Magiczny Kraków

Кібернасильство

2026-11-23

Чи знали Ви, що кожна п'ята дівчинка стикалася з кібернасильством? Розпізнаємо його, реагуємо на це, запобігаємо цьому. Кібернасильство є все більш поширеною, але відносно новою формою насильства, яку часто применшують або ігнорують. Кібернасильство - це дії або погрози з використанням інформаційно-комунікаційних технологій, найчастіше комп'ютерів і смартфонів, підключених до Інтернету, які завдають (або можуть завдати) фізичної, сексуальної, психологічної чи економічної шкоди або страждань. Хоча іноді під кібернасильством розуміють насамперед насильство з боку однолітків/дітей та підлітків, вікових обмежень не існує - кібернасильство застосовується і проти дорослих, причому це насильство також "має" стать, а також вік, сексуальну орієнтацію, рівень фізичної підготовки, віросповідання.

Розпізнаємо

Нижче описані різні форми насильства з використанням нових технологій. Знання цього має вирішальне значення. Іноді люди, які зазнають такого насильства, не знають слів, щоб описати свій досвід. Без описів і знань також важко створювати правові, освітні, просвітницькі та інші інструменти для запобігання, реагування та переслідування кривдників, які вчиняють таке насильство.

До найбільш поширених зловживань в Інтернеті відносяться:

- методичне та наполегливе надсилання образливих електронних листів та повідомлень (наприклад, через месенджери),
- надсилання погроз,
- публікація інтимних фотографій чи відео,
- надсилання людині небажаних матеріалів сексуального характеру,
- відстеження людини різними способами (онлайн - за допомогою додатків для відстеження або в "реальному житті"),
- мова ворожнечі в Інтернеті/підбурювання до насильства, глибокої образи або ненависті до особи, яка належить до дискримінованої групи (наприклад, жінки).

До специфічних форм кібернасильства також належать доксинг, тролінг, флеймінг, секстинг та грумінг.

Інструментами такого насильства є переважно електронна пошта, чати, месенджери, вебсайти, блоги, соціальні мережі, форуми, сервіси SMS і MMS, а також мобільні додатки (наприклад, для відстеження) та електронні пристрої, керовані дистанційно і підключені до Інтернету (наприклад, камери, мікрофони тощо).

Magiczny Kraków

Реагуємо

Хоча абсолютна більшість людей вважає кібернасильство неприйнятною і водночас серйозною загрозою, часто - незалежно від того, чи відчуваємо його на собі, чи стаємо свідками - ми не знаємо, що робити.

Якщо Ви зіткнулися з кібернасильством:

- зверніться за підтримкою до довіреної особи/довірених(осіб - розкажіть комусь про те, що сталося/відбувається, разом обміркуйте, що робити далі, кого поінформувати,
- Ви можете повідомити про насильство в поліцію або прокуратуру; **винним завжди є злочинець, а не особа, проти якої хтось вчинив насильство**,
- Ви можете - зберігаючи анонімність - зателефонувати на гарячу лінію: 116 111 - Фонду "Даємо дітям силу" або 24/7 116 123 - Національної служби екстреної допомоги жертвам насильства в сім'ї "Блакитна лінія" Інституту психології здоров'я,
- вимагайте негайного видалення відео чи фото, знятого проти Вашої волі (волі жертви/потерпілої особи), або припинення будь-яких інших дій кібернасильства,
- блокуйте контакти з небажаними людьми в месенджерах та електронній пошті,
- вимагайте від адміністратора сайту видалити компрометуючі матеріали з мережі,
- документуйте докази насильства (зберігайте текстові повідомлення, історію спілкування, робіть скріншоти тощо),
- якщо насильство сталося в установі: школі, на роботі, в громадському центрі тощо - вимагайте, щоб Вам гарантували безпеку, а кривдника притягнули до відповідальності.

Що робити, якщо Ви стали свідком кібернасильства?

