіз ситуації та

будь-які докази, які можуть допомогти в розслідуванні, незалежно від того, чи продовжувалося переслідування. Слід мати на увазі, що, як правило, кіберзлочинці мають десятки жертв одночасно. Їхню діяльність обов'язково необхідно розслідувати та притягнути винних до відповідальності, щоб вони не могли продовжувати свою ганебну діяльність.

Кожен випадок є особливим, і підхід до нього також повинен бути особливим. За певних обставин може бути доцільним обережно слідувати за переслідувачем, щоб ідентифікувати його або зібрати докази. В інших випадках найрозумнішим варіантом може бути негайне звернення до поліції. Зверніть увагу, що все вищезазначене є рекомендаціями, які можуть бути ефективними в більшості випадків, коли поліція надає свою допомогу.

Десять порад щодо боротьби з грумінгом

Нижче наведено десять профілактичних рекомендацій щодо запобігання сексуальному кібербулінгу, якими вчителі можуть поділитися з учнями:

1. Не довіряйте зовнішньому вигляду.

Легко піддатися першому враженню. Прикидатися кимось іншим або мати спільних друзів - це звичайний вид обману.

2. Перевіряйте особу своїх нових контактів.

Якщо ви збираєтеся додати когось у нові контакти, спочатку перевірте його особу.

3. Захищайте свою особисту інформацію та секрети.

Ваші особисті речі, ваші секрети, те, про що ви не хочете, щоб хтось знав, - це скарб, який потрібно захищати.

4. Якщо хтось змушує вас почуватися погано, припиніть будь-який контакт.

Коли хтось змушує вас почуватися некомфортно, ображає вас або тисне на вас, припиніть будь-який контакт.

5. Попросіть про допомогу, якщо хтось вам погрожує або шантажує вас.

Якщо хтось погрожує вам або намагається шантажувати вас, попросіть про допомогу дорослого, якому ви довіряєте.

6. Захищайте свою кібербезпеку.

Ваша особиста безпека залежить від безпеки ваших підключених пристроїв (мобільного телефону, планшета, комп'ютера тощо).

7. Захищайте свою приватність.

Чим більше інші знають про вас, тим більшої шкоди вам можуть завдати. Подбайте про себе, підвищивши рівень своєї приватності.

8. Будьте обережні з гарними словами від поганих людей.

Якщо хтось намагався завдати вам шкоди, він не заслуговує на вашу довіру. Обіцянки чи «угоди» не мають жодної цінності.

9. Пам'ятайте, що ви не винні.

Навіть якщо ви почуваетесь погано або зробили щось, чого не слід було робити, не ховайтеся і попросіть про допомогу.

10. Завжди йдіть на побачення в супроводі дорослого.

Якщо ви йдете на побачення з кимось, з ким ви познайомилися в Інтернеті, завжди зустрічайтеся в громадському місці і в супроводі дорослого.



Секстинг

Вступ

Практика секстингу з використанням інтимних зображень існує вже понад десять років. За ці десять років вона перетворилася з незначної проблеми на відносно поширену практику, що здійснюється різними способами. Слід зазначити, що, незалежно від етичних або юридичних питань, які можуть виникнути стосовно неповнолітніх, секстинг сам по собі не травмує. Це дія, яка може спричинити серйозні проблеми, іноді через помилку, а частіше через злі наміри. Тому це ризикована практика. Секстинг також поширений серед дітей, тому його необхідно обговорювати в класі.

ЩО ТАКЕ СЕКСТИНГ?

Секстинг - це створення, надсилання або обмін власними інтимними фотографіями, відео чи текстовими повідомленнями сексуального або еротичного змісту за допомогою інформаційно-комунікаційних технологій (мобільних телефонів, соціальних мереж, месенджерів тощо). Основний ризик такої поведінки полягає в тому, що передані матеріали можуть бути збережені, скопійовані або поширені без згоди особи, зображеної на них. У разі потрапляння до третіх осіб такі матеріали можуть використовуватися для психологічного тиску, шантажу, приниження або інших форм онлайн-насилення. У правовому полі України важливо чітко розмежовувати добровільний обмін інтимними матеріалами між повнолітніми особами та дії, що можуть містити ознаки кримінального правопорушення. Зокрема, надсилання, отримання, зберігання або поширення матеріалів сексуального характеру із зображенням неповнолітніх підпадає під дію Кримінального кодексу України, зокрема статей 301 (виготовлення, збут і розповсюдження порнографічних предметів) та 301-1 (дитяча порнографія). Крім того, встановлення контакту з дитиною з метою отримання інтимних матеріалів або вчинення інших дій сексуального характеру може кваліфікуватися за статтею 156-1 Кримінального

кодексу України (домагання дитини для сексуальних цілей). У таких випадках дитина розглядається як потерпіла сторона та потребує захисту і підтримки.

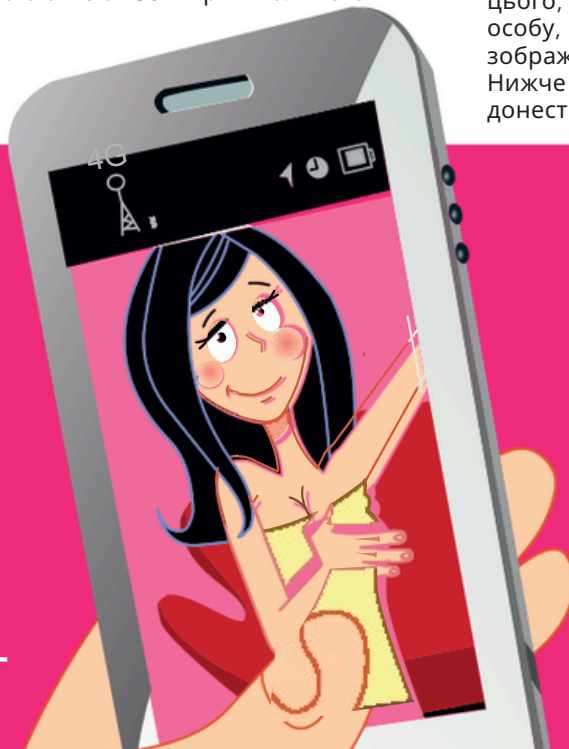
ЯКІ МОЖЛИВІ РИЗИКИ ІСНУЮТЬ ДЛЯ ТИХ, ХТО ЗАЙМАЄТЬСЯ СЕКСТИНГОМ?

Секстинг є ризикованою практикою. Це пов'язано з тим, що існування таких інтимних зображень може стати проблемою для людей, які на них зображені. Вони можуть перестати бути приватними, якщо одержувач поділиться ними або опублікує їх без дозволу, або якщо вони будуть загублені, вкрадені чи надіслані помилково. Якщо вони будуть поширені, крім порушення права на власний імідж та приватність, ви можете стати жертвою кібербулінгу. Більше того, ви також можете стати жертвою сексторції, якщо особа, яка володіє зображеннями, вимагає грошей або ставить інші вимоги в обмін на те, що не оприлюднить їх. У будь-якому випадку, необхідно враховувати закони щодо створення, володіння, розповсюдження та комерціалізації сексуального контенту дітей.

До цієї категорії також можна віднести так звану «порнопомсту» (revenge porn), відому також як «мстиве» або «помстиве» порно. Такі дії стають дедалі поширенішими. Вони є формою порушення приватності та інтимності, а також різновидом гендерно-зумовленого кібернасилення. Суть цієї практики полягає в «покаранні» партнера - нібито з помсти або зі злості - шляхом публікації зображень сексуального характеру, на яких його зображено. Коли ситуація кібербулінгу щодо жертви, зображеної на матеріалах, не відбувається в обмеженому і близькому середовищі, а має масовий характер, ми можемо говорити про «цифрове лінчування», навіть якщо його вплив є незначним.

Важливо не звинувачувати особу, яка стала жертвою секстингу, у шкоді, заподіяній в результаті цього, а перекласти повну відповідальність на особу, яка вчинила неналежні дії з приватними зображеннями інших осіб.

Нижче наведено кілька ключових ідей, які слід донести до дітей.



Пам'ятайте

- Секстинг - це ризикована практика. Якщо ви займаєтесь цим, ви можете серйозно постраждати в результаті неправомірних дій інших людей або навіть випадково чи через неосторожність.
- Ви повинні прийняти обдумане рішення щодо секстингу, без будь-якого тиску, і бути поінформованими про шкоду, яку ви можете зазнати або заподіяти.
- Будь-яке зображення або відео, яке переглядається на екрані, може бути збережене і поширене назавжди.
- Ні за яких обставин ніхто не має права поширювати інтимні зображення, навіть якщо вони були зроблені з вашої згоди.
- Якщо ви отримали інтимні зображення іншої людини, поведіться з ними з повагою і видаліть їх. Якщо ви поширите їх, крім заподіяння шкоди, ви можете вчинити серйозний злочин.

Запобігання необдуманому, неусвідомленому або здійсненому під тиском секстингу

Секстинг може мати кілька негативних наслідків. Тому ті, хто вирішив займатися цим, повинні робити це з власної волі, без будь-якого тиску з боку однокласників, партнерів або соціальних причин. Крім того, це має бути обґрунтоване рішення, прийняте з достатнім розумінням потенційних ризиків. Нарешті, оскільки це важливе питання, до нього слід підходити обдуманно, а не поспішно. Запрошення до роздумів про причини, що свідчать проти секстингу, є необхідною протиповагою, яку необхідно чітко і явно донести. Це не є ні нав'язуванням, ні заборонаю.

ПОДУМАЙТЕ, ПЕРЕД ТИМ ЯК ЗРОБИТИ СЕКСТИНГ. 10 ПРИЧИН НЕ РОБИТИ СЕКСТИНГ. ВИ ВИРІШУЄТЕ!

- 1. У цьому задіяна інша людина, від якої ви тепер залежите.**
Це не залежить від вас. Хтось інший може приймати рішення, які можуть вплинути на вас.
- 2. Люди та стосунки змінюються.**
Певні ситуації в житті змінюють наші почуття, і іноді найкращі друзі стають найбільшими ворогами.
- 3. Захист цифрової інформації є складним завданням.**
Дуже важко гарантувати повну безпеку.
- 4. Розповсюдження цифрової інформації неможливо контролювати.**
Всі зображення, що з'являються на екрані, втрачаються назавжди.
- 5. Зображення може містити багато інформації.**
Акcesуари, татування, пірсинг тощо. Номер мобільного телефону, пов'язаний із зображенням, або особа, яка має ваше фото, можуть розкрити вашу особу.
- 6. Існують закони, які карають дії, пов'язані з секстингом.**
Будьте особливо обережні, якщо на цих зображеннях є особи віком до 18 років.
- 7. Сексторція відбувається, якщо зображення секстингу потрапляє до рук шантажистів.**
Секстинг-зображення в неправильних руках створюють ризик сексторції.
- 8. Інтернет є швидким і потужним.**
Секстинг-зображення можуть опинитися в Інтернеті, найпотужнішому каналі поширення інформації, який коли-небудь існував.
- 9. Соціальні мережі надають інформацію людям, які знаходяться поруч з вами.**
Інтернет і соціальні мережі допомагають вам зустріти людей, з якими у вас можуть бути спільні інтереси.
- 10. Існує серйозний ризик кібербулінгу, якщо сексуальні зображення стануть публічними в Інтернеті.**
Деяким людям, здається, подобається завдавати шкоди. Для них ви будете винними, і вони зроблять вас своїми жертвами.

10 правил захисту приватного життя

Діти іноді можуть опинитися в ситуації, коли хтось пропонує обмінятися особистими або інтимними матеріалами. Найбезпечніша стратегія - взагалі не створювати і не ділитися інтимним контентом. Однак важливо знати правила, які допоможуть уникнути ризиків тиску, шантажу, поширення особистої інформації та інших форм цифрової небезпеки:

1. Будьте свідомі ризиків. Завжди пам'ятайте, що будь-який цифровий матеріал може бути збережений, пересланий або використаний проти вас - навіть якщо вам обцяють конфіденційність.
2. Не робіть нічого під тиском. Якщо ви відчуваєте примус, погрози, емоційне маніпулювання або терміновість, це вже небезпечна ситуація. Ви маєте повне право сказати «ні».
3. Поважайте особисті кордони. Ваша приватність має значення. Якщо хтось пропонує обмінятися особистими матеріалами, це не означає, що ви повинні погодитися.
4. Технологічна безпека. Переконайтеся, що ваші пристрої захищені - використовуйте антивірусне програмне забезпечення, регулярно оновлюйте систему та не встановлюйте підозрілі програми.
5. Не створюйте контент, який може зашкодити вам у майбутньому. Будь-яка фотографія або відео, навіть ті, що призначені «тільки для вас», можуть потрапити до рук інших людей.
6. Захист особистих даних. Не діліться інформацією, яка може полегшити вашу ідентифікацію або визначення вашого місцезнаходження (геолокація, документи, деталі вашого оточення, інтер'єри приміщень тощо).
7. Пам'ятайте про правила кібербезпеки. Майте на увазі, що «безпечні» месенджери не гарантують абсолютної безпеки. Ніщо в Інтернеті не є на 100% приватним.
8. Уникайте публічних мереж. Не передавайте особисту інформацію через відкриті мережі Wi-Fi - вони часто є небезпечними для даних.
9. Думайте наперед. Якщо хтось просить вас надіслати щось особисте, запитайте себе: «Чи хотів би я, щоб хтось інший це побачив?» Якщо відповідь «ні», відмова є абсолютно нормальною.
10. Контролюйте, що зберігається на ваших пристроях. Видаляйте непотрібні або надто особисті матеріали, захищайте хмарне сховище, використовуйте паролі та двофакторну автентифікацію.

Що робити у разі виникнення проблеми?

Незважаючи на запобіжні заходи, інтимні зображення, передані в цифровому середовищі, можуть потрапити до осіб, для яких вони спочатку не були призначені. Причини цього можуть бути різними: від несанкціонованого поширення отримувачем до втрати контролю над цифровими даними. У таких випадках наслідки для постраждалої особи можуть бути подібними незалежно від обставин поширення матеріалів. Подібні ситуації іноді трапляються і серед дітей. У таких випадках ключову роль у підтримці дитини відіграють батьки або інші законні представники. Саме вони мають допомогти дитині оцінити ситуацію, надати емоційну підтримку та, за потреби, звернутися до відповідних фахівців або компетентних органів. Водночас реагування має здійснюватися з дотриманням принципів конфіденційності та поваги до приватного життя дитини. Важливим напрямом профілактики є також підвищення обізнаності дітей і дорослих щодо ризиків поширення інтимних матеріалів у цифровому середовищі та можливих правових наслідків їх зберігання чи розповсюдження, особливо якщо йдеться про зображення за участю неповнолітніх. У разі виникнення подібних ситуацій важливо діяти виважено та з максимальною дискретністю щодо постраждалої особи.

- Спробуйте з'ясувати, хто і як отримав або поширив інтимні зображення вашої дитини поза межами приватного середовища.
- За можливості спробуйте заблокувати або видалити такі зображення з цифрових платформ, пам'ятаючи, що результати можуть бути обмеженими.
- Підвищуйте власну обізнаність щодо серйозних правових наслідків зберігання або розповсюдження інтимних зображень через цифрові канали, особливо якщо це стосується дітей, та навчайте дитину основам цифрової безпеки та приватності.
- Збирайте докази та звертайтеся із відповідною скаргю до компетентних органів





Сексторція

Вступ

Сексторція є одним із видів кіберзлочинів, що найшвидше поширюються, через низку взаємопов'язаних причин. З одного боку, щодня зростає поширення самостійно створених приватних зображень. З іншого боку, зростає можливість їх отримання силовим шляхом (за допомогою шкідливого програмного забезпечення) або обманом. Водночас загроза сексторції є настільки серйозною, легкою у здійсненні та складною у припиненні, що будь-який злочинець може вимагати майже будь-яку суму грошей або змусити жертву зробити будь-що.

ЩО ТАКЕ СЕКСТОРЦІЯ

Сексторція полягає у шантажуванні жертви з метою змусити її вчинити певну дію або заплатити під загрозою оприлюднення або поширення приватних зображень. Типи жертв, мотивація та кінцева шкода, що завдається, можуть значно відрізнятись.

ЯКІ НАСЛІДКИ?

Жертва може зазнати різних наслідків, серед яких:

- Найкращий сценарій: шантаж не приймається, і кіберзлочинець не виконує свою погрозу.
- Найгірший сценарій: шантажист виконує свою погрозу і публікує приватні зображення іншої особи (жертви). Для жертв це є порушенням їхньої приватності, честі та особистого іміджу. Крім того, може бути завдано побічної шкоди іншим особистим справам або людям, яких торкнулося поширення цих зображень.

Варто зазначити, що наслідки можуть бути різноманітними, залежно від форми, частоти та регулярності сексторції. Широкий спектр наслідків дуже часто є частиною стратегії кіберзлочинців, кінцевою метою яких може бути грумінг або сексуальне кіберзловживання щодо дітей. Секстинг також може становити або бути формою ґендерно-зумовленого кібернасильства.

Пам'ятайте

- Сексторція є одним із найпоширеніших та найдинамічніше зростаючих видів кіберзлочинів.
- Поширення секстингу та інших сексуалізованих практик в Інтернеті, що нормалізують фіксацію інтимних дій, розширення технологічних можливостей запису й поширення зображень, а також вразливість пристроїв до кіберзагроз сприяють поширенню сексторції.
- Наслідки сексторції для жертв можуть бути надзвичайно серйозними на емоційному рівні, але також можуть мати фінансові наслідки. Навіть після того, як

шантажист припинив свої дії, наслідки можуть тривати. Більше того, не можна бути впевненим, що він або вона не спробують знову шантажувати жертву, оскільки їх неможливо «роззброїти».

- Усі ми можемо допомогти зупинити несанкціоноване поширення приватних зображень і, отже, їхні негативні наслідки. Захист інтимності інших людей, ігнорування та нерозповсюдження приватних зображень інших людей є нашою відповідальністю.



Як запобігти сексторції

Для запобігання сексторції та її негативних наслідків слід розглянути три напрямки дій, які необхідно вжити на різних рівнях. Перший напрямок має бути зосереджений на захисті зображень. Другий має бути спрямований на усунення основної мотивації шантажистів. Третій має бути зосереджений на освіті та підвищенні соціальної обізнаності.

ЯК ЗАПОБІГТИ ТОМУ, ЩОБ ЗОБРАЖЕННЯ ПОТРАПИЛО В «НЕВІДПОВІДНІ» РУКИ

Зображення може бути більш-менш відвертим або компрометуючим (незалежно від того, чи це фотографія чи відео) і походити з різних джерел:

- добровільно передане самою особою, зображеною на ньому;
- отримане іншими людьми або знайдене випадково;
- вилучене з пристрою, який було втрачено або передано на ремонт;
- зламане або викрадене шляхом несанкціонованого доступу до системи;
- зафіксоване за взаємною згодою або приховано;
- отримане шляхом віддаленої активації камери.

Іноді це не справжнє зображення, а надзвичайно схоже підроблене, яке може бути фотомонтажем або навіть підробленим відео («діпфейк»).

Заходи щодо захисту приватного життя та кібербезпеки мають фундаментальне значення у боротьбі з сексторцією, хоча вони не завжди можуть запобігти появі деяких із зазначених вище джерел зображень.

РОЗУМІННЯ МОТИВІВ СЕКТОРЦІЇ

Три найпоширеніші цілі сексторції:

1. Сексуальне задоволення або домінування:

а. грумінг, коли зловживання полягає у вимаганні додаткових зображень або сексуальної зустрічі;

б. ґендерно-зумовлене сексуальне кібернасильство, що негативно впливає на сексуальну свободу партнера або колишнього партнера.

2. Фінансова вигода - коли жертву змушують передати гроші або інший вид майна чи послуги.

3. Поведінкове зумовлення - коли кіберзлочинець вимагає від жертви виконувати певні дії або, навпаки, утримуватися від них.

Якщо відомі обставини та мета використання приватних зображень у сексторції, ризиковані практики й уразливі ситуації можна виявити на ранньому етапі.

ОСОБИСТА ТА СОЦІАЛЬНА ПРОФІЛАКТИКА

Щоб зменшити ризик стати жертвою сексторції, можна вжити індивідуальних та колективних запобіжних заходів:

- Захист власних зображень і відмова від їх поширення, перегляду або споживання - як власних, так і чужих.
- Сприяння освіті, що поважає приватність інших людей. Усе залишається приватним доти, доки його не переглядають і не поширюють.

Необхідно підвищувати обізнаність щодо того, що зображення не буде поширене й не стане вірусним, якщо люди не братимуть у цьому активної участі. Ніхто не повинен повторно травмувати постраждалих, виокремлюючи такі зображення, висловлюючи негативні коментарі або даючи їм оцінки.



Десять правил для жертв сексторції

Найбільша проблема, що виникає в результаті сексторції, полягає в тому, що тиск на жертву є надзвичайно великим, оскільки вона зазнає подвійної шкоди: окрім людини, яка їй погрожує, вона відчуває почуття провини або сорому, що дуже часто заважає їй звернутися по допомогу. У випадку з дітьми найгіршим сценарієм є те, що про це дізнаються їхні батьки. Ось чому особливо важливо надати жертвам інструменти та рекомендації, щоб, якщо вони вирішать самостійно впоратися з ситуацією, вони могли принаймні зменшити потенційну шкоду і навіть покласти край сексторції. Саме тут вчителі повинні намагатися допомогти, бути поруч і підтримувати, спираючись на свою роль дорослих, яким довіряють.

Для самопомогти жертвам рекомендуються наступні десять кроків. Їх можна надати учням, наголошуючи на тому, що порядок має значення, тому їх слід виконувати саме в такому порядку.

1. Попросіть про допомогу.

Попросіть про підтримку дорослого, якому довіряєте. Важливо мати пораду від людини, яка має певний життєвий досвід і може допомогти вам спокійно проаналізувати ситуацію, надавши точку зору, що контрастує з вашими думками, які можуть бути наслідком страждань і стресу.

2. Не піддавайтеся шантажу.

