Federal Foreign Office

CIVIL SOCIETY COOPERATION

Global Project Partners e.V.

СУСПІЛЬСТВО НАУКА ЕКОНОМІКА ДОВКІЛЛЯ

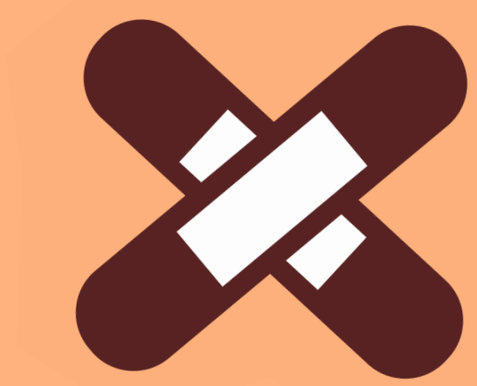
ІНСТИТУТ РЕГІОНАЛЬНОГО РОЗВИТКУ

ЯК ПОЧУВАТИСЯ БЕЗПЕЧНО В ІНТЕРНЕТІ

#civilsocietycooperation

Посібник підготовлено в рамках Проєкту SafetyNet, що реалізовувався в Україні Global Project Partners e.V. (www.global-project-partners.de) спільно з Інститутом Регіонального Розвитку (https://www.institute.lviv.ua/) за фінансової підтримки Федерального Міністерства Закордонних Справ Німеччини

КІБЕРБУЛІНГ — це один з різновидів цькування



Уявляєте своє життя без інтернету і соціальних мереж? Навряд чи. Дослідження ESPAD1, що охопило 8 509 українських підлітків (від 14 до 17 років), показало, що **не менше половини старшокласників проводить у будні дні до 3 годин на день у соціальних мережах, а на вихідних – більше 4 годин.** З одного боку це – навчання і спілкування з друзями онлайн. А з іншого – нові небезпеки, спрямовані на особисті дані, що може призвести до цькування у мережі, або ж кібербулінгу.

Кібербулінг – це один з різновидів цькування: знущання, приниження, агресивні напади, які здійснюють за допомогою різних гаджетів (зокрема телефонів), з використанням інтернету, будь-яких електронних (цифрових) технологій. Кібербулінг, як і офлайн цькування, має на меті принизити людину, завдати їй моральної шкоди, знищити її репутацію але відбувається за допомогою засобів комунікації і, зокрема, онлайн-сервісів.

Під час локдаунів, пов’язаних із пандемією COVID-19, кібербулінг серед учнів у європейських країнах почастішав. Це пов’язано з багатьма факторами, у тому числі і зі збільшенням кількості часу, який підлітки проводять в інтернеті. Аналогічною є картина і серед українських підлітків.

кожен 5

Фонд ЮНІСЕФ з'ясував, що кожен п'ятий український підліток визнавав себе **жертвою онлайн-знущань.**

Дослідження також відмічає, що підлітки **у віці 13-15 років** вдаються до такого **частіше**, ніж старші чи молодші школярі.

кожен 3

Кожен третій підліток **визнав свою участь у випадках образження або приниження інших** упродовж останніх двох місяців: кожен п'ятий робив це раз або двічі, а 3,5% кілька разів на тиждень.

13-15 років

ДІВЧАТА ЧАСТІШЕ СТАЮТЬ ОБ'ЄКТАМИ КІБЕРБУЛІНГУ

Багато досліджень також свідчить, що об'єктами кібербулінгу у соціальних мережах дівчата стають частіше, ніж хлопці і, до того ж, стикаються із кіберагресією у більш ранньому віці. Так проявляється у тому числі сексизм – небезпечне явище, коли люди вважають, що дівчата і жінки (просто внаслідок приналежності до жіночої статі) є гіршими, ніж хлопці і чоловіки. Якщо не протистояти таким упередженням, це призводить до розповсюдження насильства. І не лише у кіберпросторі, адже насильство легко виходить за межі онлайну і починає проявлятись у повсякденному житті і взаємодії між людьми.

ЧИМ ВІДРІЗНЯЄТЬСЯ НЕБЕЗПЕКА В ІНТЕРНЕТІ ВІД ОФЛАЙН-ЗАГРОЗ?

Ми приходимо в Інтернет, щоб спілкуватися з іншими людьми. Але тут, як і в реальному світі, люди мають різні наміри: хтось доброзичливі, хтось - ні. Соціальні мережі – це той простір, де зловмисників, шахраїв та злочинців може бути складно відрізнити, а у них, в свою чергу, з'являються нові можливості, щоб швидко, відносно легко і без загрози бути одразу покараним зашкодити іншим.

Прояви кібербулінгу досить різноманітні і кожен з них має особилвості. **Нижче – деякі розповсюджені форми, з якими підлітки стикаються у різних ситуаціях.**

Нападки Жертва постійно отримує образливі повідомлення, коментарі під фото чи своїми постами або стикається із спеціальними принизливими публікаціями про себе. Агресія може бути персональною чи груповою (нападки на людей певної національності, релігії, походження, місця проживання), але в кінцевому підсумку вона шкодить конкретній людині. В залежності від соціальної мережі нападки можуть мати форму текстових чи голосових повідомлень, відео, сторіз, картинок.

Наклеп Агресор поширює неправдиву інформацію. В цифровому середовищі наклеп, так само як і нападки, не обов'язково може мати форму брехливих текстів, а міститись у мемах, змонтованих відео, відфотошоплених зображеннях.