- не пересилайте далі шкідливі матеріали, які Ви отримуєте в Інтернеті,
- дайте знати людині, на яку напали, що Ви бачите, що відбувається, і підтримуєте її,
- повідомте про те, що Ви бачите, чуєте або читаєте в інтернеті, на порталах, у групах, довіреній (дорослій) особі, організації або поліції,
- завжди підтримуйте подруг та друзів, які стали жертвами кібернасильства, Ви або Він/Вона можете зателефонувати за номером 116 111.

Запобігаємо

Чим більше ми знаємо про насильство, в тому числі про кібернасильство, тим краще для нас. Другий принцип - подолання мовчання, табу і солідарність з тими, хто зазнав насильства. Наступний - розробити в кожній спільноті: у групі друзів, у школі, вдома - плани запобігання та

реагування на ситуації кібернасильства. Ми також повинні чинити тиск на державні установи, які відповідають за захист нас від насильства. Кібернасильство не є нашою приватною проблемою.

Як дбати про свою безпеку в Інтернеті?

Хоча людина, яка стикається з насильством, ніколи не є винною, є речі, які Ви можете зробити, щоб підвищити свою безпеку:

- оновити свої знання про кібернасильство та цифрову безпеку,
- дбати про конфіденційність своїх персональних даних,
- надати своїм онлайн-профілям захищений статус (приватний),
- захищати свої паролі та логіни,
- з обережністю вирішувати, які фото та відео Ви публікуєте в Інтернеті і кому Ви їх надсилаєте,
- намагайтеся не обмінюватися мобільними телефонами з колегами,
- намагайтеся не відповідати на онлайн-переслідування,
- використовуйте налаштування безпеки у власних профілях; подумайте, чи не підходить вам більше приватний профіль: вимкніть коментарі або увімкніть фільтри мови ворожнечі в додатках,
- дізнайтеся, як повідомляти про контент на Ваших улюблених порталах, і використовуйте цю функцію, коли виявляєте публікації, що містять ненависть, залякування, неправдиві новини або фейкові профілі.

Як користуватися інтернетом і телефоном, щоб не завдавати шкоди іншим?

- ставтеся до інших з повагою (не обзивайте, не ображайте, не погрожуйте тощо),
- не публікуйте в Інтернеті матеріали (відео, фото, тексти), які можуть завдати комусь шкоди,
- завжди питайте дозволу, якщо хочете когось сфотографувати або зняти на відео, а тим більше, якщо хочете опублікувати цей матеріал,
- не використовуйте мобільний телефон для надсилання фотографій, відео або текстів, які можуть спричинити комусь страждання чи шкоду.

Глосарій термінів, пов'язаних з Інтернетом та кібернасильством:

- Бодішеймінг (bodyshaming)
- Кріпшот (creepshot)
- Кіберсталкінг (cyberstalking)

- Кібербулінг (cyberbullying)
- Кіберфлешинг (cyberflash)
- Деднеймінг (deadnaming)
- Діпфейк (deepfake)
- Доксинг (doxing, doxxing)
- Флейминг (Flaming)
- Геолокалізація
- Грумінг (Grooming)
- Хакерство
- Фільмування побиття (Happy slapping)
- Розпалювання ненависті в інтернеті
- Шпигунське програмне забезпечення (stalkerware)
- Пасивне стеження
- Аутинг (Outing)
- Порнопомста
- Насильство з використанням пристроїв, підключених до Інтернету
- Тролінг (Trolling)
- Змушення до мовчання
- Секстинг (Sexting)
- Секс-шантаж (Sexual extortion)
- Сватинг (Swatting)

Бодішеймінг

критика тіла - це коментування та висміювання форми, розміру чи зовнішнього вигляду чийогось тіла, може відбуватися як в Інтернеті, так і за межами цифрового світу.

Кріпшот (creepshot)

фотографії людей сексуального характеру, зроблені без їхньої згоди.