Не піддавайтеся вимогам шантажистів. Таким чином ви тільки посилюєте їх. Шантаж стане ще більш інтенсивним і болісним, якщо ви піддастесь. Таким чином ви можете дати зрозуміти, що існують нові можливості контролю над вами. Коли відбувається шантаж (оскільки у них є в розпорядженні компрометуюча інформація), ситуація може тільки погіршитися, якщо ви продовжуєте піддаватися.

3. Не надавайте додаткової інформації.

Будь-які деталі або інформація можуть бути використані зловмисниками та кіберзлочинцями. Деталі, якими володіють шантажисти, завжди є потенційною загрозою. Чим більше ви знаєте про когось, тим вразливішим він є. Необхідно уникати надання додаткової інформації, навіть якщо вона здається неважливою.

4. Зберігайте докази.

Якщо хтось погрожує вам, показує вам конфіденційну інформацію тощо, зробіть знімок екрана та запишіть дату, час і URL-адресу. Важливо зберегти докази або сліди погроз, записавши дату і час, коли вони були зроблені. Обидва ці елементи можуть бути корисними для більш спокійного аналізу ситуації та консультації з іншими людьми.

5. Видаліть всю свою конфіденційну інформацію.

Видаліть або зберігайте в безпечному місці свою приватну інформацію або зображення та закрийте камеру комп'ютера. Шантажисти можуть спробувати отримати компрометуючі зображення або деталі, які дадуть їм більше влади. Щоб запобігти цьому, почніть з видалення конфіденційної інформації з пристрою, навіть з жорсткого диска. Перевірте, з ким ви ділитеся своїм життям і секретами в соціальних мережах.

6. Видаліть шкідливе програмне забезпечення.

Переконайтеся, що на вашому пристрої немає шкідливого програмного забезпечення (троянських програм, шпигунських програм тощо). Шкідливе програмне забезпечення є «союзником ворога на вашій території», і його необхідно уникати за будь-яку ціну. Позбутися його нелегко. Для цього необхідно застосовувати проактивний та наполегливий підхід. Безпека обладнання гарантує безпеку користувача.

7. Змініть свої особисті паролі.

Шантажист може шпигувати за вашими повідомленнями в соціальних мережах. Перевіривши, що на вашому пристрої немає шкідливого програмного забезпечення, обов'язково змініть паролі для входу в електронну пошту, соціальні мережі тощо. Постарайтесь максимально ускладнити подальше шпигунство.

8. Перевірте, чи зможе шантажист здійснити свою погрозу, якщо це можливо і не пов'язано з додатковими ризиками.

Багато погроз є помилковими і неможливими для виконання. Можливо, погроза не може бути виконана, оскільки у вимагача насправді немає приватного зображення або неможливо ідентифікувати особу, яка на ньому зображена.

9. Попередьте свого кривдника, що його дії є серйозним злочином.

Він або вона повинні знати, що можуть бути притягнуті до кримінальної відповідальності, і що вам про це відомо. Шантажисти не завжди замислюються над злочинами, які вони вже вчиняють або можуть вчинити у разі реалізації своїх погроз. Вони мають усвідомлювати, які саме злочини до них застосовні, а також те, що жертва знає про можливе покарання.

10. Подайте скаргу.

Закони суворо карають за такого роду злочини, особливо якщо ви неповнолітній або дитина. Погрози опублікувати або поширити несанкціоновані зображення або записи, а також записувати за допомогою шкідливого програмного забезпечення з метою маніпулювання чужим комп'ютером або викрадення секретних паролів є незаконними діями. Якщо ваша приватність, честь або фізична чи психологічна цілісність знаходяться під загрозою або були порушені, ви повинні повідомити про це.



**Сексуальність та
споживання
порнографії в
Інтернеті**

Вступ

Серед контенту, який вважається шкідливим для маленьких дітей і, наприклад, заборонений для перегляду, є такий, що містить надмірне насильство та відверті сексуальні сцени. Вплив таких матеріалів вважається шкідливим для хлопців і дівчат молодшого віку, оскільки вони ще не мають необхідного рівня розвитку та навичок, щоб впоратися з цим.

Однак за лічені роки ми перейшли від обмеження телевізійного контенту в час перегляду дітьми до неконтрольованого (і досить часто надмірного) та безконтрольного доступу до контенту, який може бути шкідливим для дітей. Також може трапитися випадкова наявність такого аудіовізуального контенту на мобільних телефонах, планшетах та комп'ютерах дітей. Водночас контент у порноіндустрії стає дедалі більш різноманітним, дешевим та екстремальним

Будь-хто, хто має доступ до Інтернету, тепер може отримати доступ до мільйонів безкоштовних зображень, які кілька років тому були доступні в Інтернеті за окрему плату.

Сьогодні порнографічний контент став надзвичайно доступним у цифровому середовищі. Його можна знайти онлайн без чітких вікових бар'єрів, у будь-який час і з будь-якого місця, часто безкоштовно та анонімно. Порноіндустрія, зі свого боку, робить все можливе, щоб «розмістити» свій продукт на ринку. Контент може бути спочатку безкоштовним, але все одно приносить прибуток завдяки рекламі. Це означає, що навіть ті, хто ще не досяг зрілості, можуть випадково або з цікавості зіткнутися з таким матеріалом, але через свій вік ще не мати достатніх навичок критичного сприйняття та психологічного фільтрування подібного контенту.

Пам'ятайте

- Все більш глобалізоване, пов'язане та цифровізоване суспільство, в якому ми живемо, чинить постійний тиск на ранню еротизацію та гіперсексуалізацію дітей, чому необхідно постійно та активно протидіяти.
- Прояви чоловічого шовінізму та патріархату, які іноді можуть бути обмежені в офлайн-середовищі, в Інтернеті поширюються без обмежень і поза контролем. Отже, серед молоді необхідно розвивати критичне мислення, адже незалежно від власного бажання рано чи пізно вони можуть натрапити на порнографічний контент в Інтернеті.
- Багато дітей випадково або зрідка, а то й регулярно, переглядають порнографію. Це спричиняє негативний психологічний та емоційний вплив, а також спотворює уявлення про емоційність, сексуальність та сексуальні стосунки.
- Порнографічна індустрія стала основним джерелом статевого виховання дітей.
- Порнографія пропагує та закріплює викривлене уявлення про здорові стосунки, стереотипи та сексуальне насильство.
- Молоді люди, які дивляться порнографію, вчать, що «справжній чоловік» не поважає відмову, тому насильство розглядається як «чоловіча» сила і влада. Молоді жінки привчені думати, що сексуальне насильство є нормальним явищем під час сексуальних контактів. Порнографія не є сексуальною освітою.
- Дослідження показують, що порнографічні сцени містять 10% позитивних поведінкових моделей, таких як поцілунки, обійми та посмішки, а решта - це сцени агресії.
- Порнографічний контент, незалежно від того, чи відповідає він рівню зрілості споживачів, дуже часто призводить до поширення мачо-цінностей і навіть до дій, що суперечать закону та порушують права людини.
- Хоча необхідно пропагувати сексуальне та репродуктивне здоров'я, ми також повинні зосередитися на афективно-сексуальній освіті, яка обмежує вплив гіперсексуалізованого середовища, перевантаженого порнографією, яку часто споживають діти.



- Вкрай важливо, щоб відповідальні дорослі поступово і відповідно до віку надавали дітям молодшого віку якісну сексуальну освіту, щоб відсутність такої інформації не створювала вакуум, який дитина могла б заповнити випадковим і небезпечним контентом з інтернету.

Визначення та особливості

Для того щоб оцінити реальні масштаби впливу порнографії на дітей або її споживання ними, необхідно проаналізувати змінні та фактори, що на це впливають.

ДЖЕРЕЛА, ДОСТУП ТА СПОЖИВАННЯ ПОРНОГРАФІЧНОГО КОНТЕНТУ

Джерела високосексуального, а точніше - порнографічного контенту, який потрапляє на наші екрани, можуть бути різними. Тому доступ до нього дуже складно обмежити. Найпоширенішими формами є, у такому порядку:

- основні порнографічні веб-сайти великих корпорацій;
- інші менш відвідвані веб-джерела, що надають менш відібраний та маргінальний порнографічний контент;
- приватні повідомлення WhatsApp у формі вірусних або розподільних ланцюжків;
- прямі трансляції, як публічні, так і обмежені для певної аудиторії.

Це можуть бути не єдині джерела доступу до порнографії. Є й інші, які можуть відвідувати діти, багато з яких використовують фальшиві дані та способи оплати.

- Більш-менш складні послуги між приватними особами, коли одна особа отримує доступ до зображень, а інша пропонує зображення за оплату. Популярним прикладом є OnlyFans. Цей сайт був створений для уникнення цензури в звичайних соціальних мережах, а зараз використовується як сервіс «порно на замовлення».
- Живі веб-камери, також звані порно-відеодзвінками.

Ці можливості не обмежуються наведеними прикладами, але вони наочно окреслюють широкий спектр способів споживання порнографії, що існують нині, масштаби присутності онлайн-порнографії, а також труднощі обмеження її поширення та доступу до неї для дітей.

З іншого боку, хоча для жодної окремої країни не існує систематичної статистики, можна припустити, що перший контакт із порнографією зазвичай відбувається до 10 років — випадково або внаслідок дитячої цікавості. Також можна стверджувати, що порнографію регулярно споживає значна кількість дітей віком від 12 років, причому більшість із них — хлопці.

Слід також зазначити, що внаслідок здешевлення та зростання потужності інтернет-з'єднань на стаціонарних і портативних пристроях виникає серйозна перешкода для контролю доступу до такого контенту. Це приводить до висновку про необхідність ужиття термінових заходів у цій сфері. Крім того, варто зауважити, що для доступу до безкоштовної порнографії дітям зазвичай достатньо лише задекларувати досягнення встановленого законом віку в країні доступу. У такий спосіб вони звільняють постачальників контенту від будь-якої відповідальності. Водночас самі постачальники контенту могли б уживати більше заходів для запобігання доступу до такого контенту для хлопчиків і дівчаток.

ВИГАДКА З РЕАЛІСТИЧНИМ ВИГЛЯДОМ ТА РЕАЛЬНИМИ НАСЛІДКАМИ

Однією з особливостей порнографії, що посилює її потенційний негативний вплив на молодь, є те, що вона використовується як джерело інформації або натхнення для сексуальності. Порнографія, яку переглядають молоді люди, може бути шкідливою з двох причин: під час її споживання немає впливу інших джерел інформації або захисних факторів (сім'я, школа тощо); ступінь реалістичності, який демонструє порнографія, є дуже низьким, і молоді люди схильні забувати, що це вигадка. Це враження, ніби вони є свідками реальних порнографічних сцен, може посилюватися з кількох причин, зокрема:

- Існують відео, в яких знімаються аматорські актори та актриси.
- Є професійні актори та актриси, які вдають, що вони не мають відношення до порноіндустрії, а є звичайними людьми.
- Є справжні відео (вкрадені з терміналів або таємно записані на відкритому повітрі), змішані з професійними зображеннями.



Таким чином, якщо те, що споживається, розмиває сприйняття різниці між реальністю та вигадкою, можливо, з метою підвищення збудження, споживачі можуть зробити висновок, що те, що відбувається там, може статися з будь-ким. Отже, вважається, що вони також можуть імітувати поведінку та ставлення, які є частиною цих сцен і досягають нас майже підсвідомо.

НАСИЛЬСТВО ЩОДО ЖІНОК

Багато популярних порнографічних сцен містять фізичне насильство над жінками. Іноді це більш-менш вимушена частина сценарію. Іноді це просто безпричинне насильство, яке здається самоціллю. Сила, іноді насильство і побиття, застосовуються для того, щоб змусити жінок терпіти або виконувати певні сексуальні дії. Їх ґвалтують, іноді навіть група людей. Також можна побачити зображення агресії проти жінок, яких ґвалтують, користуючись їхньою слабкістю, наприклад, коли вони перебувають під впливом алкоголю або наркотиків. Все це здається виправданим і ніхто не ставить це під сумнів. Сценарії здаються логічними, і такі типи поведінки, здається, набувають певного ступеня нормалізації та легітимізації завдяки постійному повторенню.

ВІДНОСИНИ ДОМІНУВАННЯ-ПІДКОРЕННЯ ТА ОБ'ЄКТИВІЗАЦІЯ ЖІНОК

Окрім насильства, зображеного в порнографії, яке прагне виправдати та уможливити домінування чоловіків над жінками, жінки завжди зображуються як об'єкти, єдиною метою яких є задоволення чоловічого сексуального бажання. Їхні потреби, імпульси, інтереси чи задоволення не показуються в порнографічних сценах.

НЕГАТИВНІ ПСИХОЛОГІЧНІ ТА СОЦІАЛЬНІ НАСЛІДКИ

Надмірне споживання порнографії без критичного мислення може мати надзвичайно шкідливий вплив на здоров'я та самооцінку людей та їхніх сексуальних партнерів. Світ, який вони зображують як ідеальний, з чудовими тілами,

надмірно великими геніталіями та сповненими задоволення марафонськими сексуальними контактами, показується як норма, якої слід дотримуватися, щось, що потрібно повторювати. Реальність, однак, дуже відрізняється від цієї вигадки і це може згодом призвести до плутанини, низької самооцінки, фрустрації, травми та дисфункціональних стосунків.

СЕКС БЕЗ КОХАННЯ

Коли порнографія використовується для визначення рольових моделей у нашій поведінці та сексуальному житті, всі афективні компоненти видаляються. Немає діалогу, немає щедрості, немає турботи про іншу людину, а почуття та прихильність залишаються невидимими. Сексуальні контакти зводяться до імпульсивних або егоїстичних компонентів пристрасті і, через імітацію, до гімнастичної хореографії, яку виконують андроїди. Сексуальні стосунки, які за своєю суттю є як афективними, так і сексуальними, стають атлетично-сексуальними, зведеними до базових генітальних дій.

РИЗИКОВАНІ ПРАКТИКИ

Заходи контрацепції та профілактика захворювань, що передаються статевим шляхом (ЗПСШ), не мають місця в порнографічних сценах. Не має значення, чи йдеться про стосунки між двома або кількома людьми, а також чи подаються вони як випадкові чи регулярні. Ризики вагітності або інфікування не враховуються - їх просто ігнорують. Незахищений секс часто подається як практика підвищеного ризику, адже партнери в одній сцені можуть бути випадковими, різними та численними. Унаслідок цього незахищений секс нормалізується.



ПРОБЛЕМНЕ ВИКОРИСТАННЯ

Як і будь-яка інша приємна діяльність, споживання порнографії викликає викид дофаміну і активує систему винагороди в мозку. Хоча залежність від онлайн-порнографії (також відомої як «кіберпорнографія» для позначення способу її споживання) науково не визнана як адиктивний розлад, реальність показує, що зловживання є проблемою, яку в багатьох випадках дуже важко подолати. Зростання толерантності, серйозне втручання в повсякденну діяльність та використання її як модулятора ставив дисфорії роблять її дуже схожою на поведінкову залежність, таку як компульсивне азартне гравство. Так само, як і в разі інших нехімічних розладів, що викликають залежність, люди з існуючими захворюваннями можуть «зачепитися» за джерело задоволення, яке є дешевим, зручним, анонімним, доступним і нескінченним.

Стратегії профілактики споживання порнографічного контенту

Втручання вимагає чотирьох напрямків дій:

- підвищення обізнаності громадськості;
- афективно-сексуальна освіта, адаптована до нових реалій;
- обмеження доступу;
- просування критичної соціальної позиції щодо цієї індустрії.

Деякі з цих заходів можна застосовувати безпосередньо вдома, інші – у співпраці зі школою. Активна участь батьків у таких питаннях допомагає дитині безпечно орієнтуватися у цифровому середовищі та формує здорове ставлення до сексуальності й власного тіла.

ПІДВИЩЕННЯ ІНФОРМОВАНOSTІ ГРОМАДСЬКОСТІ

З різних культурних або соціальних причин у деяких місцях або громадах обговорення сексу є табу або, принаймні, дуже незручним. Аналогічно, про доступність порнографії для дітей зазвичай не говорять. Коли порнографія потрапляє на перші шпальти ЗМІ, люди часто відчують однаково і збентеження, і подив. Сором, ігнорування теми або шок від неї не допомагають. Звичайно, багато дорослих знають, що в Інтернеті є порнографія, але вони не усвідомлюють, наскільки вона легкодоступна та наскільки вона різноманітна і екстремальна. Однак батьки заявляють, що доступ до невідповідного контенту є однією з їхніх головних турбот щодо використання Інтернету їхніми дітьми. Вони не усвідомлюють грубості сучасної порнографії і, звичайно, всіх можливих шкідливих наслідків, крім сексуальної відвертості, які можуть бути результатом її споживання дітьми. Необхідно підвищити обізнаність

сімей, щоб вони не недооцінювали наслідки повсюдності цього потужного супротивника в Інтернеті.

АФЕКТИВНО-СЕСУАЛЬНА ОСВІТА, АДАПТОВАНА ДО НОВИХ РЕАЛЬНОСТЕЙ

Афективно-сексуальна освіта є протиотрутою від впливу ранньої еротизації, гіперсексуалізації та чоловічого шовінізму, присутніх у нашому суспільстві та переважаючих у порнографії. Сім'ї та школи повинні бути орієнтирами для дітей у їхніх перших сексуальних інтересах, щоб вони не сприймали порнографічні веб-сторінки як свою сексуальну Вікіпедію. Однак, хоча основи цієї освіти є однаковими, можливо, її зміст та планування (вік, методи...) повинні еволюціонувати, щоб адаптуватися до нової переважаючої та стійкої реальності, а також пропонувати нові чоловічі рольові моделі. Порнографія існує: ми можемо натрапити на неї або споживати її. Сучасна порнографія відрізняється від тієї, яку ми уявляємо і яка була доступна лише десять років тому. Необхідна рішуча освітня реакція, адаптована до цих нових часів.

Сім'ї та школи повинні бути орієнтирами для дітей у їхніх перших сексуальних інтересах, щоб вони не сприймали порнографічні веб-сторінки як свою сексуальну Вікіпедію. Однак, хоча основи цієї освіти є однаковими, можливо, її зміст та планування (вік, методи...) повинні еволюціонувати, щоб адаптуватися до нової переважаючої та стійкої реальності, а також пропонувати нові рольові моделі.

ОБМЕЖЕННЯ ДОСТУПУ

Раніше вже згадувалося, що порнографія може потрапляти на наші цифрові екрани різними шляхами. Однак найпоширенішим, найзручнішим і найдоступнішим є порнографічні веб-сторінки. Існує кілька рішень для батьківського контролю, які допомагають уникати, обмежувати, контролювати або наглядати за доступом до небажаного контенту. Це інструменти, які необхідно оцінювати, адаптувати та налаштовувати для кожної ситуації (платформа, пристрій, тривалість тощо) та віку, але їх не можна вважати остаточними. Без сумніву, вони можуть бути дуже корисними, особливо у випадку з молодшими дітьми. Спірним є питання, чи повинні вони мати окремий цифровий пристрій, підключений до Інтернету.

Іншою стратегією обмеження доступу до потенційно шкідливого контенту, такого як певні види порнографії, може бути також підвищення видимості конкретних альтернатив, що замінюють більш токсичні види споживання. Як наслідок, протягом останніх кількох років з'явилося кілька пропозицій щодо інших видів порнографії під гаслами «етичної», «феміністичної» або

«освітньої»; всі вони прагнуть створити іншу модель індустрії, засновану на принципі: «якщо її неможливо усунути, то зменшення або заміна можуть бути меншим злом».

ПРОСУВАННЯ КРИТИЧНОГО СОЦІАЛЬНОГО ПОЗИЦІЮВАННЯ

Безкоштовний доступ дітей до порнографічного контенту має серйозні наслідки, які вимагають комплексного реагування. Як і в будь-якій іншій галузі (а ця є особливо прибутковою), ми повинні вимагати не лише дотримання законодавства. Необхідно наполягати на впровадженні заходів, що обмежують шкідливий вплив (якщо такий має місце), застосовуючи етичні критерії, що посилюють стандарти соціальної відповідальності.

Необхідно сформувати колективну свідомість, яка ставить під сумнів і висвітлює безвідповідальні практики, щоб чинити достатній тиск на компанії цього сектору. Така свідомість також допоможе вимагати більш суворих змін до законодавства і, отже, більш жорстких обмежень у складному глобальному середовищі Інтернету, де не можна відмовлятися від вимоги дотримання принципу найкращих інтересів дітей.

10 рекомендацій щодо безпечного та усвідомленого ставлення до онлайн-контенту

Оскільки в Інтернеті іноді можна випадково натрапити на матеріали, що містять спотворені або нереалістичні зображення людських стосунків, важливо мати рекомендації, які допоможуть зменшити їхній потенційний негативний вплив. Нижче наведено десять коротких рекомендацій, спрямованих на розвиток критичного мислення, захист особистих кордонів та виховання відповідального ставлення до онлайн-контенту:

- Пам'ятайте, що багато онлайн-матеріалів є інсценованими. Те, що показують в Інтернеті, часто не відображає реальне життя.
- Підходьте до будь-якого контенту критично. Онлайн-відео або зображення не є надійним джерелом інформації про стосунки або людську поведінку.
- Покладайтеся на власні почуття та комфорт. Ваші межі, уподобання та темп мають значення. Немає необхідності слідувати зразкам з Інтернету.
- Будь-яка взаємодія з іншими людьми повинна відбуватися за взаємною згодою. Це стосується як спілкування, так і будь-яких дій у реальному житті.
- Будуйте стосунки на основі поваги та рівності. Інша людина є партнером у спілкуванні, а не інструментом для задоволення чи виконання чужих очікувань.
- Завжди відкидайте будь-які форми насильства або примусу. Повага до себе та інших є основою безпечної взаємодії.
- Аналізуйте контент, який ви бачите. Якщо щось виглядає принизливим, небезпечним або нереалістичним, до цього слід ставитися критично і не підтримувати.
- У реальному житті дбайте про свою безпеку та здоров'я. Не беріть за приклад поведінку персонажів з відео або фільмів - їхні дії не є прикладом для наслідування.
- Зберігайте своє приватне життя без тиску та порівнянь. Ваші межі та комфорт важливіші за очікування інших або соціальні стандарти.
- Звертайте увагу на свої звички перегляду або використання онлайн-контенту. Якщо це негативно впливає на ваш настрій, самооцінку або повсякденне життя, варто звернутися за допомогою до дорослого, якому ви довіряєте, або до фахівця.





**Дезінформація та
місінформація в
Інтернеті**

Вступ

Стаття 19 Загальної декларації прав людини, прийнятої Генеральною Асамблеєю Організації Об'єднаних Націй, гласить: «Кожна людина має право на свободу думки і висловлювання; це право включає свободу дотримуватися думок без втручання і шукати, отримувати і поширювати інформацію та ідеї через будь-які засоби масової інформації і незалежно від кордонів». Це означає, що кожна людина повинна отримати освіту, яка дозволить їй розвинути достатні здібності для доступу, оцінки та аналізу інформації (зображень, повідомлень тощо), що поширюється традиційними засобами масової інформації (друкованою пресою, телебаченням, радіо тощо) та новими формами ЗМІ, що надходять з підключених цифрових пристроїв, а також здібності для створення такого контенту.

У цьому контексті ключову роль відіграє медіа- та інформаційна грамотність (МІГ). МІГ можна визначити як процес набуття знань і навичок (вмін і установок), що дає людям можливість розуміти роль ЗМІ та інших постачальників інформації, критично оцінювати контент і приймати обґрунтовані рішення як користувачі або творці інформації та знань. У сучасному суспільстві, де Інтернет відіграє ключову роль, цифрова грамотність повинна бути включена до МІГ.

Пам'ятайте

Ми живемо в час зростаючого інформаційного перевантаження, дезорганізованого та упередженого інтересами, про які ми не знаємо. Створення дезінформації стало демократизованим і автоматизованим, що підтверджується існуванням вебсайтів, чії сервіси (інколи навіть безкоштовно) надають можливість створювати фейковий контент, який виглядає як справжній. У цьому контексті відповідальне цифрове громадянство має реалізовуватися через активну участь і спиратися на достовірну інформацію, водночас вимагаючи рішучої протидії поширенню дезінформації.

З точки зору етичного громадянства, важливо пам'ятати, що дезінформація має такі наслідки:

- Створення невизначеності та плутанини, що ускладнює розсудливість та позиціонування.
- Маніпулювання особистими рішеннями, прямо чи опосередковано.
- Пошкодження репутації або дискредитація людей, компаній або установ шляхом маніпулювання сприйняттям та думкою про них.
- Отримання фінансового прибутку.

Надання людям можливостей за допомогою МІГ є однією з найважливіших вимог для забезпечення рівного доступу до інформації та знань, а також для сприяння розвитку вільних, незалежних і плюралістичних медіа та інформаційних систем.

Легкість створення контенту та швидкість його поширення і вірусного розповсюдження в глобальному, динамічному та взаємопов'язаному цифровому суспільстві призвели до так званих «інформаційних розладів» (дезінформації та місінформації), що є предметом занепокоєння через серйозні наслідки, які вони можуть спричинити.

Коротко кажучи, можна сказати, що виявлення, викриття та загалом боротьба з помилковим контентом та інформацією, створеними навмисно чи ненавмисно, стали як особистим викликом, так і колективною потребою.

У суспільстві, де доступ до інформації та дезінформації, їх створення та обмін ними є настільки ж зручним і легким, як і швидким та ефективним, необхідно пам'ятати слова Ноама Чомскі: «Справжнє навчання відбувається через відкриття істини, а не через нав'язування офіційної істини, оскільки останній варіант не веде до розвитку критичного та незалежного мислення».

- Формування громадської думки з метою створення стану, який може бути вигідним для певних ідеологічних або інтересів груп.

З особистої точки зору, ті, хто потрапляє під вплив дезінформації:

- Марнують свій час і відволікаються без користі.
- Можуть бути маніпульовані і, як наслідок, не діяти або не мати вільної думки. Вони також можуть діяти помилково.
- Можуть несвідомо стати ланкою в ланцюзі поширення інформації.
- Можуть зазнати наслідків, навіть юридичних, внаслідок участі в поширенні дезінформації, що негативно впливає на інших людей.

Боротьба з дезінформацією безпосередньо залежить від здібностей кожної людини. Ця боротьба полягає в тому, щоб знати, але особливо в тому, щоб ставити під сумнів те, що ми бачимо або читаємо. Це завдання полягає в уважному спостереженні та слуханні, а не в простому акті бачення або слухання.

Визначення, поняття та особливості

ДЕЗІНФОРМАЦІЯ ТА МІСІНФОРМАЦІЯ

У доповіді Ради Європи «Інформаційний безлад: на шляху до міждисциплінарної рамки для досліджень та формування політики» (2017) наведено деякі визначення, прийняті Програмою розвитку Організації Об'єднаних Націй (ПРООН) у її інформаційній записці щодо COVID-19 від травня 2020 року:

- Дезінформація. Неправдива інформація, навмисно створена з метою заподіяння шкоди особі, соціальній групі, організації або країні.
- Місінформація. Інформація, яка є неправдивою, але не була створена з метою заподіяння шкоди.

Крім того, зловмисне використання інформації може стосуватися інформації, яка має слабе відношення до реальності, але використовується для заподіяння шкоди особі, організації або групі.

У цьому контексті необхідно уточнити деякі аспекти, які допомагають доповнити та зрозуміти значення і сферу застосування вищезазначених визначень:

- Дезінформація часто є спланованою, організованою і має необхідні засоби для досягнення шкідливої мети.
- У випадках місінформації слід зазначити, що, окрім відсутності шкідливих намірів, ті, хто її поширюють, як правило, не усвідомлюють, що це неправдива інформація.
- Характерною рисою зловмисного використання інформації є її використання в неетичних цілях.

Нарешті, використання терміна «фейкові новини» для позначення неправдивих новин в жодному разі не рекомендується, оскільки це надає статус новин тому, що ними не є.

Згідно з Організацією Об'єднаних Націй з питань освіти, науки і культури (ЮНЕСКО), поняття дезінформації використовується для позначення навмисних спроб (часто спланованих і скоординованих) заплутати або маніпулювати людьми шляхом поширення неправдивої інформації.

Дезінформація вважається особливо небезпечною, оскільки зазвичай є організованою, добре ресурсно забезпеченою та використовує передові техніки й технології, які підвищують її ефективність і масштаби поширення. Існує кілька ресурсів і стратегій, здатних породжувати певні форми місінформації:

- Сатира та пародія.

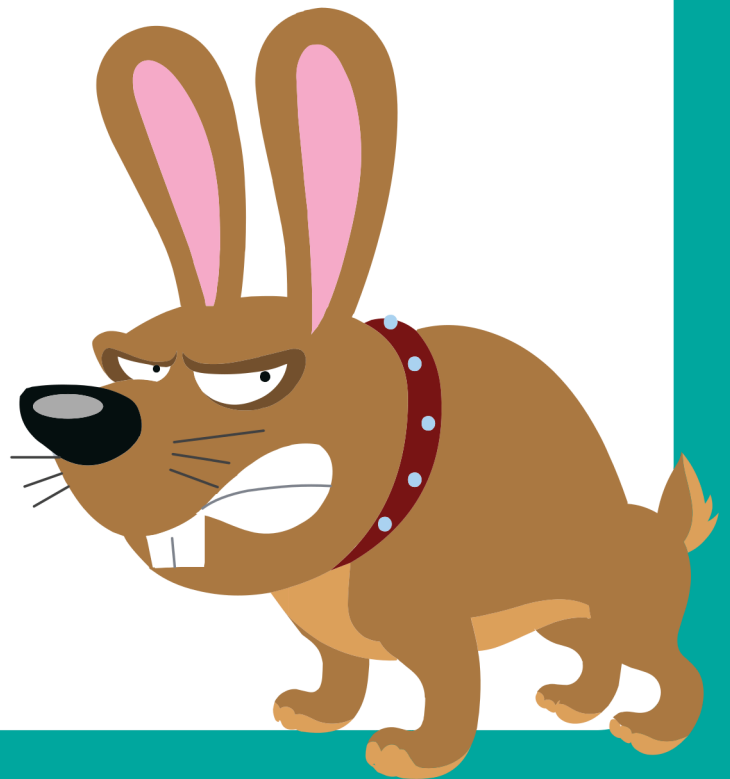
- Заголовки, розроблені як приманка для отримання кліків (заголовки-клікбейти).
- Нечесне використання підзаголовків, візуальних ресурсів або статистичних даних.
- Справжній контент, який поширюється поза контекстом.
- Підроблений контент (коли використовуються імена журналістів або логотипи ЗМІ, які не мають відношення до справи).
- Маніпульований та сфабрикований контент.

МЕДІА- ТА ІНФОРМАЦІЙНА ГРАМОТНІСТЬ

Протягом багатьох років міжнародні освітні установи, такі як ЮНЕСКО та Організація економічного співробітництва та розвитку (ОЕСР), привертають увагу до необхідності навчання критичної та розумної взаємодії із засобами масової інформації (медіаграмотності) з раннього віку.

ЮНЕСКО визначила навички та вміння, що складають медіа- та інформаційну грамотність (включно з цифровою грамотністю, що стосується цифрових медіа), як необхідну умову для розвитку інклюзивної, заснованої на знаннях освіти з раннього віку.

Ця грамотність надає людям автономію та навички для ефективного функціонування в технологічних, цифрових та комунікаційних середовищах, а отже, дозволяє вільно та повною мірою реалізовувати громадянські права.



Медіа- та інформаційна грамотність зосереджується на п'яти базових навичках, визначених як «п'ять С»: розуміння (Comprehension), критичне мислення (Critical thinking), креативність (Creativity), міжкультурна свідомість (Cross-cultural Consciousness) та громадянськість (Citizenship). Відповідно до критеріїв ЮНЕСКО, здатність критично мислити під час сприйняття та створення медіапродуктів включена до МІГ і, отже, сприяє розвитку здатності протидіяти споживанню, створенню та поширенню неправдивої або маніпульованої інформації, яка може спричинити плутанину, дезінформацію або навіть шкоду.

КРИТИЧНЕ МИСЛЕННЯ, НАВИЧКИ ТА СТАВЛЕННЯ

Критичне мислення є однією з «життєвих навичок», визначених Всесвітньою організацією охорони здоров'я (ВООЗ) у 1993 році як «здатності до адаптивної та позитивної поведінки, що дають змогу людині ефективно справлятися з вимогами та викликами повсякденного життя».

Слово «критичний» походить з грецької мови і означає «відокремлювати, розрізнити або судити». Критичне мислення допомагає відрізнити хороше від поганого, справедливе від несправедливого, або розрізнити правду від неправди. Насамперед, критичне мислення можна розвинути, практикуючи його на собі. Важливо розвинути упередження, заздалегідь сформовані думки та когнітивні упередження за допомогою логічних аргументів та запитань.

Згідно з науковою роботою Пітера А. Фационе «Критичне мислення: що це таке і чому воно важливе», критичне мислення включає:

- цікавість до широкого кола тем;
- прагнення стати і залишатися добре поінформованою людиною;
- пильність щодо можливостей використання критичного мислення;
- довіра до обґрунтованих процесів постановки питань;
- впевненість у власній здатності міркувати;
- відкритість до різних поглядів на світ;
- гнучкість при розгляді альтернатив та думок;
- розуміння думок інших;
- справедливість в оцінці;
- визнання та чесне протистояння власній упередженості, стереотипам або егоцентризму;
- розсудливість у призупиненні, винесенні або зміні суджень;
- готовність переглянути та переосмислити точки зору, коли чесна саморефлексія вказує на те, що така зміна є виправданою.

З процедурної точки зору критичне мислення передбачає принаймні п'ять ключових дій:

- Інтерпретація інформації для з'ясування її значення.
- Перевірка достовірності інформації на основі її джерела, узгодженості та інтенціональності або можливих наслідків, а також власних попередніх знань.
- Постановка запитань до явних і прихованих даних та інформації й їх зіставлення шляхом визначення альтернатив.
- Поглиблення розуміння шляхом отримання додаткових даних, а також виявлення невідомих фактів.
- Самооцінка шляхом аналізу власного мисленнєвого процесу, що супроводжує роботу з інформацією, з метою поставити під сумнів, підтвердити або переглянути міркування та остаточні висновки.

Залишається відкритим питання, наскільки результат цих дій пов'язаний з інтелектуальними здібностями людини. Можна сказати, що існує логічна кореляція між інтелектом (розуміється як рівень інтелектуального коефіцієнта (IQ), який можна виміряти) та критичним мисленням. Ця кореляція здається очевидною, оскільки для правильної оцінки інформації необхідно її отримати, обробити та зрозуміти, а також тому, що люди з найвищим IQ є більш стійкими до когнітивних упереджень. Однак критичне мислення також залежить від інших когнітивних здібностей, які не можна виміряти за допомогою тестів на інтелект або рис особистості.

З іншого боку, дослідження виявили три риси людей, які сприяють критичному мисленню:

- Цікавість або відкритість, що заохочує до відкритого дослідження.
- Бажання знайти істину, яке слугує мотивацією для докладання зусиль.
- Інтелектуальна скромність, яка є життєво важливою, оскільки критичне мислення передбачає ставити під сумнів інших людей, але, перш за все, себе самого. Критичне мислення - це ставлення, яке починається з припущення про відсутність знань.

Нарешті, варто зазначити, що розвиток критичного мислення означає стимулювання високого рівня мисленнєвих здібностей, які, згідно з дослідженнями, дають переваги в інших сферах життя шляхом:

- сприяння прийняттю кращих рішень;
- зменшення частоти негативних подій;
- покращення академічної успішності;
- підвищення ефективності діяльності, що вимагає аналітичних навичок.

На закінчення слід зазначити, що розвиток і активізація критичного мислення є не тільки необхідністю, зумовленою дезінформацією та місінформацією, але й можливістю

поліпшити своє особисте та професійне життя, що пояснює включення цього навичку до переліку навичок для життя, розробленого ВООЗ.

ЦИФРОВЕ ЖИТТЯ ДІТЕЙ І КРИТИЧНЕ МИСЛЕННЯ

Критичне мислення в підлітковому віці є фундаментальним, особливо для цифрової частини їхнього життя. Інтернет є середовищем, схильним до обману: він дуже проникний для неправди, і водночас це місце, де кількість і швидкість дуже часто переважають якість або точність.

Використання критичного мислення в ранньому віці, окрім того, що є питанням соціальної відповідальності, є інструментом безпеки та добробуту. Хлопчики та дівчатка стикаються з ризиками, наприклад, коли споживають дезінформацію або місінформацію, пов'язану зі здоров'ям (розлади харчової поведінки, чудодійні дієти тощо). Вони також перебувають у зоні ризику, коли людина, з якою вони нещодавно познайомилися й якій почали довіряти, поводить з ними певним чином або надає привілеї, що мають бути притаманні лише справді близьким людям. Вони можуть зіткнутися з проблемою під час доступу до нових онлайн-послуг, які не були перевірені або перехресно перевірені, або під час їх використання. З іншого боку, якщо діти ставлять під сумнів те, що вони роблять, чому і хто насправді отримує від цього найбільшу користь, вони будуть краще управляти своїм цифровим споживанням, не впадаючи в зловживання.

У молодих людей необхідно виховувати критичне ставлення до цифрового світу, ставлячи під сумнів інформацію, людей і послуги, а також їхню власну екосистему, починаючи з самооцінки своєї особистої поведінки, яка дуже часто характеризується зловживанням і компульсивним використанням. На додаток до цієї мотивації для активізації критичного мислення, їх необхідно навчати знанням, процедурам і навіть інструментам.

УПЕРЕДЖЕННЯ, ЕМОЦІЇ ТА ЇХНЕ ЗНАЧЕННЯ В ДЕЗІНФОРМАЦІЇ

Дезінформація може набувати різних форм. Хоча не всі вони можуть мати однакову мету, деякі можуть мати спільні стратегії для досягнення ефективності. Ми, люди, знаходимося по цей бік екрану, і дезінформація буде більш-менш успішною залежно від того, як ми на неї реагуємо.

Наша реакція на щось проходить через наш мозок і серце. Вона проходить через наше мислення та емоції. Таке обґрунтоване тлумачення інформації іноді відбувається несвідомо і може бути під впливом когнітивних упереджень.

Когнітивне упередження - це систематична

помилкова інтерпретація доступної інформації, яка впливає на спосіб обробки думок, винесення суджень і прийняття рішень. Когнітивні упередження мають кілька джерел: культура, соціальні впливи, емоційні або етичні мотивації, спрощення процесів обробки інформації, спотворення при відтворенні спогадів, пам'ять тощо.

Упередження - це скорочення, які наш мозок розвинув для спрощення проблем і полегшення прийняття рішень. Упередження є результатом еволюційної потреби вибірково фільтрувати стимули, звільняючи мозок від частини завдань з аналізу інформації. Однак вони зазвичай є перешкодою для виявлення дезінформації. Розглянемо деякі з найпоширеніших упереджень:

- Найбільша упередженість називається «сліпа пляма». Ця упередженість стосується ситуації, коли ми помічаємо упередженість інших людей, але не можемо або не усвідомлюємо власну.
- Упередження підтвердження змушує нас переоцінювати інформацію, яка відповідає нашим власним переконанням (цінностям, ідеологіям, упередженням); або, якщо це не вдається, переходити до наших домінуючих переконань і несвідомо ігнорувати ті, що не відповідають нашим власним думкам.
- Упередження звичності з його контрпродуктивним ефектом полягає в тому, що чим частіше ми стикаємося з певною інформацією (незалежно від її правдивості), тим більша ймовірність, що ми вважатимемо її правдивою.
- Соціальна взаємодія спонукає нас робити те, що роблять інші люди, підсилюючи таке первинне почуття, як приналежність до групи.
- Ефект візуальної переваги походить від того, що наш мозок обробляє зображення в 60 000 разів швидше, ніж написаний текст. З іншого боку, ми запам'ятовуємо 80% того, що бачимо, 20% того, що читаємо, і 1% того, що чуємо. Контент, який супроводжується зображеннями, отримує на 84% більше відвідувань і поширюється в 40 разів частіше, ніж контент без них.
- Мотивоване міркування - це тип емоційного упередження, що стосується нашої несвідомої схильності обробляти інформацію таким чином, щоб дійти висновків, які можуть відповідати певній меті або задачі.

Емоції також не допомагають боротися з дезінформацією, оскільки наш процес мислення є не тільки раціональним, але й емоційним. Коли інформація викликає певну емоцію, це може вплинути на аналіз інформації з метою розробки раціонального обґрунтування.

Деякі емоції особливо важко контролювати, і вони змушують нас втрачати самоконтроль. Серед них: гнів, співчуття, захоплення, цікавість, страх і терміновість. Дезінформація підживлює їх, і через емоційну складову нашого мислення спонукає нас ділитися нею.

ФІЛЬТР-БУЛЬБАШКА ТА ЕХО-КАМЕРИ

Поняття «фільтр-бульбашки», також відоме як «інформаційна бульбашка», означає, що інформація, яку нам пропонує Інтернет (пошукові системи, соціальні мережі, розважальні платформи, онлайн-магазини тощо), обмежується нашими власними характеристиками. Технології дозволяють нам підбирати інформацію так, щоб вона подавалася нам відповідно до її ймовірної актуальності чи важливості для нас. Елі Парізер у своїй книзі «Фільтр-бульбашка: як нова персоналізована мережа змінює те, що ми читаємо і як ми мислимо» у 2017 році знову детально розглянув цю проблему, на яку він звернув увагу ще шість років тому у своїй попередній роботі.

Щоб боротися з дезінформацією, ми повинні бути свідомі цього, адже критичне мислення має охоплювати не тільки те, що є очевидним і досяжним, а й те, що може не з'являтися перед нами. Такі фільтр-бульбашки обмежують нашу здатність до відкриттів і результати нашої цікавості, а також можливість ставити питання або заглиблюватися в тему, серед іншого. Вони є перешкодою для критичного мислення і, отже, союзниками дезінформації.

Що стосується споживання медіа, теорія «ехо-камер» стверджує, що якщо люди виявляють перевагу до подібних людей та інформації, будуть створені так звані «ехо-камери», тобто порожні простори, де відбиваються наші власні ідеї. Ця теорія передбачає, що цифрові технології не розширюють наш вибір, а обмежують наші можливості, діючи в цих камерах. Можливо, ми не усвідомлюємо цього і часто не активуємо механізми для збагачення наших джерел навіть впливами та ідеями, які спочатку суперечать один одному.

Коротше кажучи, ми вважаємо, що все гаразд і що так простіше, зручніше і швидше. Таким чином ми перестаємо брати участь у колективному будівництві за допомогою критичного мислення та індивідуального внеску. Ми повинні замислитися, чи є ми такими вільними, як думаємо, як у цифровому, так і в реальному світі.

Що можна зробити для запобігання та боротьби з дезінформацією?

Існує кілька напрямків втручання для виховання відповідального покоління, яке критично і активно протидіє дезінформації, як зазначено вище.

ЗУПИНИТИСЯ, ЩОБ ПОДУМАТИ, І РОЗГЛЯНУТИ ВАРІАНТ НЕ ДІЛИТИСЯ

Обмін інформацією здається стандартною поведінкою, якщо тільки не вказано або не мотивовано інше. Необхідно замислитися над цим і усвідомити, що обмін інформацією без її перевірки не є актом щедрості, а скоріше чимось, що не сприяє підтримці. Нічого не слід поширювати, не витративши достатньо часу на перевірку. Якщо у вас немає часу, бажання або можливості провести достатньо ретельну перевірку отриманої інформації, єдиним відповідальним варіантом є просто не поширювати її.

Нижче наведено п'ять причин, чому не варто ділитися інформацією без попередньої перевірки:

- Якщо ви ділитеся інформацією імпульсивно або поспішно, ймовірність того, що вона є неправдивою, є вищою. Якщо ви вважаєте, що поширення цієї інформації є важливим, також важливо витратити необхідний час на перевірку її достовірності.
- Дезінформація зазвичай завдає шкоди іншим людям або інтересам. Якщо ви берете участь у її поширенні, ви також несете відповідальність за її наслідки.
- Участь, висловлення думок, захист ідей, спроби допомогти іншим людям тощо є правом і обов'язком громадянина. Однак поширення неперевіреної інформації є необдуманим і неетичним.
- Коли ви несвідомо поширюєте неправдиву інформацію, ви є жертвою, але також і несвідомим спільником тих, хто її створив. Більше того, беручи в цьому участь, ви можете звинувачувати та шкодити іншим.
- Свобода вираження думок або повторення того, що поширюють інші люди, не звільняє вас від юридичної відповідальності, яка іноді може виникнути в результаті поширення неправдивої інформації.

Нарешті, важливо пам'ятати, що якщо інформація була поширена і виявилася неправдивою, необхідно вжити певних заходів, щоб спростувати її і спробувати компенсувати заподіяну шкоду.

УСВІДОМЛЕННЯ НАСЛІДКІВ І ВІДПОВІДАЛЬНІСТЬ ЗА СВОЇ ДІЇ

Дезінформація, а іноді й місінформація, мають негативні наслідки для інших. Незалежно від того, чи знаємо ми, якого роду, як і кому завдається шкода. Крім того, як уже згадувалося раніше, ми стаємо більш-менш непомітними жертвами наслідків цих інформаційних розладів. Тому для боротьби з дезінформацією корисно думати не тільки про абстрактні та віддалені поняття, а й про конкретні та близькі. Візуалізація, виявлення негативних наслідків та нашої відповідальності за них має допомогти запобігти нашій участі, свідомій чи несвідомій, у ланцюгах дезінформації.

Занадто часто основна увага приділяється виявленню та боротьбі з фейковими новинами та дезінформацією шляхом розвитку відповідних навичок у ранньому віці. Однак, можливо, важливіше зробити акцент на мотивації, підвищенні обізнаності, наданні причин для формування такого критичного та відповідального ставлення. Недостатньо просто знати, як це робити, потрібно ще й хотіти це робити та мати достатню мотивацію.

СТИМУЛЮВАННЯ КРИТИЧНОГО МИСЛЕННЯ В ШИРОКОМУ РОЗУМІННІ

Окрім розвитку здатності аналізувати та оцінювати інформацію (дедукція та висновки), важливо пропонувати завдання, які допоможуть учням ставити під сумнів себе та власні підходи, щоб вони навчилися стримувати поспішне та запальне висловлювання своїх думок чи суджень.

Часто корисно організувати заняття, під час якого їх просять раціонально обґрунтувати протилежну точку зору. Це змусить їх поставити під сумнів власні враження, без виклику чи особистої конфронтації, і глибше зануритися у вивчення інформації, що оцінюється.

ЗНАННЯ, ЩОБ УНИКНУТИ ВПЛИВУ УПЕРЕДЖЕНЬ ТА ЕМОЦІЙ

Боротьба з дезінформацією - це свідомо і постійна боротьба проти обмежень, які несвідомо накладаються на нас упередженнями та емоціями. У цьому сенсі боротьба з дезінформацією починається з того, щоб краще пізнати себе, визначити та зрозуміти свої упередження, а також те, як вони можуть впливати на нашу оцінку ситуації та наші відчуття, коли ми стикаємося з нею. Тільки усвідомивши мимовільні та несвідомі процеси, ми можемо вжити заходів для обмеження їхнього впливу в суспільстві, яке затоплене дедалі більш замаскованою та витонченою дезінформацією. У цьому можуть допомогти такі поради:

1. Бороться з власними упередженнями.
2. Уникайте врахування певної інформації тільки тому, що вона повторюється багато разів.
3. Ставте під сумнів будь-яку інформацію, навіть ту, яку отримуєте від сім'ї чи друзів.

4. Будьте пильні, якщо є зображення, оскільки вони привертають нашу увагу і можуть бути змінені.

5. Зупиніться та «поставте на карантин» усе, що викликає сильні емоції - особливо гнів, страх, надмірну цікавість, співчуття, захоплення або відчуття терміновості.

З упередженням підтвердження можна боротися, ставлячи під сумнів інформацію, яка найближча до наших думок, тому що, незважаючи на те, що ми розумні істоти, ми також запрограмовані не змінювати своїх думок. З цієї причини ми повинні ставити під сумнів все, особливо те, що відповідає нашому способу мислення або є малоймовірним.

ЗНАЙТЕ СВОЇ СТРАТЕГІЇ: ЯКА МЕТА І ЯК ПРАЦЮЄ ДЕЗІНФОРМАЦІЯ

Знання свого опонента завжди є перевагою в боротьбі. У цьому контексті дезінформація часто долає раціональну обережність людей, використовуючи та активуючи стратегії, що спираються на когнітивні упередження та емоції. Усвідомлення цього вже саме по собі є позитивним кроком. Наступним кроком може бути спроба визначити, яким саме чином відбувається цей процес.



З іншого боку, корисно знати мотив, що стоїть за створенням дезінформації. Іноді дезінформація створювалася просто для розваги, як виклик або для створення хаосу заради розваги. Інколи дезінформація має фінансові або ідеологічні цілі.

Необхідно мати здатність аналізувати те, що здається очевидним з точки зору можливої організованої загрози. Знання загальних цілей місінформації, аналіз мотивів, що стоять за нею, та її кінцевих наслідків, а також звичайних стратегій, що використовуються, ймовірно, допоможуть викрити шахрайство та ускладнити відповідальній особі досягнення її мети.

ЗНАННЯ ТА ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ДЛЯ ПЕРЕВІРКИ ІНФОРМАЦІЇ

Наприкінці процесу перевірки певної інформації завжди є конкретні дані (включаючи метадані, текстову інформацію, зображення, аудіо- або відеоматеріали), які необхідно перевірити. Це завдання має підтримуватися однією або декількома з таких навичок:

- Використання ефективного пошуку інформації на різних веб-платформах або в соціальних мережах.
- Доступ до надійних та актуальних джерел інформації.
- Знання та вміння користуватися програмами та сервісами для швидкої перевірки зображень та відео.
- Детальне вивчення інформації, не забуваючи про використання логічного мислення та дедукції.

Залежно від випадку, слід активувати додаткові або альтернативні процедури. Наприклад, перевірити на державних чи інших платформах, чи інформація, яку ви хочете поширити не фейкова. В Україні у вільному доступі можна скористатися такими ресурсами як Центр протидії дезінформації або інші.

Десять правил боротьби з дезінформацією

Загальне правило полягає в наступному: якщо ви не впевнені в правдивості чогось, не слід це поширювати. Тому перед тим, як поширювати інформацію, слід її перевірити. Для цього слід врахувати такі аспекти:

ДЖЕРЕЛО

1. Перевірте джерело інформації. Якщо ви його не знаєте або воно не вказане, будьте пильні та перевірте інформацію за допомогою джерел, яким ви довіряєте.
2. Оцініть її зовнішній вигляд: змінену URL-адресу, орфографію, якість, дивний або яскравий дизайн, дати тощо. Слідкуйте за подробицями.
3. Будьте обережні, коли інформація надходить від когось, кому ви довіряєте, від членів сім'ї або родичів. Це не є ознакою якості, оскільки немає гарантії, що вона була перевірена.

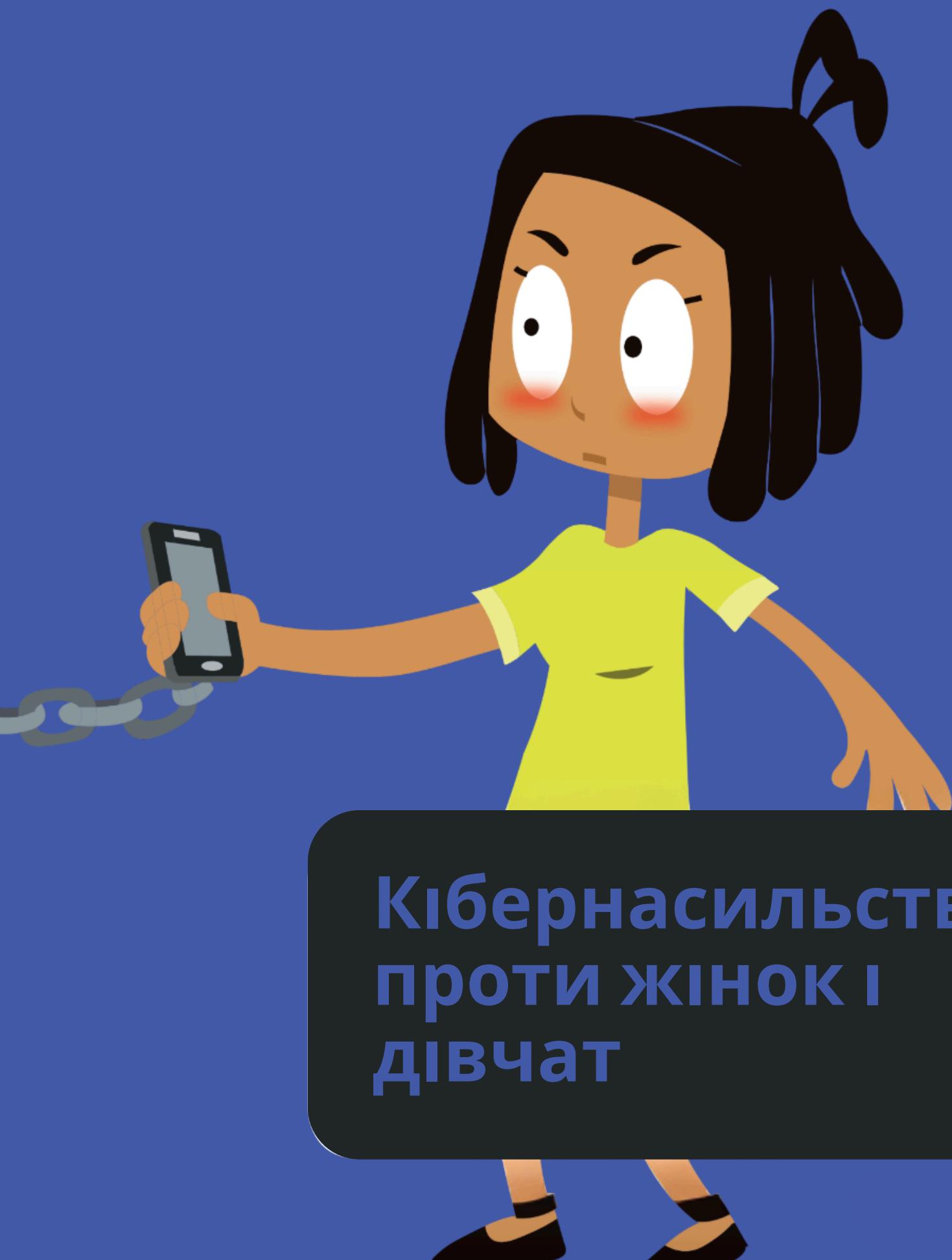


ЗМІСТ

4. Оцінюйте всю інформацію, а не тільки заголовок. Будьте обережні з цитатами або зображеннями, вирваними з контексту.
5. Звертайте увагу на зображення або відео. Їх можна легко неправильно представити або вони можуть не відповідати події чи часу, з якими вони нібито пов'язані.
6. Порівняйте інформацію з іншими надійними ЗМІ або джерелами. Будьте обережні, якщо не можете її знайти. Щодо питань, пов'язаних зі здоров'ям, попереджень або надзвичайних ситуацій, використовуйте лише офіційні джерела.
7. Остерігайтеся інформації, яка поєднує неправдиві дані з перевіреними або такими, що підлягають перевірці, аби маскуватися під цілком достовірну.

НАМІРНІСТЬ

8. Будьте пильні до інформації, яка викликає почуття гніву, занепокоєння або терміновості. Це стратегія, до якої часто вдаються ті, хто створює дезінформацію.
9. Новини та інформація, які є надто хорошими або надто дивовижними, також є способом приховування дезінформації. Залишайтеся об'єктивними у своїх аналізах.
10. Виявляйте гумор і сатиру. Існують веб-сторінки, які спеціалізуються на таких новинах у формі жартів і роблять це професійно, але не завжди безкорисливо.



**Кібернасильство
проти жінок і
дівчат**

Вступ

У всьому світі різні форми насильства щодо жінок і дівчат є серйозною структурною та глобальною проблемою. Різні прояви чоловічого та ґендерно-зумовленого насильства знайшли в Інтернеті сприятливе середовище для поширення й відтворення через особливості цифрового простору. Віктимізація дітей і жінок набуває багатьох форм, значна частина яких є наслідком виховання, просякнутого ґендерними упередженнями та стереотипами, що не сприяють рівності між усіма людьми.

Натуралізація чоловічого насильства означає, що воно залишається непоміченим, захищеним і прихованим у патріархальному суспільстві. Денатуралізація насильства та мікронасильства в

суспільстві є необхідним для того, щоб зробити насильство видимим та боротися з ним у цифровому та фізичному просторі. Важливо підкреслити, що насильство, яке може відбуватися в Інтернеті, може бути як миттєвим, простим і непомітним, так і серйозним.

Механізми запобігання насильству йдуть рука в руку з більш справедливим і рівноправним суспільством, де громадяни загалом, але особливо чоловіки, усвідомлюють і поділяють відповідальність за боротьбу з цими формами кібернасильства. Також необхідне відповідне законодавство, щоб забезпечити необхідну співпрацю великих інтернет-платформ і сервісів, де проявляється таке насильство.

Ключові моменти, про які слід пам'ятати

- Цифрове насильство щодо жінок є відображенням суспільства і підсилюється особливостями Інтернету, які використовуються для всіх видів кіберзлочинів.
- Ґендерно-зумовлене кібернасильство є насильством і, як таке, завдає шкоди жертві.
- Нормалізація певних форм поведінки в суспільстві, яке все ще є сексистським, прихований характер деяких форм віктимізації та, на перший погляд, нешкідливості інших форм є перешкодами на шляху до цифрового життя, вільного від насильства проти дівчат та жінок.
- Поряд з освітою в галузі рівності та відповідним законодавством, а також з метою припинення цифрового насильства з боку чоловіків, потрібна
- колективна відповідальність, особливо з боку чоловіків.
- Необхідно використовувати потенціал Інтернету для підвищення обізнаності, публічного викриття правопорушень та розширення можливостей жінок і феміністичних активісток у боротьбі з цією загрозою.
- Цифрове середовище, в якому ростуть дівчата, може мати каталізуючий ефект на проблему безкарності різних видів вираженого та проявленого кібернасильства.

Визначення та особливості

Нижче наведено деякі прояви кібернасильства щодо дівчат та жінок.

ГРУМІНГ

Хоча ця проблема стосується не лише дівчат, саме вони зазнають її значно частіше, і кількість випадків щодо них є більшою. Дівчата стають мішенню сексуальних агресорів, які прагнуть здійснювати різні форми сексуального насильства над дітьми та сексуальної експлуатації. Певною мірою поширеність і легітимізація різних форм насильства щодо жінок також лежать в основі цього типу зловживань.

Детальнішу інформацію про грумінг можна знайти в повному розділі цього посібника..





КІБЕРХАРАСМЕНТ І КІБЕРСТАЛКІНГ ЩОДО ФЕМІНІСТСЬКИХ АКТИВІСТОК

Різні форми домагань (образливі повідомлення, поширення фейкових новин, погрози, крадіжка особистих даних тощо) часто посилюються щодо жінок, які займаються феміністичним кіберактивізмом: використовують онлайн-простір для вираження своїх ідей, викриття несправедливості та боротьби з нерівністю. Ці жінки через свої ідеї та публічність страждають від усіх видів онлайн-домагань та насильства, яке іноді набуває форми цифрового лінчування. З цим видом насильства, принаймні на рівні його джерел, пов'язана також мізогінна ненависть, широко поширена в соціальних мережах.

СЕКСИСТСЬКИЙ АБО ҐЕНДЕРНО-ЗУМОВЛЕНИЙ КІБЕРБУЛІНГ

Кібербулінг - це навмисна та повторювана віктимізація особи (ізоляція, погрози, образи, висміювання, приниження тощо). Іноді агресор діє самостійно, а іноді їх декілька, і вони простими діями (наприклад, натисканням кнопки «Подобається» або «Поділитися») посилюють переслідування і, таким чином, перетворюють одну дію на домагання. Кібернасильство проти жінок набуває форми ґендерно-зумовленого кібербулінгу, коли зміст переслідування пов'язаний із нбито відповідністю жертви стереотипним правилам поведінки, статусу або зовнішнього вигляду, які приписуються жінкам у сексистському та патріархальному суспільстві. Приклади цього можна знайти в декількох аспектах повсякденного цифрового життя, де сама присутність жінок, хай навіть незначна або нова, стає приводом для переслідування. Зазвичай цей тип насильства має сексуальний підтекст або стосується їхнього сексуального життя. Шкідливі стереотипи щодо маскуліності та фемінності підсилюються низкою додатків та соціальних мереж, де жінки виглядають гіперсексуалізованими, тоді як

вираження їхньої власної сексуальності піддається цензурі.

СЕКСУАЛЬНИЙ КІБЕРБУЛІНГ

Інтернет, соціальні мережі та різні сервіси і додатки, що забезпечують комунікацію між людьми, спростили встановлення зв'язків між людьми, навіть якщо це небажано для однієї зі сторін. У цьому сенсі сексуальний кібербулінг означає будь-яку поведінку сексуального характеру або наміру, що здійснюється через Інтернет і є небажаною для отримувача. Деякі з найпоширеніших проявів сексуального кібербулінгу проти жінок в Інтернеті – це непристойні коментарі, повторювані прохання привернути увагу або встановити особистий контакт із яскраво вираженим сексуальним підтекстом, наприклад, надсилання сексуальних повідомлень або зображень чи прохання надіслати інтимні фотографії.

КОНТРОЛЮЮЧЕ КІБЕРНАСИЛЬСТВО

Це, мабуть, найпоширеніший і найчастіший вид насильства в підліткових парах. Він передбачає використання цифрових інструментів і цифрового контексту для контролю, впливу та обмеження свободи іншого партнера. Цей вид насильства стає дедалі поширенішим, оскільки стосунки перенеслися на мобільні телефони, соціальні мережі та програми для обміну миттєвими повідомленнями, такі як WhatsApp. Вимагання від партнера пароля до соціальної мережі, запит на її геолокацію або прохання видалити з її профілю фотографії, на яких вона виглядає привабливо або з іншими людьми, - це лише деякі з форм такого насильства.

Цей вид насильства може бути непомітним, оскільки відбувається в межах подружньої пари, їхньої приватної сфери та спілкування. Однак це одна з найпоширеніших форм насильства проти жінок. Цей вид насильства може здаватися не надто інтенсивним, але насправді він обмежує свободу, повну самореалізацію та права жінок, які його зазнають. Оскільки цей контроль базується на концепції «володіння партнером» (виведеної з міфу про чисте романтичне кохання), його також застосовують жінки щодо своїх чоловіків. Через це важко запобігти такому виду віктимізації як форми насильства проти жінок. У цьому сенсі ми повинні пам'ятати, що ґендерно-зумовлене насильство є структурним і з ним необхідно боротися відкрито. Наше суспільство оцінює поведінку за подвійними стандартами, залежно від того, чи її проявляють чоловіки, чи жінки. І саме тому це контролююче кібернасильство має більшу здатність підкорювати жінок, ніж чоловіків: або тому, що жінки можуть вважати, що вони повинні діяти відповідно до цієї соціально-встановленої ідеології, щоб поступитися вимогам свого партнера щодо контролю, або тому, що непідкорення таким вимогам може мати більш шкідливі наслідки.



СЕКСУАЛЬНЕ КІБЕРНАСИЛЬСТВО

Кібербулінг можна було б віднести до цієї категорії. Однак ми навмисно вирішили виділити його окремо як за інтенсивністю шкоди, так і за навмисністю. В обох випадках агресор використовує інтимні зображення жінки (порушуючи тим самим її право на честь, особисте життя та самооцінку), щоб принизити її або шляхом поширення цих зображень без її згоди, або шляхом погроз зробити це.

Сексторція означає вимагання від жертви певних дій під загрозою поширення приватних зображень жертви. Ви можете ознайомитися з окремим розділом, присвяченим цій темі.

Несанкціоноване поширення приватних зображень є формою насильства, в якій може брати участь значна частина населення. Перегляд або поширення зображень оголеної актриси, зроблених у приватності її будинку, або розкриття

місця, де їх можна побачити, є діями, до яких вдавалися багато людей. Завантаження інтимних зображень партнера або колишнього партнера на веб-сторінку або обмін ними з іншими людьми також є надто поширеним явищем. Коли метою таких дій є заподіяння шкоди жертві, це зазвичай називають «порнопомстою» або порнографією з метою помсти. Однак така назва є досить недоречною, оскільки ці зображення не були зняті для споживання іншими людьми, як це буває у випадку порнографії. Крім того, не існує попереднього «правопорушення», яке могло б пояснити нібито помсту.

Слід враховувати, що обидві форми насильства мають особливі наслідки для жертв, що є результатом мачо-сприйняття жінок, яке критикує вільне вираження жіночої сексуальності, на відміну від того, що відбувається у випадку сексуальної активності чоловіків.

Що можна зробити для запобігання та боротьби з цим?

ОСВІТА В ГАЛУЗІ РІВНОСТІ

В основі сексистської поведінки лежить недостатня освіта щодо поняття та значення рівності. Це проявляється на різних рівнях: у відносинах, економіці, символіці, суспільстві тощо. Сексистське насильство є одним із найсерйозніших проявів нерівноправного суспільства. Необхідно боротися з усіма формами цифрового кібернасильства. Для цього освіта є потужним інструментом. За її допомогою ми можемо працювати над досягненням реальної та ефективної рівності між чоловіками та жінками.

ФОРМУВАННЯ ЕМПАТІЇ ТА ВИДИМОСТІ НАСИЛЬСТВА

Іноді труднощі у сприйнятті страждань інших є причиною деяких форм насильства. Це стає більш поширеним, коли між агресором і жертвою немає прямого або одночасного контакту, або коли це відбувається в контексті, який толерує насильницькі практики або насичений насильством. Ці два фактори можуть співпадати в цифровому контексті і призводити до того, що агресори ініціюють або приєднуються до насильства. Деякі можуть бути не в змозі повністю або частково ідентифікувати

страждання жертви.

В інших випадках насильство не сприймається іншими людьми, незалежно від того, чи є вони агресорами, чи ні. Той факт, що насильство здійснюється в цифровому середовищі і може набувати різних форм не сприяє цьому. Ось чому так важливо зробити кібернасильство проти жінок видимим: це допомагає людям ідентифікувати, розпізнавати, запобігати та боротися з насильством.

РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ ПРО ПРАВОВІ НАСЛІДКИ

Хоча поширення інформації про чинне законодавство не є освітньою діяльністю, це є заходом, який може запобігти деяким насильницьким діям. У багатьох країнах ґендерно-зумовлене насильство вважається обтяжуючою обставиною, що на практиці означає значне посилення покарання за певні злочини. Якщо потенційний агресор усвідомлює юридичні наслідки своїх дій, він може відмовитися від своїх намірів. З іншого боку, якщо жертва усвідомлює, що вона є об'єктом злочину, це може допомогти їй вжити додаткових заходів для зменшення або припинення шкоди або

для сприяння притягненню винних до відповідальності.

ПРОСУВАННЯ КІБЕРБЕЗПЕКИ ТА ПРИВАТНОСТІ

Кібербезпека та конфіденційність є взаємопов'язаними поняттями, які управляються індивідуально та колективно. Основна увага завжди повинна бути спрямована на запобігання застосуванню насильства з боку агресора без обмеження свободи жертви. При цьому слід передбачити певний рівень розумних заходів самозахисту. З іншого боку, кожен може поставити під загрозу інших людей, з якими він контактує, навіть якщо спочатку не усвідомлює цього. Наприклад, якщо у них вкрали особисті дані або вони володіють конфіденційною чи приватною інформацією, яка їм не належить. Коротко кажучи, про конфіденційність та кібербезпеку слід дбати не тільки в своїх власних інтересах, але й з соціальної відповідальності та поваги до тих, з ким ми взаємодіємо, особливо якщо це жінки, з огляду на їхню особливу вразливість до цього виду злочинів.

КОЛЕКТИВНА УЧАСТЬ

Насильство проти жінок є колективним викликом. Кожен, особливо чоловіки, повинен долучитися до його викоринення. Часто ми є свідками насильницьких висловлювань щодо жінок у

соціальних мережах, групах миттєвих повідомлень, на форумах чи веб-сторінках тощо. Інколи ми стаємо співучасниками такого насильства, наприклад, коли бачимо або поширюємо вкрадене інтимне відео, яке хтось надіслав. Ми повинні бути більш свідомими, залишатися пильними, відкидати та протистояти таким формам сексистської кібервіктимізації.

КІБЕРАКТИВІЗМ

Окрім реагування на чоловіче шовіністичне кібернасильство, необхідно вжити активних заходів для його викоринення. Так само, як Інтернет приніс нові форми віктимізації, він також приніс нові можливості для боротьби з нею, надавши голос тим, кого зазвичай не чують. Феміністичний кіберактивізм під гаслом #MeToo досяг значних успіхів. Участь або підтримка таких рухів, звичайно, є способом покласти край цій біді як в Інтернеті, так і в реальному житті. Крім того, це стає способом дізнаватися і навчати про права жінок та ґендерну рівність.



Визначення десяти форм контролюючого кібернасильства

Боротьба з кібернасильством проти жінок знаходить свого найкращого союзника в мобільних телефонах, програмах миттєвого обміну повідомленнями та соціальних мережах. Оскільки це поширена форма насильства, яка нормалізувалася і помилково сприймається як прояв співучасті, турботи і навіть, певною мірою, кохання, важливо виявляти її в конкретних діях, щоб його було легше розпізнати.

Контроль кібернасильства необхідно ідентифікувати, по-перше, щоб уникнути його, а по-друге, тому що неможливо запобігти чи боротися з тим, що не сприймається як загроза.

ДЕСЯТЬ ОЗНАК КОНТРОЛЮЮЧОГО КІБЕРНАСИЛЬСТВА:

1. Переслідування або контроль партнера за допомогою мобільного телефону.
2. Втручання в онлайн-стосунки партнера з іншими людьми.
3. Шпигування за мобільним телефоном партнера.
4. Цензурування фотографій партнера, які він або вона публікує та поширює в соціальних мережах.
5. Контроль за діями партнера в соціальних мережах.
6. Вимагання від партнера підтвердження свого місцезнаходження за допомогою геолокації.
7. Примушування партнера надсилати вам інтимні фотографії.
8. Змушування партнера надавати свої паролі.
9. Примушування партнера показувати чати з іншими особами.
10. Виявляти гнів за те, що партнер не завжди відразу відповідає в Інтернеті.





**Цифровий слід,
репутація та
цифрова
ідентичність**

Вступ

Ми все більше живемо в цифровому середовищі. Іноді це є продовженням або невід'ємною частиною нашого життя поза мережею. Однак в інших випадках обидві сторони нашого життя, здається, не мають багато спільного, або тому, що середовище не дозволяє такої безперервності, або тому, що Інтернет, з усіма його можливостями, правилами та людьми, які його населяють, робить нашу поведінку, наше життя різними або такими, що здаються різними, по обидва боки екрану. У будь-якому випадку, це наше життя, єдине, яке проходить через обидва сценарії. З цієї причини і незважаючи на його очевидну незалежність, те, що робиться в одній зі сторін, зазвичай має відгомін, відображення в іншій, навіть якщо воно регулюється дуже різними параметрами.

Слід враховувати, що Інтернет має певні особливості (які часто не беруться до уваги), за допомогою яких він може визначати те, що відомо про кожного з нас,

як вони нас бачать і ставляться до нас. В Інтернеті ми залишаємо цифровий слід того, що робимо. Ми можемо показувати різні аспекти нашого життя залежно від конкретного середовища або соціальної групи. Інші формують думку про нас, не усвідомлюючи цього. Наша цифрова персона є дуже важливою річчю, яка може визначити чиєсь майбутнє. Цифрова інформація зберігається у часі, має необмежене охоплення і поширюється з величезною швидкістю. Однак багато людей, особливо наймолодші, не вважають важливим те, яке враження вони залишають про своє життя в Інтернеті. Це може спричинити для них незручності в коротко-, середньо- та довгостроковій перспективі.

Пам'ятайте

- Дуже молодим людям бракує життєвого досвіду, необхідного для того, щоб замислитися над наслідками своїх дій у середньо- та довгостроковій перспективі. Вони відчують, живуть і діляться своїм онлайн-життям для конкретної потенційної аудиторії (відомої чи невідомої) у конкретний момент часу.
- Діти не здатні уявити наслідки своїх дій або враження, яке вони справляють на оточуючих, або на людей, які не мали можливості з ними познайомитися. Ми повинні допомогти їм у цьому.
- Необхідно виховувати здорове використання технологій, що дозволяє розвивати критичне ставлення до

- соціального тиску (моди та звички) та комерційних інтересів, які заохочують постійне, надмірне і навіть компульсивне бажання ділитися своїм життям в Інтернеті.
- Приватність та кібербезпека також є ключовими факторами, що визначають, які дані стають частиною, добровільно чи мимоволі, цифрового сліду, репутації та цифрової ідентичності кожної людини.
- Цифровий Слід, репутація та цифрова ідентичність містять різні елементи, що виходять за межі того, що людина публікує. Де вона взаємодіє, з ким взаємодіє, які коментарі робить або навіть те, що вона робить чи не робить, може бути важливою інформацією.



Визначення та особливості

ЦИФРОВИЙ СЛІД

Відвідування веб-сторінок, використання таких сервісів, як Google, Yahoo, Bing тощо), встановлення певного додатка на мобільний телефон, завантаження фотографії, перевірка нашого місцезнаходження, здійснення відеодзвінка, натискання кнопки «Подобається» або читання публікації в блозі можливі завдяки сервісам, програмам і цифровим платформам, які взаємодіють з Інтернетом. Всі вони залишають слід. Незважаючи на те, що дії або процеси є миттєвими та «унікальними», слід, який вони залишають, може зберігатися назавжди. Кожного разу, коли ми виходимо в Інтернет, ми залишаємо незліченні сліди, навіть просто роблячи це. Вони зберігаються різними агентами (провайдером послуг) і можуть бути доступними для публічного або приватного доступу. Водночас кожен «крок» може поєднуватися з іншими - того самого типу з часом або іншого типу в той самий момент, - унаслідок чого формується щораз більш значуща та релевантна інформація. Так само, як кілька шляхів можуть розкрити наш уподобання щодо маршруту, набір слідів описує шлях і навіть спосіб його проходження. Поєднання даних, що стосуються різних реальностей, навіть з різних джерел, але пов'язаних з однією і тією ж особою, може генерувати додаткову інформацію з високою доданою вартістю.

Коротко кажучи, наше перебування в Інтернеті залишає слід, який приватні особи та компанії можуть реєструвати анонімно або під своїм ім'ям. У багатьох випадках наша згода на це надається майже несвідомо. Ці сліди зберігаються з різною метою. Серед основних причин зберігання виділяються три: отримання фінансового прибутку, надання умовного доступу до Інтернету та поліпшення якості й ефективності послуг або досвіду, що надаються. З цієї причини наш цифровий слід може, на краще чи на гірше, впливати на наше сьогодення та майбутнє, впливаючи на можливості, які можна знайти в Інтернеті, а також поза ним.

ЦИФРОВА ІДЕНТИЧНІСТЬ

Цифрова ідентичність людини, за найпростішим визначенням, - це те, що про цю людину розповідає нам Інтернет. Іншими словами, це сукупність даних і характеристик, які можна приписати цій людині під час доступу до неї або пошуку її в Інтернеті. Ця ідентичність може бути більш-менш широкою або детальною, так само як ви можете знати людину більш-менш добре залежно від часу, який ви витратили на її пізнання, та інформації, яку ви про неї отримали. Іноді знання про людину можуть бути обширними, але частковими, оскільки ми маємо доступ лише до упередженої або певної частини її життя.



Два місця в Інтернеті, де найчастіше можна знайти інформацію про людину, це:

- Браузери (такі як Google, Yahoo, Bing тощо), які насправді не містять самої інформації, але допомагають її знайти. Для цього використовуються невеликі тимчасові копії частини цієї інформації створюються з метою оптимізації процесу. Пошукові системи каталогізують та індексують інформацію, доступну на вебсторінках, а також дані з інших сервісів і платформ, що надають їм таку можливість.
- Соціальні мережі та платформи, які є нічим іншим, як великими базами даних, де, як правило, інформація пов'язана з конкретним профілем, і люди зазвичай ідентифікуються за допомогою тегів, псевдонімів або імен користувачів.

Таким чином, найпростіший спосіб побачити цифрову ідентичність людини - це набір інформації, що повертається браузерами та соціальними платформами. Цифрова ідентичність може впливати на відносини людини з іншими і, як наслідок, на важливі аспекти її життя. У цьому сенсі важливо розвивати нашу цифрову ідентичність і дбати про неї.

ЕЛЕМЕНТИ, ЯКІ СКЛАДАЮТЬ ЦИФРОВУ ІДЕНТИЧНІСТЬ

Важливо пам'ятати, що цифрова ідентичність виходить за межі даних (переважно тексту, зображень або відео), опублікованих про особу, які можуть бути ідентифіковані нею самою або іншими особами. Це становить найбільш очевидну та впізнавану ідентичність. Найповніша цифрова ідентичність також визначається іншими елементами, такими як:

- Ім'я користувача, зображення профілю та короткий текст, за допомогою якого визначається, представляється або оголошується його статус.

- Люди, з якими він або вона взаємодіє.
- Місця або платформи, де людина має профіль або бере участь, а також ті, які, будучи загальними, уникаються або не використовуються.
- Коментарі та взаємодії (лайки, пересилання тощо), які можуть бути на закритих або відкритих платформах, де її можна ідентифікувати.
- Будь-який цифровий слід, який може бути відкрито доступним.

ОСОБЛИВОСТІ ЦИФРОВОЇ ІДЕНТИЧНОСТІ

Окрім природи елементів, що формують ідентичність, важливо знати, якими особливостями вона володіє, щоб розуміти, як вона поводить себе і як на неї впливати:

- **З різними версіями.**

Цифрова ідентичність може бути, як зазначено вище, більш-менш детальною або розширеною, залежно від обсягу, типу та якості проаналізованих даних. Вона також може бути більш повною або лише частковою, залежно від того, чи базується вона на обмежених і конкретних джерелах інформації.

- **Динамічна.**

Цифрова ідентичність є динамічною і змінюється з часом. Її можна змінити, змінивши компоненти, з яких вона складається. Хоча, як правило, легше додавати атрибути або інформацію, ніж видаляти їх. Цифрова ідентичність змінюється під впливом змін, не пов'язаних з людьми, які користуються Інтернетом, таких як модифікації технічних термінів, використання або індексація самих платформ, що впливають на спосіб доступу до інформації, яка її складає. Конкретним прикладом цього може бути ситуація, коли певна соціальна мережа в певний момент вирішує дозволити або заборонити індексацію свого контенту та баз даних

- **Зростаюча складність.**

Широке використання соціальних мереж, яке відбулося приблизно в 2010 році, супроводжувалося більш складною цифровою ідентифікацією осіб. Цифрові ідентичності тепер складаються з більшої кількості елементів, оскільки люди публікують інформацію та взаємодіють з іншими більш точно, просто та регулярно.

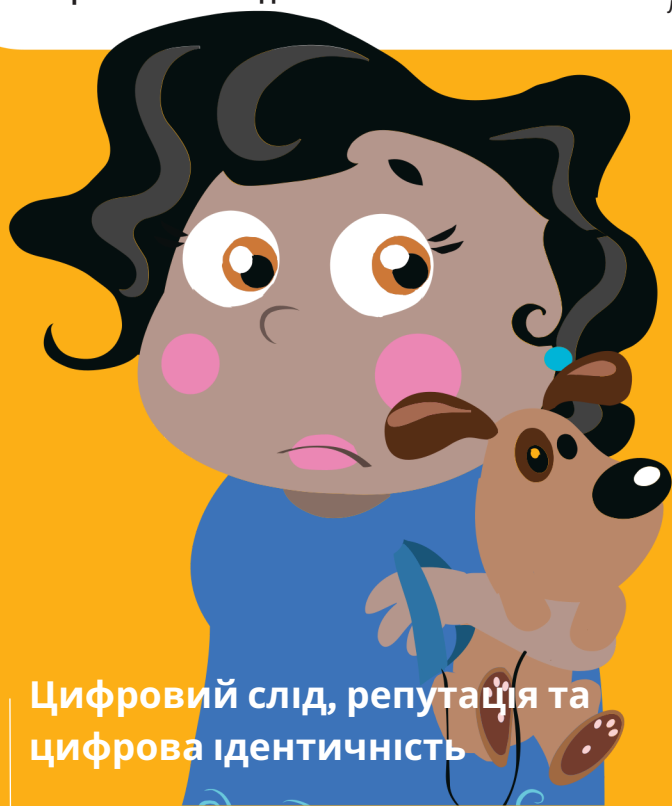
- **Висновок: важко контрольоване управління.**

Взаємодії, які стали можливими завдяки соціальним мережам, також ускладнили контроль над цифровою ідентичністю її власником, тобто особою, якої вона стосується, і більш залежним від того, що з нею роблять інші люди, оскільки всі взаємодії на цих соціальних платформах пов'язані з конкретними профілями, які є конкретними та ідентифікованими. Як приклад цього можна навести те, що коли людина позначає іншу особу в соціальній мережі, вона тим самим певним чином, позитивно чи інакше, впливає на її цифрову ідентичність, незважаючи на те, що це також може вплинути на її приватність.

ЦИФРОВА РЕПУТАЦІЯ

Поняття цифрової репутації пов'язане з тим, як людину сприймають інші на основі її цифрового життєвого шляху. Це пов'язано з цифровою ідентичністю, оскільки включає те, що про людину розкривається в Інтернеті. Однак це поняття йде далі, оскільки включає ширший часовий вимір і більш-менш суб'єктивну оцінку. Репутація означає оцінку даних у часі, а не лише їх місцезнаходження або сприйняття в певний момент часу.

Важливість цифрової репутації полягає в тому, що вона може переважати цифрову ідентичність у наших онлайн- та офлайн-відносинах і можливостях. Іншими словами, може бути важливішим те, як Інтернет «каже», ким людина була, ніж те, як Інтернет показує, ким ця сама людина є зараз або в певному контексті. Це також



може бути правдою в офлайн. Однак залишається питання про те, що Інтернет має безпрецедентну здатність записувати, зберігати і, що більш важливо, виносити на перший план конкретні дані або події з більш-менш віддаленого минулого людини, незалежно від необхідності або можливості це робити.

Усвідомлення того, що наш час в Інтернеті залишає майже незгладимий цифровий слід, здатний вплинути на наше життя в майбутньому, є дуже необхідним з раннього віку. Особливо в світі, де швидкість і миттєвість перешкоджають рефлексії та прогнозуванню наслідків у середньодовгостроковій перспективі.

Що можна зробити, щоб запобігти цьому та вжити відповідних заходів?

УСВІДОМЛЕННЯ ЕЛЕМЕНТІВ, ЩО ВХОДЯТЬ У ЦЕ, ТА ЇХНІХ ВЗАЄМОВІДНОСИН

Багато людей, особливо діти, заявляють, що діють з добрими намірами і не мають чого приховувати. Отже, вони стверджують, що їм не потрібно турбуватися про свій слід, репутацію чи цифрову ідентичність.

У цьому контексті слід наголосити на трьох основних аспектах:

- Приватність є фактором самозахисту. Чим більше ви знаєте про когось, тим вразливішим він є.
- Кібербезпека необхідна для гарантування приватності, а приватність, в свою чергу, є гарантією кібербезпеки.
- Приватність та кібербезпека є колективними питаннями, що регулюють відносини в групі. Те, що роблять інші люди, може впливати на нас і навпаки.

Згідно з цією логікою, слід, ідентичність та цифрова репутація кожної людини формуються інформацією та діями, які залишають про них сліди в Інтернеті. У свою чергу, ці сліди залежать як від самих людей, так і від інших, з якими вони взаємодіють, а також від платформ або послуг, якими вони користуються.

ЯКІ ПРОБЛЕМИ МОЖУТЬ БУТИ ПОВ'ЯЗАНІ З ЦИФРОВИМ СЛІДОМ?

Цифровий слід людини може бути використаний будь-ким, хто володіє його частиною. Цифровий слід надає профіль про типи послуг або інформації, що пропонуються конкретній особі, про те, яким чином і на яких умовах вона погоджується на них. Це може бути перевагою або серйозним недоліком. З огляду на те, що «інформація - це влада», якщо одна компанія або

особа з поганими намірами володіє частиною нашої інформації, залишеної у вигляді цифрового сліду, це може бути використано зловмисно і надати компанії велику владу та перевагу над особою (клієнтом або користувачем компанії) або потенційною жертвою кіберзлочину. Якщо ми також врахуємо, що досить часто ми не усвідомлюємо слід, який залишаємо за собою, і не маємо засобів, щоб дізнатися про нього, змінити або стерти його, можна стверджувати, що цифрові сліди є надзвичайно важливою інвестицією або потенційною вразливістю.

ЯК ЗМЕНШИТИ ЦИФРОВИЙ СЛІД

Нелегко визначити слід, який ми залишаємо, або зробити його вигідним для нас. Тому єдиний спосіб уникнути негативного впливу нашого цифрового сліду - це зменшити його. Є три способи зробити це:

- Зменшення кількості випадків, коли ми залишаємо слід. Це означає зменшити використання цифрових пристроїв та послуг, підключених до Інтернету. Це не завжди можливо, але є очевидні можливості для цього. Наприклад, не використовувати інтелектуальні та автоматизовані цифрові послуги, які не додають великої цінності, такі як «розумні» колонки або певні додатки.
- Обмеження збору даних шляхом налаштування сервісів, пристроїв і застосунків у максимально обмежувальному режимі. У багатьох випадках це не є ні простим, ні зручним. Наприклад, одним зі способів може бути вимкнення геолокації.
- Ускладнення агрегування даних в один цифровий слід або запобігання поєднанню даних із цього сліду для створення більш цінної, зокрема додаткової, інформації. Цього можна досягти, наприклад, використовуючи різні електронні поштові акаунти для кожного випадку, мети або на різних пристроях. Мета полягає в тому, щоб ускладнити відстеження, тобто щоб інші не могли знайти ідентифіковані сліди, «що носять те саме взуття». Якщо ми завжди використовуємо один і той самий пристрій, один і той самий обліковий запис електронної пошти або профіль, наприклад, наш обліковий запис у Facebook, для входу в служби та веб-сайти, які його використовують і вимагають, ми сприяємо створенню широкого та чіткого сліду про нас.

ЯКІ ПРОБЛЕМИ МОЖУТЬ БУТИ ПОВ'ЯЗАНІ З НЕГАТИВНОЮ РЕПУТАЦІЄЮ ТА ЦИФРОВИМ СЛІДОМ?

Виклики, з якими стикається наша цифрова ідентичність і репутація, пов'язані з тим, що людина може бути правильно і позитивно ідентифікована там, де це необхідно, в той час як сприйняття її іншими може бути несприятливим. Якщо це не так, можливості людини зменшуються, оскільки вона або

неправильно ідентифікована в неправильному місці, або в неправильний час. Її можуть навіть відкинути тільки через її репутацію.

ЯК СТВОРИТИ ГАРНУ ЦИФРОВУ ІДЕНТИЧНІСТЬ ТА РЕПУТАЦІЮ

Мати цифрову ідентичність і підтримувати позитивну репутацію - завдання не з легких. Воно вимагає постійних зусиль, іноді проти течії, і залежить від кількох факторів, зокрема від інших людей. Однак можна виділити чотирнадцять рекомендацій, які допоможуть у цьому. Вони наведені нижче і згруповані за трьома категоріями:

Основи:

1. Будьте особливо обережними з тим, як ви презентуєте себе в Інтернеті. Ваше фото профілю, псевдонім та вступне речення або статус завжди мають бути поважними та позитивними.
2. Звертайте увагу на умови конфіденційності та кібербезпеки на ваших пристроях, у додатках та соціальних мережах. Чим вони суворіші, тим більший контроль.
3. Двічі подумайте, перш ніж опублікувати щось, особливо коли вас охоплюють емоції, такі як гнів або надмірна ейфорія.
4. Перш ніж опублікувати щось, поміркуйте, спрогнозуйте та уявіть, який ефект це може мати, якщо це побачать публічно зараз або в майбутньому.
5. Беріть активну участь, проявляючи своє цифрове громадянство, у правильний, контекстуальний та поінформований спосіб, адже це залишить слід.