Гріфінг є різновидом кібербулінгу **у комп'ютерних іграх**, коли відбувається спрямоване притиснення одного з учасників комп'ютерної гри: цілеспрямоване вбивство персонажа, нападки у ігровому чаті, обмеження доступу до ресурсів та інші способи персонально заважати грі конкретного персонажу. Метою гріфера є зашкодити ігровому процесу та принизити іншого гравця, не отримуючи для свого персонажа ігрових переваг. Так гріфінг відрізняється від звичайного змагання у комп'ютерних іграх.

Публічне розголошення Розміщення у відкритому доступі у мережі інформації приватного характеру. Це може бути особисте фото, скріни приватної переписки, записи розмов. Будь-що, що ви хотіли б зберегти у таємниці. Розголошення інформації про сексуальну орієнтацію та гендерну ідентичність іншої людини без її згоди це також публічне розголошення, що має назву **аутинг.** Часто публічному розголошенню передує ошуканство — отримання персональної інформації «по секрету», щоб потім передати тим, кому вона не призначалася, або оприлюднити. Часто публічне розголошення приватної інформації у поєднанні із персональними даними (номером телефону, адресою проживання тощо) може супроводжуватись закликами до насильства, які підбурюють до того, щоб насильницькі дії виходили в офлайн.

Самозванство — це злам сторінки та надсилання повідомлень або публікація фотографій від імені жертви. Агресивні або наклепницькі пости, що розповсюджуються самозванцем, викликають зворотню агресію і справжня людина, якій належить акаунт, стає жертвою і втрачає репутацію. Часто жертва навіть не знає, що зловмисник отримав контроль за акаунтом і діє від імені іншої людини.

Кетфішинг схожий на самозванство, але в цьому випадку створюється фейковий акаунт і від імені жертви кібербулінгу пишуться повідомлення або оприлюднюється фейкова інформація чи приватні матеріали.

Кібергрумінг – побудова дорослим довірливих стосунків з підлітком з метою сексуального насильства онлайн чи у реальному житті. Нерідко кібегрумінг переростає також у сексторшен, коли незнайома людина спочатку втирається до жертви у довіру, а потім вимагає приватні матеріли, фото чи відео інтимного характеру. Далі з такими фото і відео легко шантажувати жертву, вимагаючи додаткових матеріалів чи грошей або знущатись через публічне розголошення. Чи треба казати, що дорослі, які вчиняють кібергрумінг або сексторшен ховаються за віртуальними особистостями однолітків і ніколи спочатку не проявляють своїх реальних намірів?

Секстинг – пересилання особистих інтимних фотографій, повідомлень інтимного змісту.

Онлайн-відчуження шкодить пасивно. Жертву можуть ігнорувати у спільних чатах або навіть видалити з онлайн-групи.

Тролінг — кепкування у коментарях не завжди є безневинним і може принижувати людину, а, отже, бути проявом кібербулінгу.

Переслідування (сталкінг) — небажане нав'язування уваги. Сталкер може переслідувати постійними повідомленнями, коментарями усіх подій в житті жертви або вийти в офлайн і шпигувати за людиною. Небажані подарунки, вимоги зустрітися і спілкуватися, нав'язливі «випадкові зустрічі» і умовляння, залякування це також сталкінг.

Хепіслепінг (happy slapping) — відносно новий вид кібербулінгу, який починався в англійському метро, де підлітки, прогулюючись пероном, раптом ляскали один одного, тоді як інший учасник знімав цю дію на телефон і розповсюджував у інтернеті. У подальшому за будь-якими відеороликами, у яких записано реальні напади, закріпилась назва хепіслепінг. Ці відео розміщують в інтернеті, де його можуть продивлятись тисячі людей, зазвичай без жодної згоди жертви. Це саме по собі неприємно, і, до того ж, може викликати наклеп, насмішки і агресію по відношенню до людей, схожих на жертв хепіслепінгу.

Флеймінг (flaming) — обмін короткими гнівними й запальними репліками між двома чи більше учасниками в «публічних» місцях Інтернету, на чатах, форумах, дискусійних групах. Як і тролінг, безневинна перепалка відрізняється від флеймінгу метою принизити жертву.

Порнопомста — поширення в інтернеті фото та відео інтимного змісту інших людей із принизливими написами, або на спеціальних сайтах, через які надають сексуальні послуги. Фото і відео, які використовуються у порнопомсті, зовсім не обов'язково мають бути реальними – фото і відеоредактори допомагають робити фейки, використовуючи картинки з інтернету і фото (відео) з соціальних мереж.

Секстінг, кібергрумінг, сексторшен, кіберпереслідування та порнопомсту вважають кібернасильством.

Попри всі відмінності у різновидах кібернасильства та кібербулінгу, вони спільні у наступному: через інтернет можливість принизити, образити, тероризувати реалізується тільки за допомогою комп'ютера або мобільного телефону. Для кіберагрессора не обов'язково мати фізичну силу, авторитет і вплив на однолітків чи менших, щоб відчувати свою перевагу. До того ж, потужним двигуном кібербулінгу є анонімність. Люди здатні відчувати безкарність і наважитись робити багато чого, коли їх не бачать, не чують і не знають, хто вони насправді.

Найпоширенішими місцями кібербулінгу є

- Соціальні мережі, такі як Facebook, Instagram, Snapchat і Tik Tok
- Текстові повідомлення та месенджери — програми обміну повідомленнями (Telegram, