

БРОШУРА про БЕЗПЕКУ В ІНТЕРНЕТІ



Все, що вам потрібно знати!



United Nations
Office on Drugs and Crime



United Nations Office on Drugs and Crime

Ця публікація не була офіційно відредагована.

Зміст цієї публікації не обов'язково відображає погляди чи політику UNODC або організацій, що брали участь у її підготовці, і не означає їхньої підтримки. Цей матеріал було розроблено з метою сприяння використанню інклюзивної мови, спрямованої на просування ґендерної рівності.

Повне або часткове відтворення цього матеріалу дозволяється за умови зазначення UNODC як джерела та без будь-яких змін у змісті. Використання цієї публікації в комерційних цілях заборонено. UNODC зберігає за собою право вживати юридичних заходів у разі неправомірного використання цієї публікації відповідно до правил і положень ООН.



GLOBAL PROGRAMME ON CYBERCRIME

Управління Організації Об'єднаних Націй з наркотиків і злочинності (UNODC) сприяє підвищенню безпеки у світі, протидіючи незаконному обігу наркотиків, організованій злочинності, корупції та тероризму.

Глобальну програму ООН з боротьби з кіберзлочинністю було створено у 2013 році з метою надання допомоги державам-членам у протидії кіберзлочинності шляхом нарощування потенціалу та надання технічної допомоги відповідно до резолюції Генеральної Асамблеї 65/230 (2011), а також резолюцій 22/7 і 22/8 Комісії з попередження злочинності та кримінального правосуддя.

Місія Глобальної програми з кіберзлочинності полягає в посиленні заходів із запобігання та протидії кіберзлочинності шляхом упровадження інноваційних, інтегрованих і адаптованих рішень. У межах цієї місії Програма підтримує держави-члени в досягненні таких цілей:

- Підвищення інституційної ефективності та результативності у розслідуванні, судовому переслідуванні та судовому розгляді кіберзлочинів з дотриманням принципів прав людини.
- Створення ефективних нормативно-правових рамок, що забезпечують стійку та довгострокову протидію кіберзлочинності відповідно до міжнародних стандартів.
- Посилення національної та міжнародної координації між органами державної влади, правоохоронними органами та приватним сектором з метою підвищення ефективності реагування на кіберзлочини.
- Підвищення рівня знань і обізнаності суспільства з метою зменшення ризиків, пов'язаних із кіберзлочинністю.

ІНТЕРНЕТ Є ДУЖЕ КОРИСНИМ ІНСТРУМЕНТОМ,

коли знаєш, як ним правильно користуватися...

- Інформаційно-комунікаційні технології (ІКТ) змінили світ і з кожним днем роблять його кращим. У нову цифрову еру стало значно легше вирішувати повсякденні завдання.
- Інтернет - це універсальний інструмент, який дає змогу здобувати нові знання та слугує простором для розваг.
- Серфінг в Інтернеті, використання соціальних мереж і спілкування за допомогою цифрових технологій можуть бути корисним і позитивним досвідом.
- Доступ до Інтернету за допомогою різних типів пристроїв стає дедалі простішим.
- ІКТ надають дітям, підліткам і дорослим широкі можливості для спілкування та навчання, однак для цього їх необхідно використовувати відповідально та безпечно.

ВИКОРИСТОВУЙТЕ ІНТЕРНЕТ НА СВОЮ
КОРИСТЬ,

ЩОБ НЕ ЗАВДАТИ ШКОДИ СОБІ АБО ІНШИМ





КІБЕРБУЛІНГ

Чи доводилося вам коли-небудь відчувати переслідування, дискримінацію або отримувати образливі коментарі через соціальні мережі, електронну пошту чи миттєві повідомлення?

Чи траплялося, що вас цькували, погрожували, переслідували, принижували або турбували через соціальні мережі чи мобільний телефон?

Кібербулінг - це використання інформаційно-комунікаційних технологій (ІКТ) для повторного, навмисного та ворожого заподіяння шкоди. Це може включати, зокрема, використання Інтернету, мобільних телефонів або інших електронних пристроїв для поширення чи надсилання текстів або зображень, які завдають шкоди або принижують людину.

Що я можу зробити?