Кіберсталкінг (cyberstalking)

включає методичне та наполегливе надсилання образливих електронних листів та повідомлень (наприклад, через месенджери), надсилання погроз, публікацію інтимних фотографій чи відео, а також стеження за людиною різними способами (онлайн або в "реальному житті" - за допомогою додатків для відстеження). Результатом цього є, зокрема, підрив почуття безпеки переслідуваної особи.

Кібербулінг (cyberbullying)

постійне залякування, примус або переслідування, що має на меті спричинити серйозні емоційні страждання та/або страх перед фізичною шкодою. Більшість жертв такого насильства - молоді люди та діти з вразливих груп. Кібербулінг також може включати в себе вимагання

сексуальних послуг або надання небажаного образливого, принизливого або залякуючого контенту, а також погрози та розпалювання ненависті в соціальних мережах.

Кіберфлешинг (cyberflash)

передбачає надсилання небажаних зображень відверто сексуального характеру через додатки для знайомств, програми для обміну повідомленнями або SMS, а також через Airdrop або Bluetooth.

Деднейминг (deadnaming)

навмисне використання імені, зазначеного у свідоцтві про народження трансгендерної людини (яке не відповідає її статі), з метою викликання почуття сорому, погроз, залякування або знущання над нею.

Діпфейк (deepfake)

відео, у якому оригінальне обличчя/персонаж було (непомітно) замінено на інше за допомогою алгоритмів, а звук змінений таким чином, щоб створити ілюзію дій і висловлювань іншої людини.

Доксинг (doxing, doxxing)

цей тип зловживань передбачає пошук, збір та публічне розголошення персональних даних (домашньої адреси, фотографії, імені жертви та її родичів) та конфіденційних даних (наприклад, походження, сексуальної орієнтації) без згоди цієї особи. Доксинг може спричинити серйозні психологічні наслідки. Крім того, дозволяючи фізично визначити місцезнаходження жертви, він також може передувати фізичному насильству. Зловмисники отримують інформацію шляхом пошуку в загальнодоступних базах даних та соціальних мережах, а також використовують хакерство та маніпуляції. Доксинг може використовуватися для переслідування та фінансового, сексуального та іншого шантажу або навіть для "вистежування" жертви в реальному світі.

Флейминг (Flaming)

це форма агресивного та ворожого спілкування в Інтернеті, яка завжди містить образи, неприязнь та ненависть. Типографічно коментарі зазвичай пишуться великими літерами і містять знаки оклику. Цей вид кібернасильства використовується для того, щоб спровокувати реакцію з боку іншого користувача/користувачки. Воно тісно пов'язане з тролінгом і, як правило, не визнається насильством у законодавстві чи політиці. Флейминг може бути відверто жінконенависницьким і часто містить погрози чи фантазії про сексуальне насильство або підбурює до нього

Геолокалізація

функція пристрою, яка уможливлює визначення свого географічного розташування на основі сигналів GPS або інших форм зв'язку.

Грумінг (Grooming)

примушення людини розкривати або ділитися власними еротичними або сексуальними матеріалами. На відміну від прямого примушення, це процес, в якому злочинець, використовуючи маніпуляції, вступає у стосунки з жертвою з метою отримання сексуального контенту, наприклад, фотографій в оголеному вигляді, інтимних розмов або інших онлайн-взаємодій. Грумінг починається зі встановлення контакту з жертвами, особливо неповнолітніми, з метою побудови довірчих відносин, де злочинці використовують фейкові профілі, щоб видати себе за іншу особу і сприяти фальшивій дружбі, яка закінчується примушенням.

Хакерство

процес отримання незаконного або небажаного доступу до комп'ютерної системи або мережі.

Фільмування побиття ("Happy slapping") (знятий на відео напад)

зафільмований напад/атака (фізичний або із сексуальним підтекстом) на жертву з метою зйомки нападу та розміщення його в Інтернеті. "Happy slapping" - це евфемізм для позначення нападу та побиття.

Розпалювання ненависті в інтернеті

підбурювання до насильства або ненависті щодо особи, яка належить до дискримінованої групи (наприклад, жінок). Хоча розпалювання ненависті - це широкий термін, який зазвичай асоціюється з насильством проти груп на основі їхньої етнічної, релігійної чи національної приналежності, вона також трапляється і проти жінок. Розпалювання ненависті на гендерному ґрунті включає, зокрема, сексуалізацію, об'єктивацію та принизливі коментарі щодо зовнішності, а також погрози зґвалтування та фізичного насильства, заохочення інших користувачів інтернету до такого насильства.

Шпигунське програмне забезпечення (stalkerware)

програмне забезпечення, зазвичай у вигляді додатка, що завантажується на чийсь телефон або пристрій і використовується для відстеження активності цього пристрою. Шпигунське програмне забезпечення вважається сталкерським у контексті домашнього насильства.

Пасивне стеження

правопорушник не відповідає на чиїсь повідомлення або не спілкується безпосередньо, але продовжує переглядати їхній контент онлайн (ставить лайки, переглядає історії тощо).

Аутинг (Outing)

практика розголошення інформації про сексуальну орієнтацію або гендерну ідентичність людини без її згоди, часто публічно.

Порнопомста

публічне поширення контенту сексуального характеру за участі однією або кількох людей без їхньої згоди. Більшість людей, які зазнають таких нападів, - жінки. Зазвичай такі матеріали поширює колишній партнер/хлопець дівчини/жінки. Злочинець отримує сексуально відверті зображення чи відео під час стосунків або зламує чи викрадає їх з комп'ютера, акаунтів у соціальних мережах чи телефону жертви, щоб поділитися ними в Інтернеті.

Насильство з використанням пристроїв, підключених до Інтернету

Для переслідування і контролю над жертвою використовуються такі пристрої, як розумні дверні дзвінки, гучномовці, камери спостереження або інші підключені до Інтернету пристрої, якими можна керувати дистанційно. Прикладами цього виду насильства є вмикання або вимикання вимикачів (наприклад, світла або опалення в будинку жертви), замикання (позбавлення волі) іншої людини в якомусь місці за допомогою управління розумною системою безпеки або запису з камер спостереження чи персональних електронних пристроїв.

Тролінг (Trolling)

це навмисне залучення інших осіб з метою зірвати дискусію/подію онлайн. Він передбачає публікацію у великих кількостях матеріалів, які відхиляються від теми дискусії, або перешкоджання дискусії шляхом надсилання агресивних та оманливих повідомлень. Тролі можуть не знати жертв. Сексистський тролінг - це образи за ознакою статі, жорстокі висловлювання та погрози зґвалтуванням та/або смертю, що здійснюються організованою групою з метою приниження жінок, особливо тих, хто висловлює свою думку.

Змушення до мовчання

у цифровій сфері означає перешкоджання повноцінній участі та самовираженню в Інтернеті, людині, яка замовкає через страх насильства та переслідувань, що в кінцевому підсумку призводить до виключення зі спільноти та публічних дебатів, у яких вона хотіла б брати участь.

Секстинг (sexting)

передбачає обмін, надсилання або отримання відверто сексуальних повідомлень, часто із зображеннями або відео, через повідомлення SMS або чат.

Секс-шантаж (Sexual extortion)

також відоме як "сексторсінг", передбачає використання погроз опублікувати сексуальний контент (фотографії, відео, фальшивий контент, чутки сексуального характеру) з метою залякування, примусу або шантажу, а потім отримати більше сексуального контенту, або з метою отримання грошей.

Сватинг (Swatting)

використання телефонів, а часто і комп'ютерних систем для обману екстрених служб з метою виклику правоохоронних органів на підставі неправдивого повідомлення.