Десять рекомендацій для позитивної цифрової репутації або ідентичності

Постійно підтримувати цифрову ідентичність або репутацію може бути досить складно. Особливо, якщо їх цінність і актуальність не легко сприймаються на момент розробки. Ось чому важливо мати чіткі та прості рекомендації, які можна застосовувати, коли це можливо:

1. Будьте вибірковими та скорочуйте обсяг публікацій.
2. Обмежте коло своїх публікацій лише необхідними особами, вибравши відповідні налаштування та канали.
3. Перед публікацією чогось уявіть собі уявну глобальну аудиторію (будь-яку) і безчасовий ефект (завжди).
4. Перш ніж завантажувати будь-який додаток, дізнайтеся, як він обробляє ваші дані.

6. Пам'ятайте, що цифровий слід видалити нелегко, оскільки його можуть зберегти та відтворити інші особи або просто тому, що ви не завжди маєте можливість його видалити.

Стосовно інших:

1. Наполягайте на тому, щоб інші люди поважали вашу приватність. Це найкраща гарантія того, що ви зможете хоча б мінімально керувати своєю цифровою репутацією та ідентичністю.
2. Уникайте відчуття тиску, інерції або необхідності публікувати те, що ви робите. Розумно керуйте тим, чим ви ділитесь в Інтернеті про своє життя, скільки, як і з ким.
3. Пам'ятайте, що те, як люди та платформи, з якими ви взаємодієте, управляють своєю приватністю та кібербезпекою, також впливає на вас.
4. Будьте особливо обережні з тим, що ви публікуєте, якщо це стосується інших людей, особливо якщо їх можна впізнати.

Будьте позитивними та проактивними:

1. Створюйте позитивну цифрову ідентичність та репутацію. Залишайте видимий слід у всьому, чим ви будете пишатися в майбутньому.
2. Практикуйте самоперегляд. Регулярно шукайте себе в Інтернеті (браузері, різні соціальні мережі та платформи тощо) та різними способами, щоб перевірити, що можна знайти про себе.
3. Створіть профіль на платформах, де беруть участь такі люди, як ви. Це може бути корисно для захисту вашої ідентичності та уникнення подробиць особи.
4. Керуйте різними профілями та ідентичностями для конкретних або тимчасових речей. Може бути корисно створювати різне враження в різні моменти.

5. Звертайте увагу та дбайте про свою конфіденційність і кібербезпеку, а також про конфіденційність та кібербезпеку інших осіб, з якими ви взаємодієте.
6. Зберігайте позитивний настрій і тон. Це корисніше для здоров'я і робить вас більш поважними.
7. Уникайте публікацій, коли вас охоплюють сильні або негативні емоції чи почуття.
8. Уникайте непотрібних конфліктів. Немає нічого більш відданого, ніж ворог.
9. Створіть різні профілі для різних середовищ і цілей.
10. Пошукайте себе в соціальних мережах, щоб дізнатися, як вас сприймають.



Як ідентифікувати жертву

Кібербулінг, грумінг та сексторція зазвичай мають дві спільні риси. Перша полягає в тому, що жертви рідко просять про допомогу. Принаймні на початку або доти, доки ситуація не стане екстремальною. Друга спільна риса полягає в тому, що ці злочини, як правило, тривають протягом тривалого часу, можливо, внаслідок вищезазначеного, а також через їх інтенсивність, яка поступово зростає.

Намагаючись виявити такі дії та шукати їхні ранні ознаки, вчителі стикаються з важливим викликом. Ці злочини впливають не тільки на їхніх жертв або тих, хто безпосередньо страждає від них, але й на шкільне середовище та спільноту. Особливо це стосується кібербулінгу.

Завдання вчителів не є легким. Профілі потенційних жертв навіть не є чіткими. У багатьох випадках три різні форми домагань (грумінг, кібербулінг або сексторція) здійснюються дуже обережно, не привертаючи уваги та не залишаючи багато видимих слідів.

Особи, які потрапили в такі ситуації в Інтернеті, виявляють симптоми, схожі на ті, що виникають у людей, які переживають несприятливі емоційні обставини, такі як втрата родича або розрив стосунків: пригнічений настрій, втома, втрата концентрації, апатія, смуток, безсоння, схильність до ізоляції, раптові зміни настрою, тривожність, дратівливість або нервозність тощо. Саме тому немає чітких показників віктимізації, хоча одним з них може бути тривалість або погіршення цих симптомів, що частіше трапляється, коли віктимізація триває довгий час, а не є конкретною травматичною подією.

Коли дитина демонструє підозрілу поведінку, першим кроком має бути виключення будь-яких причин, не пов'язаних з інтернет-жертвами. Другим можливим втручанням може бути перегляд їхньої активності в соціальних мережах, завжди з повагою до їхньої приватності та інтимності, та пошук публічного контенту. Це можна зробити за допомогою пошуку в різних контекстах (веб-сторінки, соціальні мережі тощо), використовуючи різні можливі імена, за якими його можна ідентифікувати, що може дати певні підказки про те, що так сильно на нього впливає. Далі залишається тільки спостерігати і сформулювати гіпотезу про те, що може відбуватися. Наявність складних стосунків з однокласниками або навіть попередні випадки жорстокого поводження можуть вказувати на ймовірний кібербулінг. У випадку, якщо раніше були виявлені симптоми низької самооцінки, можна розглянути можливість пошуку визнання після грумінгу або сексторції. Якщо дитина надмірно використовує та захищає свій мобільний телефон або щось викликає постійну, нагальну або нелогічну потребу мати доступ до Інтернету, це може бути ознакою того, що в її цифровому житті щось не гаразд.

Як завжди, батьки або опікуни повинні бути залучені до ситуації, як тільки ми виявляємо проблему, незалежно від того, чи знайшли ми її джерело. Водночас важливо пояснити їм, як важливо зберігати будь-які докази, які можуть допомогти підкріпити заяву в поліцію, якщо це буде необхідно: повідомлення, знімки екрана тощо. Звичайно, також корисно поділитися з ними нашими знаннями, щоб допомогти їм у їхній роботі з захисту.





**Дидактичний
посібник**

84

Кібербезпека

86

Приватність

88

Кібербулінг

90

Грумінг

92

Секстинг

93

Сексторція

95

Сексуальність та
споживання
порнографії в
Інтернеті

97

Дезінформація та
місінформація в
Інтернеті

99

Кібернасильство
проти жінок і дівчат

101

Цифровий слід,
репутація
та цифрова
ідентичність

Навчальний ресурс: Анімація



КІБЕРБЕЗПЕКА: ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, З ЯКИМ ПОТРІБНО БОРОТИСЯ

Вікова група: **8-12 років**

Вікова група: **13-15 років**

<https://www.youtube.com/watch?v=4aaYIOGpgf8>

Тривалість: 2 хв. 57 с.

ВАРТО ВРАХУВАТИ

- Трояни дозволяють іншому шкідливому програмному забезпеченню проникати у ваш комп'ютер, мобільний телефон або планшет.
- Вони залишаються непомітними та можуть виконувати різні дії, наприклад активувати камеру вашого комп'ютера або викрадати паролі й важливі дані.
- Встановіть антивірусне або інше захисне програмне забезпечення на всі свої пристрої. Підтримуйте операційну систему та програми на пристрої в актуальному стані (оновлюйте їх).
- Завантаження та встановлення нелегального програмного забезпечення може призвести до проблем. Користуйтеся лише офіційними сайтами та застосунками.

Активність: Перегляд анімації та обговорення



Вступ

Це відео у наочній формі, що сприяє кращому запам'ятовуванню, висвітлює деякі ключові питання, пов'язані з троянським шкідливим програмним забезпеченням, одним із найпоширеніших і найнебезпечніших видів шкідливого програмного забезпечення.



Тривалість

- Від 30 до 50 хвилин, залежно від особливостей групи.



Цілі

- Підвищити обізнаність про реальну загрозу, яку становлять шкідливі програми, проти яких необхідно застосовувати активні захисні заходи.
- Дізнатися про основні запобіжні заходи.



Реалізація

Крок 1: Задайте групі кілька запитань: Чи знаєте ви, що таке шкідливе програмне забезпечення або зловмисне програмне забезпечення? Чи знаєте ви, як воно працює? Чи знаєте ви випадки, коли «вірус» спричинив проблеми?

Крок 2: Перегляньте анімацію разом із групою.

Крок 3: Задайте кілька запитань, які допоможуть закріпити основні поняття:

Чому троянські програми небезпечні? Як ви вважаєте, наскільки ймовірно, що ви можете заразитися? Чи вважаєте ви, що троянська програма може взяти під контроль веб-камеру вашого комп'ютера? Як цього уникнути? Чи важливо, щоб ваші друзі також вживали заходів безпеки в Інтернеті?



Навчальний ресурс: Історія



ПРАВИЛА БЕЗПЕКИ ДЛЯ СМАРТФОНІВ

Вікова група: **9-11 років**
Шкільний клас: **4-6 класи**

ВАРТО ВРАХУВАТИ

- Ваш мобільний телефон містить дуже важливу інформацію. Завжди використовуйте графічний ключ або код для блокування екрана. Це перша лінія захисту вашої безпеки та приватності.
- Ваш мобільний телефон зберігає ваші та чужі приватні розмови й зображення. Він також зберігає вашу адресну книгу контактів і дані доступу до соціальних мереж (за умови збереження паролів). Це створює серйозні ризики, такі як крадіжка особистості, злам профілю або порушення приватності.
- У випадках, коли пристрій викрадено чи втрачено, або якщо хтось тимчасово отримав несанкціонований доступ до вашого мобільного телефону, блокування екрана є дуже корисним. Безпека та приватність тісно пов'язані між собою.

Активність: Прочитайте історію та обговоріть її



Вступ

Ця історія розповідає про те, що захист доступу до вашого мобільного телефону відіграє дуже важливу роль.



Тривалість

Від 30 до 50 хвилин, залежно від особливостей групи.



Цілі

- Підвищити обізнаність про важливість захисту доступу до мобільного телефону.
- Визначити необхідність блокування доступу до свого пристрою за допомогою блокування екрана.



Реалізація

Крок 1: Задайте групі кілька загальних питань про те, як вони захищають свої мобільні телефони та їхній вміст, пов'язуючи їх з історією Марійки: Чи втрачали ви коли-небудь свій мобільний телефон? Як ви себе почували?

Крок 2: Прочитайте історію разом з групою принаймні кілька разів.

Крок 3: Після прочитання заохотьте групу до колективного обмірковування, задаючи питання та стимулюючи дискусію. Ось деякі з можливих питань:

Якими можуть бути наслідки того, що інша людина втрутилася у ваш мобільний телефон? Чи зможе вона переглянути ваші зображення? Чи зможе вона отримати доступ до ваших профілів і змінити їх?

Чи вважаєте ви за необхідне автоматично блокувати екран? Скільки секунд ви б встановили для активації блокування екрана?

Марійка завжди була уважною до своєї цифрової безпеки. На свій телефон вона поставила складний графічний ключ, який знала лише вона.

Одного дня, коли дівчина вийшла з класу на перерву, незнайомий зловмисник тихенько зайшов усередину та викрав її телефон. Він сподівався швидко отримати доступ до персональних даних Марійки — повідомлень, фото, акаунтів.

Але щойно він увімкнув телефон, перед ним з'явився складний графічний ключ. Зловмисник водив пальцем по екрану знову і знову, пробував різні комбінації, нервував, сердився — та все марно. Телефон залишався заблокованим, а після кількох невдалих спроб система ще й тимчасово відключила можливість введення.

Зрозумівши, що зламати телефон не вдасться, зловмисник кинув його на парту й поспіхом покинув клас.

Повернувшись після перерви, Марійка помітила свій телефон на місці. Вона одразу зрозуміла: хтось намагався ним скористатися. Але завдяки надійному графічному ключу жодні її дані не постраждали.

Марійка посміхнулася — захист таки працює. І відтоді вона ще уважніше ставилася до безпеки своїх цифрових пристроїв.

Приватність

Навчальний ресурс: Анімація

Активність: Перегляд анімації та обговорення



ПРИВАТНІСТЬ – СКАРБ, ЯКИЙ ПОТРІБНО ЗАХИЩАТИ

Вікова група: 10-12 років
Шкільний клас: 5-7 класи

<https://www.youtube.com/watch?v=xX-3rMe4eFs>

Тривалість: 2 хв. 11 с

ВАРТО ВРАХУВАТИ

- Якщо ваш мобільний телефон має камеру та GPS, ваші фотографії можуть розкривати більше інформації, ніж ви думаєте.
- Вимикайте визначення місцезнаходження (геолокацію) для фото та відео, які ви публікуєте з телефону.
- Це важливо для вашого власного захисту та захисту інших.

Непомітно для нас мобільні телефони можуть додавати до нашої комунікації додаткову інформацію у вигляді метаданих, які часто містять дані про геолокацію. Зазвичай це відбувається під час створення фотографії, коли фіксується точне місце, де було зроблено знімок або відео. Деякі вебсервери видаляють геолокацію під час завантаження файлів, інші – ні. Крім метаданих, у самих зображеннях може бути багато деталей, які дозволяють визначити місцезнаходження людини.



Вступ

Це відео привертає увагу до даних, які іноді ненавмисно передаються разом із зображенням, найчастіше це місце, де було зроблено знімок.



Тривалість

Від 30 до 50 хвилин, залежно від особливостей групи.



Цілі

- Стимулювати критичне мислення щодо того, яка інформація, більш-менш несвідомо, передається в будь-який момент часу.
- Підвищити обізнаність про потенційний ризик для конфіденційності та безпеки при обміні зображеннями, що містять дані геолокації.



Реалізація

Крок 1: Задайте групі кілька запитань: Чи знаєте ви, що таке геолокація?

Що таке метадані? Чи знаєте ви, де знаходяться налаштування, пов'язані з використанням місцезнаходження вашого телефону? Чи знаєте ви, які інші програми можуть отримати доступ до вашого місцезнаходження або показувати його під час використання?

Крок 2: Перегляньте анімацію разом із групою.

Крок 3: Задайте кілька питань, пов'язаних із конфіденційністю та даними про місцезнаходження:

Які ще ситуації, на вашу думку, можуть бути небезпечними, якщо на фотографії видно ваше місцезнаходження? Що може статися, якщо фотографія, на якій видно місцезнаходження, буде надіслана або опублікована відкрито, так що її зможе побачити будь-хто? Як можна налаштувати доступ та використання налаштувань місцезнаходження для програм, які їх використовують? Якщо ви не знаєте, як це зробити, як можна це дізнатися?



Приватність

Навчальний ресурс: Історія



У СОЦІАЛЬНИХ МЕРЕЖАХ НА ВАШУ ОНЛАЙН-ПРИВАТНІСТЬ МОЖУТЬ ВПЛИВАТИ ІНШІ. ПРИВАТНІСТЬ ІНШИХ ТАКОЖ ЗАЛЕЖИТЬ ВІД ВАС

Вікова група: 10-12 років
Шкільний клас: 5-7 класи

ВАРТО ВРАХУВАТИ

«Те, що відомо про вас, також залежить від інших людей. Інші люди також покладаються на вас у дотриманні їхньої приватності».

Активність: Прочитайте історію та обговоріть її



Вступ

Ця історія з серії «Приватність» розповідає про розмову між двома людьми, в якій один з них змушує іншого задуматися про те, які зображення вони публікують, де вони їх публікують, і як це може вплинути на їхню власну конфіденційність та конфіденційність інших.



Тривалість

Від 30 до 50 хвилин, залежно від особливостей групи.



Цілі

- Підкреслити необхідність заздалегідь обдумати публікацію зображення в соціальних мережах.
- Показати, що зображення в соціальній мережі можуть побачити несподівані люди або люди, яких ми насправді не знаємо.
- Підкреслити, що поведінка з зображеннями в соціальних мережах може мати наслідки для приватного життя інших людей і що саме з цієї причини необхідно активно захищати власне приватне життя.



Реалізація

Крок 1: Задайте групі кілька відкритих питань, щоб вони пояснили свої критерії при публікації зображень: які зображення ви зазвичай публікуєте в соціальних мережах? Ви публікуєте їх публічно чи приватно? А як це роблять ваші друзі? Чи публікували вони коли-небудь фотографії або відео з вами, які вас турбували?

Крок 2: Прочитайте історію разом із групою.

Крок 3: Після прочитання історії заохотьте групу до обговорення, задавши такі питання:

- Чи вважаєте ви, що зображення в приватній зоні соціальної мережі є безпечним?
- Чи питаєте ви своїх друзів, чи діляться вони своїми пароллями до соціальних мереж з іншими людьми? Чи ділитесь ви ними?
- Чи замислювалися ви коли-небудь над тим, скільки конфіденційних зображень ви зберігаєте на своєму мобільному телефоні? Що станеться, якщо ви його загубите? А що, якщо людина, яка загубила телефон, раніше була вам довірена особою, якій ви надали приватні зображення?

Вечірка у друзів була дуже веселою: музика, жарти, танці та безліч кумедних моментів. Хлопці та дівчата майже безперервно фотографували — робили смішні гримаси, стрибали, влаштовували імпровізовані конкурси. На телефони накопичилася ціла галерея яскравих знімків.

Після вечірки один із друзів, Андрій, вирішив поділитися найсмішнішими фотографіями на своїй сторінці в соцмережі. Він вибрав кілька знімків і позначив усіх, хто був поруч — він хотів, щоб усі отримали згадки та лайки.

Коли Андрій натиснув «опублікувати», його мама випадково була поруч. Поглянувши на екран, вона лагідно попросила сина зупинитися.

«Подивись, — сказала вона тихо. — Ці фотографії можуть бути смішними для тебе, але чи всі хочуть, щоб їх бачили такими? У соціальних мережах інші люди можуть впливати на твою приватність, але ти також впливаєш на приватність тих, хто тебе оточує». Андрій замислився. Він дійсно не питав своїх друзів, чи хочуть вони, щоб ці фотографії стали публічними.

Андрій зрозумів важливе правило:

у соціальних мережах ми відповідальні не тільки за себе, але й за людей навколо нас.

Відтоді він завжди питав дозволу, перш ніж тегати когось або публікувати фотографії з друзями.



Навчальний ресурс: Анімація



ДЕСЯТЬ ПРАВИЛ ПОЗИТИВНОГО КІБЕРСПІВІСНУВАННЯ ТА ЗАПОБІГАННЯ ЦИФРОВОМУ НАСИЛЬСТВУ

Вікова група: **12-14 років**
Шкільний клас: **6-8 класи**

https://www.youtube.com/watch?v=_DF_x1SHTEg

Тривалість: 5 хв. 33 с.

Активність: Перегляд анімації та обговорення



Вступ

Цей анімаційний фільм показує різні фактори, які сприяють створенню позитивної цифрової атмосфери і, отже, зменшенню ймовірності насильницької поведінки.



Тривалість

Від 30 до 50 хвилин, залежно від особливостей групи.



Цілі

- Дізнатися про концепцію позитивного співіснування в Інтернеті та різні прояви насильства в мережі.
- Підвищити обізнаність про необхідність активної участі для запобігання погіршенню клімату співіснування та його поліпшення.
- Визначити, які цінності, ставлення та навички можуть сприяти та підтримувати гарне співіснування в кіберпросторі.



Реалізація

Крок 1: Поставте групі кілька початкових запитань і завдань: Що таке позитивне співіснування? Чи знаєте ви приклади хорошого та поганого співіснування в класі? Чи можете ви визначити наслідки кожного з них? Хто виграє від хорошого співіснування?

Крок 2: Перегляньте анімацію разом із групою принаймні кілька разів.

Крок 3: Почніть дискусію, задавши питання про кожне з десяти рекомендованих правил:

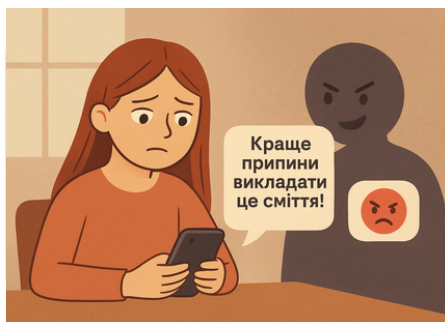
Чому вони важливі? Чи можете ви навести приклад того, що відбувається, коли ці правила не дотримуються? Чому це відбувається? Як ми можемо застосувати ці поради на практиці? Які інші дії ви могли б порекомендувати?

ВАРТО ВРАХУВАТИ

- Будьте обережні з даними інших людей. Особисті дані інших не належать вам. Уникайте використання або публікації їхніх фотографій без дозволу.
- Дискретність. Не розкривайте приватні справи інших людей, навіть якщо вам здається, що це їх не турбуватиме.
- Повага й обережність. В онлайн-просторі слід спілкуватися з іншими дуже уважно та з повагою. Вас можуть неправильно зрозуміти, або ж людина може мати поганий день, що вплине на сприйняття ваших коментарів.
- Глобальне бачення та уява. Будьте дуже обережні з жартами в публічному просторі. Навіть якщо людина, про яку йдеться, знає вас і не бачить у цьому шкоди, інші можуть сприйняти це інакше.
- Спостережливість і емпатія. Потрапляючи в нове середовище, кілька днів поспостерігайте, перш ніж діяти. Це може бути не те місце або не ті люди, якими ви їх уявляли.
- Позитивне управління емоціями. Якщо хтось вас роздратував, зробіть паузу. Можливо, сталося непорозуміння або шкода була ненавмисною.
- Залученість і чутливість. Якщо ви бачите, що хтось поводить себе необачно, повідомте про свій дискомфорт у тактовний спосіб.
- Активна та конструктивна участь. Якщо ви є частиною спільноти чи мережі, намагайтеся брати участь і робити позитивний внесок.
- Толерантність і участь. Поважайте думки інших і висловлюйте власні з повагою.
- Солідарність. Якщо ви бачите, що з кимось поводяться несправедливо або знущаються, намагайтеся допомогти, уникаючи поспішних висновків і не створюючи додаткових конфліктів.