- Більшість соціальних мереж мають механізми безпеки, повідомлення та блокування. Активуйте їх, якщо хтось ображає, переслідує або погрожує вам.
- Уникайте реагування на провокації або образи.
- Якщо вас переслідують, негайно зверніться за допомогою до батьків, вчителів або дорослих, яким ви довіряєте.
- Поводьтеся в Інтернеті з повагою до інших. Не робіть іншим того, чого не хотіли б, щоб робили вам.



ГРУМІНГ

Ви подружилися з кимось, кого зустріли в Інтернеті, але не знаєте в реальному житті?

Грумінг - це процес, під час якого доросла людина намагається встановити або розвинути стосунки з дитиною чи підлітком особисто або за допомогою Інтернету чи інших цифрових технологій з метою полегшення сексуального контакту - в Інтернеті або поза ним.

Які засоби він або вона зазвичай використовує?

- Електронні листи.
- Відеочати.
- Обмін зображеннями або відео.
- Соціальні мережі.
- Стрімінгові платформи.

Дізнайтеся про етапи грумінгу:

1. Виявлення жертви через соціальні мережі, чати або онлайн-платформи.
2. Завоювання довіри потенційної жертви.
3. Зваблення жертви за допомогою тривалого спілкування та емоційного зближення.
4. Отримання інтимної інформації та/або контенту, що дозволяє чинити тиск на жертву.
5. Домагання, шантаж, погрози та маніпуляції з метою досягнення власних цілей: отримання додаткових фото чи відео сексуального характеру або навіть організації особистих зустрічей сексуального характеру.

СЕКСТИНГ

Чи надсилали ви або отримували сексуальний чи еротичний контент через телефон, соціальні мережі або електронну пошту?

Секстинг - це самостійне створення, обмін та передача повідомлень, зображень або відео з оголеними або напівоголеними людьми, що мають сексуальний підтекст, за допомогою мобільних телефонів або інших технічних пристроїв.

Пам'ятайте, що після надсилання зображення, відео або повідомлення, навіть через веб-камеру, ви втрачаєте контроль над цим контентом. Інша особа може захопити та/або записати цей контент і опублікувати його в Інтернеті.

Найкраще і найбезпечніше - ніколи не ділитися особистими зображеннями або повідомленнями в Інтернеті, навіть з тими, кому ви довіряєте.

Найпоширеніші небезпеки секстингу:

- Завдання шкоди вашій приватності. Небажане оприлюднення цих зображень завдає непоправної шкоди приватності та інтимності особи, яка ділиться своїми зображеннями.

- Навіть якщо ви використовуєте паролі та інші механізми безпеки, ваші дані можуть бути зламані або вкрадені, та навіть поширені в Інтернеті без вашої згоди.





СЕКСТОРЦІЯ

Чи коли-небудь вас шантажували, погрожуючи оприлюднити ваші фотографії, відео або інформацію, якщо ви не зробите те, що вам кажуть?

Сексторція відбувається, коли одна людина шантажує іншу, погрожуючи оприлюднити інтимні фотографії або відео, щоб отримати сексуальні послуги, гроші, більше контенту або інші вигоди.

Жертву примушують до сексуальних дій або сплати певної суми грошей, погрожуючи оприлюднити ці зображення, якщо вона не підкориться.

Рекомендації:

1. Негайно припиніть спілкування та/або будь-які стосунки й за жодних обставин не піддавайтеся шантажу.
2. Налаштуйте свої облікові записи в соціальних мережах так, щоб ваш профіль був доступний лише для друзів.
3. Зберігайте всі докази спілкування (повідомлення, знімки екрана, посилання), щоб мати можливість звернутися до правоохоронних органів.

ЦИФРОВЕ ҐЕНДЕРНО-ЗУМОВЛЕНЕ НАСИЛЬСТВО

Цифровий простір, з огляду на свої особливості, також є середовищем, у якому відтворюються різні форми ґендерно-зумовленого насильства щодо жінок і дівчат, зокрема:

- **Кібербулінг.**
- **Кіберсталкінг.**
- **Несанкціоноване поширення інтимних та сексуальних зображень.**
- **Доксинг** (публікація приватної або ідентифікаційної інформації в Інтернеті зі зловмисною метою).
- **Сексуальне насильство.**
- **Отримання сексуальних зображень і відео без згоди.**
- **Погрози сексуальним насильством.**

Особи, які зазнали насильства в онлайн-середовищі, стикаються з серйозними психологічними, фізичними, сексуальними, емоційними, економічними, трудовими, сімейними та соціальними наслідками.

Важливо пам'ятати:

- Цифрове насильство є злочином, і необхідно вживати активних заходів для його запобігання та покарання.
- Неприпустимо нормалізувати насильство на цифрових платформах.
- Потрібно знати механізми запобігання та захисту.
- Освіта з цифрового громадянства та кібербезпеки має бути доступною для всіх.





ШКІДЛИВЕ ПРОГРАМНЕ забезпечення

Це шкідливе програмне забезпечення, призначене для пошкодження системи, викрадення інформації, внесення змін до операційної системи та отримання контролю над інфікованим пристроєм. Існує багато видів шкідливого програмного забезпечення: віруси, троянські коні або трояни, черв'яки, кейлоггери, бекдори або боти, експлойти, шпигунське програмне забезпечення, програми-вимагачі тощо.

Як ваш пристрій може бути заражений?

- Під час пошуку контенту та завантаження інформації.
- Через завантаження застосунків із неофіційних вебсайтів
- Під час підключення заражених пристроїв до вашого телефону або комп'ютера.

Як цього уникнути?

- Підтримуйте програмне забезпечення безпеки (антивірус) та операційну систему пристрою в актуальному стані.
- Скануйте будь-які носії інформації перед підключенням їх до комп'ютера.
- Не завантажуйте підозрілі файли та не відвідуйте сайти з сумнівною репутацією.



ФІШИНГ

Як це працює?

Існують шахраї, які надсилають фальшиві повідомлення, електронні посилання або електронні листи, видаючи себе за банківські установи чи інші компанії. Їхня мета - спонукати людей розкрити особисту інформацію, зокрема дані профілю, паролі або банківські реквізити, щоб згодом викрасти кошти з рахунків.

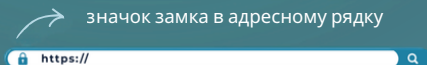
Тип викраденої інформації:

1. Особисті дані.
2. Фінансова інформація.
3. Паролі.
4. Конфіденційна інформація.

Рекомендації:

- Ніколи не натискайте на посилання, отримані в підозрілих повідомленнях.
- Ніколи не завантажуйте вкладення з підозрілих повідомлень. Вони можуть містити шкідливе програмне забезпечення.
- Регулярно створюйте резервні копії вашої інформації.
- Регулярно оновлюйте операційну систему, браузер, антивірус та інші програми на своїх електронних пристроях.
- Уникайте відвідування веб-сайтів з сумнівною репутацією або цензурованим контентом.

Завжди перевіряйте



значок замка в адресному рядку

адресу <https://>.



онлайн-ігри

Все більше і більше онлайн-ігор завантажуються на мобільні телефони, комп'ютери або граються онлайн через ігрові консолі, до яких підключені сотні мільйонів користувачів.

Іноді такі ігри вимагають розкриття конфіденційної інформації, зокрема номерів банківських карток, персональних даних, адреси тощо.

Деякі злочинці використовують ці платформи, щоб підійти до дітей та підлітків із поганими намірами, викрасти інформацію та обдурити вас або ваших батьків.

Рекомендації для геймерів

- Встановіть антивірусне програмне забезпечення.
- Оновлюйте програми.
- Використовуйте надійні та складні паролі.
- Купуйте товари тільки в офіційних інтернет-магазинах.
- Уникайте розкриття особистої інформації під час гри.
- Не погоджуйтеся зустрічатися з віртуальними гравцями в реальному світі без відома батьків.

ЗАХИСТІТЬ СВОЮ РЕПУТАЦІЮ В ІНТЕРНЕТІ!

Ваша репутація в Інтернеті - це те, як вас сприймають інші в мережі. Вона залежить від того, що ви публікуєте самі, і від того, що про вас публікують інші. На неї впливають дописи, фотографії та відео з вашою участю, доступні в Інтернеті.

Пам'ятайте, що репутація формується роками і її важко стерти або змінити, оскільки в Інтернеті нічого не забувається. Те, що ви завантажуєте в Інтернет, може залишитися там назавжди.