Кібербулінг

Навчальний ресурс: Історія



ЯК БОРОТИСЯ З КІБЕРБУЛІНГОМ? ІГНОРУЙТЕ, БЛОКУЙТЕ, ПРОСИТЬ ДОПОМОГИ ТА ПОВІДОМЛЯЙТЕ ПРО ЦЕ

Вікова група: 12-14 років

Шкільний клас: 6-8 класи

ВАРТО ВРАХУВАТИ

Чотири основні кроки, яких слід дотримуватися у випадку переслідування або булінгу:

- Ігнорувати: не варто відповідати на образи чи провокації.
- Заблокувати: якщо переслідування продовжується, спробуйте заблокувати цю людину, щоб уникнути контакту.
- Попросити про допомогу: якщо ви відчуваєте, що переслідування триває або є серйозним чи небезпечним, зверніться по допомогу.
- Повідомити: повідомлення означає інформування відповідних органів. Це можуть бути правоохоронні органи. Якщо ви звертаєтесь до поліції, важливо надати докази пережитого переслідування та будь-які підтвердження, що можуть вказувати на ймовірного кривдника.

Активність: Прочитайте історію та обговоріть її



Вступ

Історія відображає незручну ситуацію, яка переростає в булінг, і те, як головна героїня вирішує звернутися за допомогою до дорослого, якому довіряє, наприклад, до свого батька.



Тривалість

Від 30 до 50 хвилин, залежно від особливостей групи.



Цілі

- Дізнатися, як поведуться деякі хулігани, і як найкраще поводитися з ними на різних етапах і за різним ступенем серйозності булінгу.
- Визначити осіб, які несуть обов'язки по догляду (батьки, вихователі тощо), як союзників, незалежно від того, якою була поведінка (обережною чи ні).



Реалізація

Крок 1: Задайте групі початкові запитання щодо деяких питань, пов'язаних із змістом історії: Чи були ви коли-небудь жертвою булінгу в Інтернеті? Яким чином? Хто це був? Як ви себе почували? Що сталося в результаті?

Крок 2: Прочитайте історію разом з групою принаймні кілька разів.

Крок 3: Після прочитання історії запропонуйте групі спільно її обговорити, ставлячи запитання та заохочуючи до дискусії. Серед можливих запитань можуть бути такі:

- Як почувалася головна героїня? Чи правильно вона вчинила? Чому?
- Як ми можемо відрізнити погрози від жартів? Коли жарти можна вважати небезпечними?
- Хто з неї змушався? Чому? Що може статися з ним, якщо його особу буде виявлено?
- Що робить її батько, коли дізнається про проблему? Чи злиться він?
- Окрім допомоги, яку вона може отримати, чи варто вжити додаткових заходів? Якщо так, то яких саме?

У восьмому класі Оленка була спокійною дівчинкою, яка ніколи ні з ким не сварилася. Вона любила малювати і іноді публікувала свої роботи в соціальних мережах. Одного дня під її новою роботою з'явився дивний коментар від анонімного профілю:

«Ти думаєш, хтось це дивиться? Смішно».

Спочатку Оленка вирішила, що це просто нешкідливий жарт — хтось намагається привернути увагу. Але через кілька днів з'явилися нові коментарі:

«Краще припини публікувати це сміття».

«Ніхто тебе не підтримує».

Повідомлення надходили пізно ввечері, і з кожним днем Оленка почувалася все гірше і гірше.

Вона не знала, хто це був, але їй здавалося, ніби всі сміються з неї.

Одного вечора батько помітив, що дочка уникає свого телефону.

Він тихо сів поруч із нею і запитав, чи все гаразд.

Оленка не витримала і показала йому коментарі.

Вона боялася, що батько розсердиться, але він уважно вислухав її і сказав:

«Це не твоя вина. Ми разом розберемося з цим».

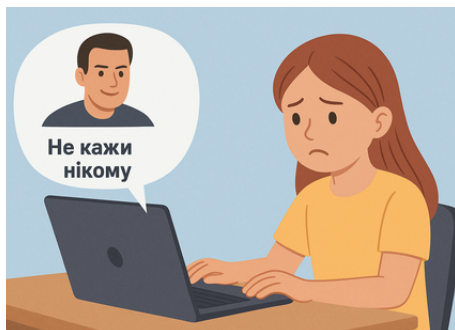
Наступного дня вони зв'язалися зі шкільним психологом та адміністрацією. Виявилось, що анонімний акаунт належав однокласнику, який, за його словами, хотів «пожартувати» і «трохи посміятися».

Але коли його особистість була розкрита, він зрозумів, що жарти мають наслідки: розмова з батьками, попередження від школи та обов'язкова зустріч із психологом.

Оленка відчувала полегшення, коли відчувала підтримку дорослих.

Але вона також зрозуміла важливу річ: жарти в Інтернеті можуть глибоко образити, і те, що сказано в мережі, не зникає безслідно.

Навчальний ресурс: Анімація



ГРУМІНГ, СТРАТЕГІЯ КІБЕРСТАЛКІНГУ

Вікова група: **12-16 років**
Шкільний клас: **6-10 класи**

<https://www.youtube.com/watch?v=MixYWWS8mGk>

Тривалість: 3 хв. 12 с.

ВАРТО ВРАХУВАТИ

Що це таке?

Грумінг — це спосіб, за допомогою якого педофіли завойовують довіру дітей (дівчат і хлопців), щоб отримати доступ до сексуальної експлуатації або вимагати інтимні матеріали.

Як це працює?

З часом вимоги стають дедалі більшими й супроводжуються шантажем: фотографії, відео, зустрічі тощо. Це не зупиняється само по собі.

Якої шкоди це завдає?

Шкода може бути надзвичайно серйозною, навіть якщо не було фізичного контакту. Страждання є глибокими й дуже болісними. Грумінг потрібно зупинити якомога швидше.

Як уникнути грумінгу?

Захищайте свою приватність і особисту інформацію. Не довіряйте тим, кого ви насправді не знаєте.

Що слід робити?

Якнайшвидше звернутися по допомогу. Дорослі повинні вас захистити. Головне для дорослих — це безпека та благополуччя дітей, а не те, що сталося або що дитина зробила.



Активність: Перегляд анімації та обговорення



Вступ

Цей мультфільм описує, як діють сексуальні хижаки в Інтернеті, та надає рекомендації щодо запобігання таким ситуаціям і реагування на них.



Тривалість

Від 30 до 50 хвилин, залежно від особливостей групи.



Цілі

- Дізнатися, як діють сексуальні кіберзлочинці та які наслідки має їхнє переслідування.
- Визначити ознаки, які можуть допомогти виявити стратегію інтернет-грумінгу на ранній стадії за допомогою критичного мислення та самозахисту.
- Підвищити обізнаність про те, що єдиний вихід із такої ситуації — звернутися за допомогою до дорослого, якому довіряєш.



Реалізація

Крок 1: Поставте групі кілька початкових запитань і завдань: Скільки людей ви зустріли в Інтернеті? Звідки ви знаєте, що вони є тими, за кого себе видають? Навіть якщо це друзі ваших друзів, звідки ви знаєте, що ваш друг добре їх знає або що вони дійсно їх знають?

Крок 2: Перегляньте анімацію з групою принаймні кілька разів. Ви можете приділити додатковий час кожній з її частин.

Крок 3: Почніть обговорення, задаючи питання, пов'язані з різними нюансами анімації.

Що змушує вас довіряти людям, яких ви зустрічаєте в Інтернеті? Чому?

Як ми можемо дізнатися, чи правдиві слова людей або інформація, яку вони нам надають?

Чи варто зберігати таємницю людини, яку ми знаємо лише в Інтернеті? Що вона може приховувати, якщо просить нас нікому не розповідати? Чи варто домовлятися з людьми, які нас шантажують? Чому? Які шанси самостійно вийти із ситуації шантажу чи булінгу без сторонньої допомоги? Яким може бути рішення, якщо вас шантажують або цькують? Якби ви були батьками дитини, яка зазнає булінгу, що б ви зробили, якби вона поділилася з вами цією проблемою?



Навчальний ресурс: Історія



WINDOWS, СПРАВЖНЯ ПРИГОДА У ВІРТУАЛЬНОМУ СВІТІ

Вікова група: 8-12 років

Вікова група: 13-15 років

ВАРТО ВРАХУВАТИ

Головна героїня цієї історії розмірковує, кому присвятити свій час і увагу. Зокрема, є двоє хлопців, які хочуть спілкуватися з нею: один — її однокласник, а інший, з яким вона не знайома особисто, живе за тисячі кілометрів від неї.

Вона обговорює свої переживання з бабусяю та друзями й зрештою вирішує обрати людей, які поруч із нею — тих, кого вона справді знає і кому довіряє.

Критичне мислення, асертивність, емпатія тощо — усе це навички, які вона застосовує, щоб прийняти непросте рішення, яке стосується кількох людей.

Активність: Прочитайте історію та обговоріть її



Вступ

Ця історія висвітлює деякі цікаві аспекти, такі як довірчі стосунки як з незнайомцями, так і з близькими дорослими, які не знають про Інтернет та його потенціал. На тлі цього розглядається проблема кібербулінгу та того, як приймати безпечні рішення за підтримки родини, відмовляючись від обіцянок і зовнішніх проявів.



Тривалість

Від 30 до 50 хвилин, залежно від особливостей групи.



Цілі

- Застосувати критичне мислення щодо того, що ми робимо в Інтернеті та з ким, у порівнянні з можливостями в офлайн.
- Визначити дорослих, яким можна довіряти, як осіб, до яких можна звернутися за допомогою у питаннях, пов'язаних з життям в Інтернеті.



Реалізація

Після прочитання історії заохочуйте обговорення в класі, задаючи питання, пов'язані з різними критичними аспектами, що викликають інтерес у цій пригоді:

- Хто такі два друга Марти? Що ми про них знаємо?
- Якби вам довелося вибирати між двома її друзями, кого б ви вибрали? Чому?
- Чи вважаєте ви, що бабуся Марти може допомогти їй прийняти рішення щодо її життя в Інтернеті?
- Чи вважаєте ви, що іноді є люди, які живуть фальшивим, нереальним життям в Інтернеті? Чи знаєте ви таких людей?
- Як ви думаєте, хлопець зі Стокгольма є тим, за кого себе видає? Чому? Чи було б добре, якби Марта це перевірила? Чи могла б вона це зробити? Як?
- Як ви вважаєте, Марта вчинила правильно? Чи врахувала вона почуття інших людей? Якщо хтось засмутиться через її рішення та поведінку, що, на вашу думку, вона повинна зробити?

Мене звали Марта. Я часто спілкуюся онлайн — граю, сиджу в соцмережах, знайомлюсь з новими людьми. Одного разу я розповіла бабусі, що маю друга з-за кордону. Вона лише зітхнула й сказала, що онлайн-дружба — це «вигадка». Я посміхнулась, але трохи засмутилась.

Його звали Даніель. Ми листувалися вже кілька місяців, і мені здавалося, що він дуже мене розуміє.

Мої друзі Оленка і Назар теж знали про нього. Назар не поділяв мого захоплення:

— Ти не знаєш, хто він насправді, — повторював він.

Одного вечора Назар написав:

“Марто, завтра зранку подивись у вікно. Потрібно поговорити.”

Наступного дня я виглянула — Назар стояв знизу й хвилювався.

— Марто, — сказав він, — інтернет — це добре, але там легко заплутатися. Реальні друзі — поруч. Я... хочу бути для тебе важливим не тільки онлайн.

Мені стало тепло й ніяково водночас. Того ж вечора я отримала два повідомлення:

— від Назара: “Ходимо після уроків на морозиво?”

— від Даніеля: “Шкода, що ти не поруч. Ми б класно провели час.”

І я раптом зрозуміла, що між тим, що виглядає ідеальним у чаті, та тим, що відбувається поруч із тобою, — величезна різниця.

Наступного дня я сказала бабусі:

— Онлайн-дружба може бути крутою. Але справжні друзі — це ті, хто поруч, хто може подзвонити у двері, а не просто написати в чат.

Секстинг

Навчальний ресурс: Анімація



СЕКСТИНГ — ЦЕ РИЗИКОВАНА ПРАКТИКА...

Вікова група: **15-18 років**
Шкільний клас: **9-12 класи**

<https://www.youtube.com/watch?v=Tf6B69-yVak>

Тривалість: 3 хв. 12 с

ВАРТО ВРАХУВАТИ

Надсилання інтимних зображень — це ризикозна практика. Добре подумайте перед тим, як це зробити, адже інші можуть завдати вам глибокого болю або серйозної шкоди.

Активність: Перегляд анімації та обговорення



Вступ

Анімація показує, наскільки ризикованою є практика секстингу, особливо з людьми, довіра до яких ще не перевірена.



Тривалість

Від 20 до 30 хвилин, залежно від особливостей групи.



Цілі

- Поінформувати про те, що секстинг є ризикованою практикою, яку слід ретельно обмірковувати.
- Взяти до уваги, що секстинг з іншою особою не знижує рівень ризику, а, навпаки, може бути додатковим фактором тиску.
- Визначити один із найпоширеніших способів, за допомогою якого секстинг пов'язаний із критичною ситуацією для секстера.



Реалізація

Крок 1: Задайте групі відкриті запитання: Чи знаєте ви людей, які займалися секстингом? З ким і в яких ситуаціях люди зазвичай займаються секстингом? Чи завжди це безпечно, чи можуть бути різні рівні ризику? Чому?

Крок 2: Перегляньте анімацію разом з групою принаймні кілька разів. Після першого перегляду відео заохочуйте учасників висловлювати коментарі, які допоможуть переглянути його вдруге з більш проникливим і критичним поглядом.

Крок 3: Заохочуйте дискусію, задаючи питання, пов'язані з ситуацією, зображеною в цьому відео.

Чи знали один одного головні герої цієї пригоди? Вони були просто друзями чи хлопцем і дівчиною? Чому почалася розсилка інтимних фотографій? Чи доречно надсилати інтимні фотографії тому, хто надіслав їх вам? Чи це обов'язково? З якими людьми, на вашу думку, безпечніше займатися секстингом? З якими людьми, на вашу думку, це небезпечно? Що ви можете зробити, якщо хтось вимагає від вас інтимне фото? Чи рекомендували б ви секстинг? Чому? Які наслідки може мати секстинг для людини, яка ним займається?



Сексторція

Навчальний ресурс: Анімація



СЕКТОРЦІЯ, ШАНТАЖ ІНТИМНИМИ ЗОБРАЖЕННЯМИ

Вікова група: 11–12

Вікова група: 13–15

<https://www.youtube.com/watch?v=MBJ0fgXhWMI>

Тривалість: 4' 43"

ВАРТО ВРАХУВАТИ

Будь-яке зображення, що відображається на екрані, можна скопіювати. Ретельно обмірковуюте свої дії перед веб-камерою та ступінь довіри до людини, яка знаходиться на іншому боці.

Молодий чоловік піддається на спокус жінки, яку він зустрів в Інтернеті. Вона заохочує його до кіберсексу. Коли він відповідає на її загравання, показуючи себе оголеним перед камерою комп'ютера, вона записує його і шантажує, погрожуючи показати відео іншим людям. Це тип пастки і кіберзлочину, який часто здійснюють організовані банди.

Завдання: Перегляд анімації та обговорення



Вступ

Ця анімаційна пригода зображує сексторцію з метою отримання фінансової вигоди, коли молодий чоловік потрапляє в пастку молодої жінки, яку він зустрічає в Інтернеті.



Тривалість

Від 30 до 50 хвилин, залежно від особливостей групи.



Цілі

Поміркувати над межами стосунків із незнайомцями через Інтернет та розривом, який іноді існує між перевагами та ризиками.

- Припустити, що все, що відображається на екрані, може бути записано, перетворюючи щось короткочасне на постійне, а приватне – на публічне.
- Визначити найпоширеніші практики сексторції серед чоловіків та молодих людей різного віку.



Реалізація

Крок 1: Задайте групі відкриті запитання: Чи знаєте ви, що таке кіберсекс? Чи знаєте ви когось, хто займався кіберсексом? Чи вважаєте ви це ризикованим? Чому?

Крок 2: Перегляньте анімацію з групою у двох частинах, тобто зупиніться на третій хвилині, до того, як історія набуває несподіваного повороту. Під час цієї короткої паузи попросіть групу оцінити те, що вони побачили, і що, на їхню думку, відбудеться далі.

Крок 3: Завершіть заняття, запропонувавши групі обговорити побачене. Для цього можна знову показати анімацію, цього разу без зупинок. Можна поставити такі запитання:

Чи можна записати будь-яке зображення, що відображається на екрані? Чи ми дійсно знаємо, хто знаходиться по той бік веб-камери комп'ютера? Чи безпечний такий вид кіберсексу? Як можна перевірити зображення людини по той бік і переконатися, що це не попередній відеозапис? Що ми можемо порадити людині, яка стала жертвою такого виду кіберзлочину?



Сексторція

Навчальний ресурс: Історія



СЕКСТОРЦІЯ ТА СЕКСУАЛЬНИЙ ШАНТАЖ ЧЕРЕЗ ВЕБ-КАМЕРУ

Вікова група: 11-12 років

Вікова група: 13-15 років

Активність: Прочитайте історію та обговоріть її



Вступ

Ця історія дуже наочно описує, як легко стати жертвою онлайн-шахрайства, і пропонує вам подумати про можливі наміри та наслідки такого шахрайства.



Тривалість

Від 30 до 50 хвилин, залежно від особливостей групи.



Цілі

- Визначити сексторцію як загрозу, яку можна стимулювати за допомогою дуже різних стратегій.
- Підвищити обізнаність про ризик оприлюднення інтимних зображень через камеру комп'ютера.



Реалізація

Після прочитання історії використовуйте наступні питання для стимулювання роздумів:

- Чи вважаєте ви, що подібні події можуть трапитися?
- Якою може бути мета людини, яка здійснює обман?
- Як можна уникнути такого роду обману?
- Що може статися, якщо інтимні зображення, які людина показала комусь у певний момент, будуть записані веб-камерою комп'ютера або мобільного телефону?

Після питань можна підбити підсумки, досягнуті під час обговорення.

Артем одного вечора випадково натрапив на онлайн-чат знайомств. Там він познайомився з дівчиною, яка представилася Аліною. Вона була дуже привабливою й швидко запропонувала додати її в друзі в соціальній мережі.

Спілкування стало регулярним: вони листувалися, іноді навіть говорили по відеозв'язку. Артему здавалося, що він знайшов нову подругу.

Та одного дня «Аліна» надіслала Артему відео. На ньому був він сам — у власній кімнаті, роздягнений, у момент, коли він думав, що камеру вимкнено. Дівчина написала:

— Якщо не заплатиш мені гроші, я надішлю це відео всім твоїм друзям і однокласникам.

Артем відчув сильний страх, сором і паніку. Але замість того, щоб відразу виконати її вимоги, він зібрався з думками й розповів про це старшому братові. Разом вони звернулися до батьків, а ті — до кіберполіції та служби підтримки соцмережі.

Вже наступного дня акаунт «Аліни» було заблоковано. Виявилося, що це шахрай, який так само шантажував інших дітей.

Артем зрозумів головне: ніколи не варто надсилати чи показувати перед камерою нічого інтимного, навіть якщо здається, що співрозмовнику можна довіряти. А якщо хтось погрожує — треба говорити дорослим і не мовчати.

Сексуальність та споживання порнографії в Інтернеті

Навчальний ресурс: Анімація



ПІДЛІТКОВИЙ ВІК, СЕКСУАЛЬНІСТЬ ТА СПОЖИВАННЯ ПОРНОГРАФІЇ В ІНТЕРНЕТІ

Вікова група: **13-18 років**

Шкільний клас: **8-12 класи**

<https://www.youtube.com/watch?v=9AugMhC9xO4>

Тривалість: 2 хв. 25 с.

ВАРТО ВРАХУВАТИ

Сексуальність та споживання порнографії. Чи є Інтернет надійним джерелом інформації?

Не використовуйте порнографію для відповідей на будь-які питання про секс. Порнографія:

- Показує відносини домінування-підкорення та містить насильство.
- Показує чоловіків і особливо жінок як об'єкти для задоволення інших.
- Вона не відображає почуттів чи емоцій.

Активність: Перегляд анімації та обговорення



Вступ

ВАЖЛИВЕ ПОВІДОМЛЕННЯ: Фасилітатор спочатку детально оцінить зміст і обсяг цього ресурсу, а також його відповідність цільовій аудиторії дітей. У цій анімації головний герой не впевнений, як підійти до питання сексуальних стосунків. Для цього він звертається до Інтернету в пошуках інформації, але це складно, оскільки в цьому питанні існує багато розбіжностей і немає надійних джерел. Він вирішує звернутися за підтримкою до своїх батьків, щоб розвіяти свої сумніви і побоювання.



Тривалість

Від 30 до 50 хвилин, залежно від розміру групи та рівня її залученості.



Цілі

- Поміркувати над джерелами інформації про секс у підлітковому віці.
- Сприяти сприйняттю сім'ї як надійного освітнього суб'єкта в питаннях здорових стосунків та сексуальності.
- Ставити під сумнів моделі сексуальних стосунків, які пропагує мейнстрім-порнографія.



Реалізація

Крок 1: Перегляньте анімацію разом з групою, а потім надайте слово учням, які повинні пояснити історію своїми словами.

Крок 2: Дітей просять пояснити переваги та недоліки пошуку інформації про сексуальні стосунки в різних джерелах: друзі, родина, Інтернет. Вчитель розгляне ті думки, які є менш доречними, та виділить ті, що є більш точними, одночасно ставлячи нові запитання з цієї теми. Це може бути пов'язано з темою дезінформації та критичного мислення.

Крок 3: Щоб завершити дискусію, зосередьтеся на розвінчанні моделей, зображених у порнографії, наголошуючи на трьох моментах:

- Секс — це повага і взаємна турбота, а не насильство і біль.
- Секс є реальним і не містить вигаданих прийомів (тіла, розміри, тривалість тощо), які показуються в порнографії.
- Секс є здоровим, на відміну від ризикованих практик, зображених у порнографії.