Ваша репутація в Інтернеті є важливою

Інтернет став найпоширенішим і найшвидшим способом дізнатися про людину. Коли ви хочете отримати стипендію або роботу, ваш співрозмовник може шукати інформацію про вас в Інтернеті. Якщо ви не захищаєте свою репутацію в Інтернеті, ваша особиста інформація може бути поширена, а ваш імідж може постраждати.



ПОРАДИ ДЛЯ ДІТЕЙ ТА ПІДЛІТКІВ

ВИБИРАЙТЕ РОЗУМНО

Додавайте до свого профілю в соціальних мережах і надавайте доступ до нього лише тим, кого ви знаєте особисто.

ВИЗНАЧАЙТЕ СВОЇ ОСОБИСТІ МЕЖІ

Зробіть свій профіль у соціальних мережах приватним і надавайте доступ лише тим, кому довіряєте.

КЕРУЙТЕ СВОЇМИ ПОВСЯКДЕННИМИ ДАНИМИ

Навіть на перший погляд проста інформація - про те, де ви навчаєтеся, працюєте, живете або проводите дозвілля, - може стати інструментом для кривдника, щоб завдати вам шкоди.

БУДЬТЕ УВАЖНІ ДО ТОГО, ЩО ВИ ЗАВАНТАЖУЄТЕ

Пам'ятайте, що завантаження або копіювання ігор, пісень чи програмного забезпечення, захищених авторським правом, є незаконним. Такі дії також можуть заразити ваш комп'ютер вірусом.

УНИКАЙТЕ ПАСТОК ТА ОБМАНУ

Деякі використовують фальшиві профілі в соціальних мережах та інших інтернет-ресурсах, щоб ставити пастки, красти або просто переслідувати інших. Ігноруйте їх!

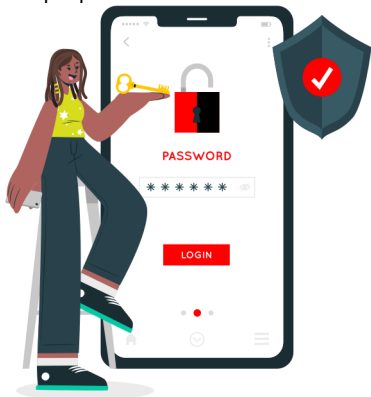
ВИ МАЄТЕ СИЛУ ЗМІНИТИ СИТУАЦІЮ

Якщо ви потрапили в неприємну ситуацію в Інтернеті і хочете запобігти подібним випадкам у майбутньому, поділіться своїм досвідом з батьками або дорослими, яким довіряєте.



ЯК СТВОРИТИ НАДІЙНИЙ ПАРОЛЬ?

- Він має містити щонайменше 8 символів.
- Він не має містити інформацію, яку легко вгадати (ім'я, дату народження тощо).
- Він має містити великі та малі літери.
- Він має складатися з цифр і букв.
- Він не повинен зберігатися на пристрої та має вводитися щоразу під час використання.
- Він має зберігатися в таємниці та не повідомлятися нікому, окрім членів сім'ї.
- Він має періодично змінюватися.
- Він має бути різним для кожної служби, соціальної мережі або програми.





ПОРАДИ ДЛЯ ДОРΟΣЛИХ

- Навчіться користуватися технологіями, не бійтеся дізнаватися, як працює Інтернет.
- Налагодьте довірчі стосунки з дітьми та інформуйте їх про небезпеки соціальних мереж.
- Навчіть дітей розрізняти добро і зло, як і в реальному житті.
- Використовуйте батьківський контроль, щоб обмежити доступ до сторінок з вмістом, який не підходить для дітей та підлітків.
- Контролюйте історію пошуку в браузері в Інтернеті.
- Встановіть обмеження на використання технологій дітьми та підлітками.
- Створіть зони, вільні від технологій, наприклад: спальні.
- Поясніть дітям, що вони ніколи не повинні повідомляти свою адресу, вік, номер телефону або іншу особисту інформацію, зокрема назву школи, яку вони відвідують, деталі свого розпорядку дня чи місця, де вони люблять грати в Інтернеті.
- Поясніть, що під час зустрічей з онлайн-друзями, яких діти не знають особисто, обов'язково мають бути присутні дорослі. Пам'ятайте, що зовнішність може бути оманливою.

ЩО РОБИТИ, ЯКЩО ВИ СТАЛИ ЖЕРТВОЮ КІБЕРЗЛОЧИНУ ?

- Припиніть будь-яке спілкування з особою, яка шантажує, переслідує або викликає у вас дискомфорт.
- Не видаляйте, не знищуйте та не змінюйте інформацію, яка є на вашому комп'ютері або мобільному телефоні.
- Фіксуйте докази: скріншоти, записи листування або інші матеріали, включаючи дату і час.
- Скопіюйте повну URL-адресу та збережіть інформацію.
- Повідомляйте про випадки кібернасильства: зверніться у поліцію за телефоном 102 або подайте електронне звернення до кіберполіції за посиланням <https://ticket.cyberpolice.gov.ua>.

Якщо ви стали жертвою, повідомте про це своїх батьків, опікунів або когось, кому ви довіряєте.

Не мовчіть, подайте заяву в найближчий до вашого дому відділок поліції.

Будьте впевнені, що поліція серйозно поставиться до вашої заяви.

Для правильної кваліфікації випадку і звернення до суду необхідна консультація з юристом. Для цього Ви можете звернутися до Центру безоплатної правничої допомоги за телефоном: 0 800 213 103, чи онлайн за посиланням: <https://legalaid.gov.ua/>



Зверніться до
найближчого відділку
поліції або
зателефонуйте за
номером

102



Термінологія

Резервна копія: копія одного або декількох комп'ютерних файлів, яка зазвичай створюється для запобігання можливій втраті інформації.

Матеріали сексуального насильства над дітьми: будь-які реальні або імітовані зображення дитини чи підлітка, які зображують їхню участь у сексуальних діях, у будь-якій формі та будь-яким способом.

Кіберзлочинність або комп'ютерна злочинність: будь-яка незаконна діяльність, що вчиняється з використанням комп'ютерів, комп'ютерних систем або інших комунікаційних пристроїв, зокрема злочини, які здійснюються за допомогою кібертехнологій або залежать від них.

Інтернет: глобальна мережа комп'ютерних мереж, призначена для забезпечення обміну інформацією між усіма її користувачами.

Інформаційно-комунікаційні технології (ІКТ): це всі ресурси, інструменти та програми, що використовуються для обробки, управління та обміну інформацією за допомогою різних технологічних засобів, таких як комп'ютери, мобільні телефони, телевізори, портативні аудіо- та відеопрогравачі або ігрові приставки.

Шкідливе програмне забезпечення: програмне забезпечення, призначене для зміни роботи комп'ютера без відома користувача. Зазвичай такі програми заражають інші системні файли з метою їх модифікації, що може призвести до знищення файлів або даних, які зберігаються на комп'ютері.

Мережевий етикет: набір правил і практик, що регулюють і визначають поведінку різних учасників у кіберпросторі. Це етикет у кіберпросторі.

Сексуальна експлуатація: будь-яке зловживання вразливим становищем, нерівністю влади або довірою іншої особи з метою отримання сексуальних послуг.

Соціальні мережі: комп'ютерні платформи, призначені для розміщення віртуальних спільнот взаємопов'язаних осіб, які обмінюються контентом, інформацією, файлами, фотографіями, аудіо- та відеоматеріалами тощо.

Сексуальне насильство: будь-яка небажана дія, вчинена проти сексуальних прав або особистої недоторканності людини, що зазвичай передбачає небажане фізичне втручання сексуального характеру. Незалежно від характеру стосунків із постраждалою особою та в будь-якому середовищі, зокрема вдома чи на робочому місці.

Програмне забезпечення: комп'ютерні програми, що дозволяють виконувати певні завдання на комп'ютері.

URL: уніфікований локатор ресурсів або веб-адреса, яка при пошуку та перегляді в браузері відображає інформаційний ресурс для користувача.

Віртуальна спільнота: люди, об'єднані через Інтернет або віртуальний простір.

Веб-сайти: набір веб-сторінок, розроблених у коді HTML, пов'язаних з інтернет-доменом, які можна переглядати у Всесвітній мережі (www) за допомогою веб-браузерів, також званих браузерами.

НОТАТКИ

НОТАТКИ

This image shows a full page of white paper with horizontal blue dashed lines, typical of primary school handwriting practice paper. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.





United Nations
Office on Drugs and Crime



Canada



GLOBAL PROGRAMME ON
CYBERCRIME