Сексуальність та споживання порнографії в Інтернеті

Навчальний ресурс: Історія



ЗГОДА — ЯК ЧАШКА ЧАЮ: ПРОСТО Й ЗРОЗУМІЛО

Вікова група: 11-12 років

Вікова група: 13-15 років

ВАРТО ВРАХУВАТИ

Згода — це найважливіше:

- Її не можна визначати як відсутність відмови.
- Вона має бути чіткою та однозначною.
- Її можна відкликати в будь-який момент.

Активність: Прочитайте історію та обговоріть її



Вступ

ВАЖЛИВЕ ПОВІДОМЛЕННЯ: Фасилітатор повинен адаптувати приклад з чашкою чаю до конкретного завдання між двома людьми, яке є відповідним і значущим для віку дітей, зосередившись на заохоченні емпатії та поваги до рішення та бажань іншої людини, яка бере участь у завданні.



Тривалість

Від 30 до 50 хвилин, залежно від розміру групи та рівня її участі.



Цілі

- Зрозуміти повне значення слова «згода» та його зв'язок із свободою, повагою та правами людини.
- Глибше дослідити необхідність того, щоб згода була явною, чіткою, вільною і завжди поважалася.
- Завжди і за будь-яких обставин усвідомлювати обов'язок отримувати згоду, а також право відмовляти в ній.
- Встановити зв'язок між згодою та міжособистісними стосунками, а також, у відповідних випадках, між подружжям.



Реалізація

Крок 1: Поставте низку питань, щоб зосередити увагу на понятті згоди у всіх видах сексуальних стосунків або контактів. Групі буде поставлено низку питань: Що таке згода? Про що можна або слід просити згоди? Чому згода є необхідною? Чи завжди згода виражається чітко? Як? Що таке відмова? Чи відсутність згоди рівнозначна відмові? У чому полягає різниця між згодою та домовленістю між двома людьми? Який варіант є кращим для обох сторін? Чи необхідна згода між партнерами? Таким чином, група буде готова переглянути відео, маючи на увазі ці підказки, над якими вони розмірковували.

Крок 2: Прочитайте історію попросивши групу спочатку спробувати визначити деякі ключові питання, які щойно обговорювалися.

Крок 3: Пов'яжіть поняття, проаналізовані на кроці 1, з конкретними моментами в історії і, нарешті, встановіть зв'язок з інтимними стосунками, якщо вік дітей дозволяє це зробити.

Олексій і Марина давно дружили. Одного вечора вони гуляли парком після школи. Марина запропонувала сісти на лавку та подивитися зірки. Вони сміялися, розповідали історії та поступово сili ближче один до одного.

Олексій відчував, що хотів би обійняти Марину, але він згадав, що згода важлива. Тому він тихо запитав:

— Тобі буде комфортно, якщо я обійму тебе?

Марина трохи посміхнулася і відповіла:

— Так, я не проти, але не дуже міцно.

Вони обійнялися, і обидва почувалися добре. Пізніше Марина відчула, що їй потрібно трохи більше простору, і сказала:

— Мені зараз трохи некомфортно, давай трохи відсторонемося.

Олексій одразу відступив і запитав, чи все гаразд. Вони продовжили сидіти поруч, розмовляти, і обоє відчували повагу та розуміння.



Дезінформація та місінформація в Інтернеті

Навчальний ресурс: Анімація



ДЕЗІНФОРМАЦІЯ ТА ЇЇ ПРОБЛЕМИ

Вікова група: 9-14 років

Шкільний клас: 4-8 класи

<https://www.youtube.com/watch?v=yRRobD7syPo>

Тривалість: 3 хв. 43 с.

ВАРТО ВРАХУВАТИ

Фейки та неправдива інформація:

- Відволікають вашу увагу.
- Забирають ваш час.
- Дезінформують вас.
- Впливають на свободу вашої думки та можуть спонукати до неправильних рішень або формування хибних переконань.
- Можуть зробити вас частиною ланцюга поширення дезінформації.

Фейки та неправдива інформація можуть завдати серйозної шкоди людям. Не дозволяйте використовувати себе та втягувати в ланцюг поширення. Перш ніж щось поширювати, перевірте, чи є інформація правдивою та вартою уваги.

Активність: Перегляд анімації та обговорення



Вступ

Ця анімаційна історія ілюструє, як неправдива інформація може впливати на конкретні аспекти нашого життя і як ми можемо ненавмисно стати розповсюджувачами та співучасниками дезінформації.



Тривалість

40–50 хвилин, залежно від розміру групи та рівня її залученості.



Цілі

- Підкреслити, що дезінформація є реальною і актуальною загрозою, яка може вплинути на кожного з нас різними способами.
- Підвищити обізнаність про роль, яку кожен відіграє у боротьбі з дезінформацією, особливо з метою уникнення того, щоб стати суб'єктом її поширення.
- Визначте, в яких випадках люди найбільш вразливі до дезінформації.



Реалізація

Крок 1: Перегляньте відео двічі поспіль, щоб переконатися, що воно правильно зрозуміле, оскільки це анімація з різними нюансами, які потрібно оцінити. Попросіть дітей поділитися своїми враженнями про те, що вони побачили, і чи вірять вони, що такі речі можуть трапитися, запропонувавши їм розповісти про будь-які фейкові новини, про які вони знають.

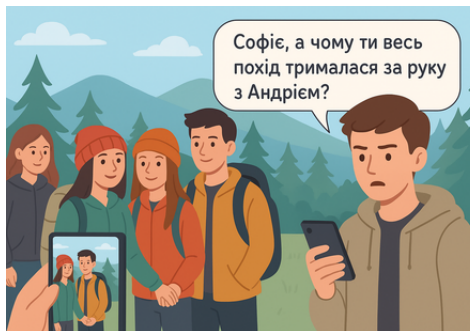
Крок 2: Заохочуйте учасників до дискусії, зосередившись на важливості перевірки інформації перед тим, як діяти на її основі або пересилати її іншим, особливо якщо її зміст може негативно вплинути на інших людей. Наведіть вигадані (але правдоподібні) приклади випадків, коли це може статися, наприклад, надсилання попереджувального повідомлення про людей, яких можна впізнати за фотографією, ім'ям, або поширення неправдивої інформації про засоби профілактики COVID-19.

Крок 3: Задайте питання, щоб виявити ситуації, в яких найімовірніше поширюється дезінформація: як фальшива інформація виглядає правдивою? Якщо інформація надходить від родича чи друга, чи є вона більш достовірною? Чому? Чи є це доречним? Якщо ця інформація була поширена багато разів, чи виглядає вона більш надійною? Чи це дійсно так? Коли інформація здається терміновою або важливою для інших, чи ви більш схильні її поширювати? Чи слід бути більш обережним щодо цього? Якщо щось викликає у вас гнів або емоції, чи схильні ви ділитися цим імпульсивно? Чи є це розумним?



Дезінформація та місінформація в Інтернеті

Навчальний ресурс: Історія



КРИТИЧНЕ МИСЛЕННЯ ТА ЕМОЦІЇ ПРОТИ ДЕЗІНФОРМАЦІЇ — ЧИ ВСЕ Є ТАКИМ, ЯКИМ ЗДАЄТЬСЯ?

Вікова група: 9-14 років

Шкільний клас: 4-8 класи

ВАРТО ВРАХУВАТИ

- Місінформація — це зазвичай неправдива інформація, створена без зловмисного наміру.
- Вона може спричинити проблеми, що виходять за межі очікувань і контролю автора.
- Важливо не приймати важливих рішень і не реагувати надмірно на інформацію, яка не була перевірена.

Активність: Прочитайте історію та обговоріть її



Вступ

Ця історія є яскравим прикладом того, як дезінформація може бути поширена без злого умислу, але все одно мати негативні наслідки для третіх осіб.



Тривалість

30–40 хвилин, залежно від розміру групи та рівня її залученості.



Цілі

- Уточнити поняття дезінформації.
- Пропагувати необхідність перевірки інформації, навіть якщо вона походить з надійних джерел, особливо у випадках, коли вона може мати негативні наслідки для когось.
- Розвивати емпатію до людей, які можуть бути джерелом неправдивої інформації, враховуючи можливість того, що вони не мали таких намірів.



Реалізація

Крок 1: Прочитайте історію двічі поспіль, щоб оцінити її нюанси.

Крок 2: Проведіть групову дискусію навколо таких питань: Що сталося в цій історії? Чи хтось постраждав? Чи є якась неправдива або оманлива інформація? Коли це сталося? В який момент? Як це поширилося? Чи були злісні наміри з боку когось із залучених осіб? Яку роль у всьому цьому відіграли соціальні медіа? Як можна було уникнути цієї ситуації?

Крок 3: Визначте випадки дезінформації в повсякденному житті дітей. Для цього попросіть їх поділитися подібними ситуаціями, коли вони, можливо, знали про дезінформацію в соціальних мережах або стикалися з нею, або, якщо це доречно, чи можуть вони уявити собі такі ситуації. Насамкінець слід наголосити на тому, наскільки делікатною і небезпечною може бути неправдива інформація, а також на ролі, яку кожна людина може відігравати у боротьбі з нею.

Клас вирушив у дводенний похід. Вночі стало дуже холодно, і Марійка почала тремтіти. Її подруга Софія зняла свою теплу червону шапку й віддала Марійці:
— Надягай, бо змерзнеш.

Уранці всі фотографувалися біля наметів — веселі, сонні, але задоволені. На груповому фото Марійка стояла поруч із Софією... у тій самій червоній шапці.

Коли вони повернулися додому, хтось із однокласників виклав фото в соцмережу й відмітив усіх, але визначив Марійку як Софію — бо на фото саме Марійка була в червоній шапці, яку завжди носила Софія.

Під постом одразу з'явився коментар від Макса — хлопця Софії:
"Софіє, а чому ти весь похід трималася за руку з Андрієм?"

Софія розгубилася:
— Але це ж не я! Це Марійка в моїй шапці!

Макс не повірив одразу — фото здавалося очевидним. Довелося пояснювати, що вночі було холодно, шапку позичили, а в соцмережі просто неправильно відмітили.

Ситуація була неприємною: через одну деталь і поспішні висновки виникло серйозне непорозуміння, тож перш ніж робити висновки про когось за фото чи дописом, треба перевіряти інформацію, уточнювати деталі й не довіряти підписам або поверхневим враженням.

Кібернасильство проти жінок і дівчат

Навчальний ресурс: Анімація



ДЕСЯТЬ ФОРМ ЦИФРОВОГО ГЕНДЕРНО- ЗУМОВЛЕНОГО НАСИЛЬСТВА

Вікова група: **13-18 років**
Шкільний клас: **8-12 класи**

<https://www.youtube.com/watch?v=2K1HyTbwnQI>

Тривалість: 5 хвилин 08 секунд

ВАРТО ВРАХУВАТИ

- Переслідування або контроль партнера за допомогою мобільного телефону.
- Втручання в онлайн-спілкування партнера з іншими людьми.
- Шпигування за мобільним телефоном партнера.
- Цензурування фотографій, які партнер публікує та поширює в соціальних мережах.
- Контроль за тим, що партнер робить у соціальних мережах.
- Вимагання від партнера доводити своє місцезнаходження за допомогою геолокації.
- Примушування партнера надсилати інтимні зображення.
- Тиск із вимогою надати свої паролі.
- Примушування партнера показувати переписку з іншою людиною.
- Прояв агресії через те, що партнер не завжди відповідає онлайн негайно.

Насильство — це не лише фізичні дії; воно також включає будь-яку поведінку, що обмежує свободу іншої людини.

Активність: Перегляд анімації та обговорення



Вступ

Ця анімація намагається наочно пояснити, як певні види поведінки, пов'язані з втручанням і контролем над цифровим життям партнера, є формою насильства.



Тривалість

Від 20 до 50 хвилин, залежно від розміру групи та рівня її залученості.



Цілі

- Підвищити обізнаність про те, що обмеження або обумовлення поведінки людини є формою насильства.
- Визначити різні способи, за допомогою яких щодня обмежують і контролюють поведінку, пов'язану з соціальними мережами або використанням мобільних телефонів, особливо в контексті подружніх пар.



Реалізація

Крок 1: Почніть із заохочення до роздумів про поведінку пари, яка викликає дискомфорт, коли доводиться терпіти таку ситуацію. На цьому етапі поставте запитання, чи деякі з цих видів поведінки однаково навіязуються чоловіками чи жінками. Ви повинні пояснити, що в обох випадках це шкідлива та токсична поведінка. Коли це відбувається щодо жінок, це пов'язано з іншими причинами і може мати різні наслідки. Це вважається ґендерно-зумовленим насильством, коли жінка страждає від цього з боку партнера або колишнього партнера.

Крок 2: Перегляньте відео від початку до кінця. Потім перегляньте його вдруге, зупиняючись на кожній з десяти перелічених форм насильства. На кожній зупинці заохочуйте дітей пояснити, як ця дія шкодить і спричиняє дискомфорт для її об'єкта та як вона може вплинути на його чи її благополуччя, свободу та особистий розвиток. Питання також можуть стосуватися того, що стоїть за цією поведінкою, чому вона відбувається та як вона може вплинути на стосунки.

Крок 3: Якщо є час, розпочніть дискусію, щоб спробувати визначити інші форми контролюючого цифрового насильства, з якими можуть стикатися жінки та дівчата.

Кібернасильство проти жінок і дівчат

Навчальний ресурс: Історія



ВИ НЕ МОЖЕТЕ ДІЛИТИСЯ НИМИ БЕЗ ЇХНЬОЇ ЗГОДИ

Вікова група: **13-18 років**
Шкільний клас: **8-12 класи**

ВАРТО ВРАХУВАТИ

- Те, що хтось погодився записати свою інтимність з іншою особою, не дає права, навіть колишньому партнеру, поширювати ці зображення.
- Хоча це називають «помстивим порно», це не порно і не помста. Нічого не може виправдати неузгоджене розповсюдження інтимних зображень.
- Ця форма гендерно-зумовленого кібернасильства має дуже серйозні наслідки для жертв і тягне за собою серйозну юридичну відповідальність для порушника.
- Важливо, щоб люди повідомляли про такі випадки.

Активність: Прочитайте історію та обговоріть її



Вступ

Ця історія розповідає про випадок розповсюдження інтимних зображень колишнього партнера без його згоди з метою заподіяння шкоди. Ця практика також відома як порно помсти. Це форма сексуального гендерного кібернасильства.



Тривалість

40–50 хвилин, залежно від розміру групи та рівня її активності.



Цілі

- Визначити несанкціоноване поширення інтимних зображень як форму гендерного кібернасильства.
- Підвищити обізнаність про різницю між згодою на зйомку зображень та дозволом на їх розповсюдження.
- Замислитися над важливістю того, щоб суспільство в цілому не брало участі у віктимізації жінок, чиє приватне життя було порушено, та уникати перегляду, коментування або поширення цих зображень.



Реалізація

Крок 1: Прочитайте історію “Злочин, який не можна побачити”.

Крок 2: Заохочуйте групову дискусію, аналізуючи роль і поведінку кожного з головних героїв та їхнього оточення. Також обміркуйте наслідки для кожного з них.

Крок 3: Складіть разом із групою список із щонайменше п'яти дій, які кожен може вжити, щоб уникнути такого роду віктимізації.

Марія зустрічалася з однокурсником Павлом майже пів року. Їхні стосунки починалися тепло, але з часом Марія зрозуміла, що вони дуже різні, і чесно сказала Павлові, що хоче розійтися.

Павло образився і не зміг прийняти її рішення. Зі злості він опублікував у мережі їхні приватні фото та відео, які колись отримав від Марії за її довірою. Марія не давала дозволу на їхній перегляд чи поширення нікому.

Наступного ранку Марію почали обговорювати в чатах, хтось пересилав матеріали далі, а хтось робив образливі коментарі. Дівчина відчувала сором, страх і безпорадність. Вона боялася виходити з дому й навіть відкривати телефон.

Коли про ситуацію дізналися подруга, вона підтримала Марію й допомогла їй звернутися до батьків, адміністрації університету та поліції. Павлові дії кваліфікували як кібернасильство та незаконне поширення особистих матеріалів, що є серйозним правопорушенням.

Поступово Марія повернула контроль над ситуацією й отримала підтримку психолога. Але вона запам'ятала назавжди:

Інтимні матеріали — не “подарунок” у стосунках. Їхнє публічне поширення — це насильство, а не помста. І відповідальність за це завжди лежить на тому, хто порушує довіру.

Цифровий слід, репутація та ідентичність

Навчальний ресурс: Анімація



ЦИФРОВИЙ СЛІД, РЕПУТАЦІЯ ТА ІДЕНТИЧНІСТЬ: ЯК ВОНИ ВПЛИВАЮТЬ НА МЕНЕ?

Вікова група: 11-16 років

Шкільний клас: 5-10 класи

<https://www.youtube.com/watch?v=aAis9WITXyc>

Тривалість: 2 хв. 17 с.

ВАРТО ВРАХУВАТИ

- Те, що розміщено в Інтернеті, може впливати на ваше життя офлайн.
- Зображення або відео в Інтернеті не показують повного контексту.
- Те, що ви публікуєте в Інтернеті, може формувати у інших думку про вас, яка негативно вплине на вас.
- Можливо, зараз вам це байдуже, але в майбутньому це матиме значення, тому важливо дбати про свою цифрову ідентичність.

Активність: Перегляд анімації та обговорення



Вступ

Ця анімація показує, як те, що ми публікуємо в Інтернеті, може створити нам проблеми, особливо коли це потрапляє до людей, яких ми не очікували, або в непередбачуваний момент у майбутньому.



Тривалість

Від 30 до 50 хвилин, залежно від розміру групи та рівня її залученості.



Цілі

- Стимулювати роздуми про важливість того, що з'являється в Інтернеті про людину, для формування її цифрової ідентичності та репутації.
- Поміркувати над тим, як певна інформація (текст, фотографія або відео) про особу, вирвана з контексту, може вплинути на інших людей, або як вона може потрапити до людей, які не були передбачені як її першочергові одержувачі, або з'явитися в несподіваний момент, що може мати негативні наслідки для особи, зображеної в ній.



Реалізація

Крок 1: Після перегляду анімації розпочніть коротку дискусію з групою, заохочуючи їх відповісти на такі питання: Що сталося? Хто програв? Чому? Як цього можна було уникнути?

Крок 2: Потім діти повинні глибше зануритися в роздуми, знову заохочуючи дискусію на основі питань, зосереджених на анімації: Як ви думаєте, чи думала головна героїня в той момент, коли вона робила знімки, що вона робить щось погане або недоречне? Чи думала вона, що це може створити їй проблеми? Чи повинна головна героїня припинити робити щось через те, що люди можуть подумати, чи достатньо того, що вона переконується, що ці знімки не будуть доступні іншим людям? Як ви вважаєте, чи має вона повний контроль, чи вона залежить від третіх осіб?



Цифровий слід, репутація та ідентичність

Навчальний ресурс: Історія



**СЛІДКУЙТЕ ЗА ТИМ,
ЩО ВИ ПУБЛІКУЄТЕ,
АДЖЕ ЦЕ МОЖЕ
ОБЕРНУТИСЯ ПРОТИ
ВАС!**

Вікова група: **11-16 років**

Шкільний клас: **5–10 класи**

ВАРТО ВРАХУВАТИ

Те, що ви публікуєте про себе, може призвести до неприємностей або створити проблеми для вас чи інших.

Активність: Прочитайте історію та обговоріть її



Вступ

Ця історія показує, як Інтернет має пам'ять і, як результат, будь-яка інформація з минулого може з'явитися в незручний час і в незручному місці.



Тривалість

40–50 хвилин, залежно від розміру групи та рівня її активності.



Цілі

- Поміркувати над тим, яке значення може мати опублікована інформація в майбутньому та для тих, кому вона була спочатку призначена.
- Підкреслити, як певні аспекти нашого життя, опубліковані в Інтернеті, можуть суперечити іншим, якщо вони розміщені в різний час або в різному контексті.
- Звернути увагу на те, як навіть наша власна інформація може бути використана іншими для заподіяння нам шкоди.



Реалізація

Крок 1: Прочитайте історію кілька разів, щоб аудиторія могла вловити всі нюанси.

Крок 2: У групах по 4-5 осіб повинні визначити або уявити конкретні ситуації, в яких певна інформація (зображення, відео, коментарі тощо), опублікована без злого наміру, може в кінцевому підсумку завдати шкоди людині, яка в ній фігурує.

Крок 3: Спільно складіть список із щонайменше п'яти корисних рекомендацій, щоб уникнути такого роду проблем.

Артем закохався в однокласницю Зою. Він довго наважувався й нарешті сказав їй про свої почуття. Але Зоя ввічливо відповіла, що зустрічається з хлопцем, який, як і вона, є вегетаріанцем.

Артем засмутився і вирішив привернути її увагу за будь-яку ціну. Він почав переглядати старі сторінки Зої в соцмережах і випадково знайшов дуже давнє фото: Зоя на барбекю у друзів, усміхається і тримає шматочок м'яса. Це був жартівливий знімок з дитинства, про який вона вже майже не пам'ятала.

Артем виклав це фото в шкільну мережу, підписавши: «Ото вам і вегетаріанка...»

Наступного дня Зоя була в сльозах. Її хлопець побачив це старе фото й вирішив, що дівчина брехала про свої переконання. Він перестав із нею спілкуватися, навіть не спробувавши розібратися.

Зоя почувалася приниженою, але ця ситуація вкотре нагадала: навіть давній цифровий слід може повернутися і нашкодити - тобі чи іншим, навіть якщо ти про нього давно забув.



Твій цифровий слід



**Коли ви підключаєтеся
до Інтернету, зробить
паузу й поставтеся до
цього відповідально**

Цей посібник має на меті бути інтерактивним педагогічним інструментом, адаптованим до потреб педагогів, батьків, опікунів та інших осіб, залучених до догляду за дітьми або їхнього виховання й освіти, а також усіх, хто зацікавлений у запобіганні кіберзлочинності та просуванні безпечного користування Інтернетом без будь-яких форм дискримінації, насильства чи злочинності.



United Nations
Office on Drugs and Crime



GLOBAL PROGRAMME ON
CYBERCRIME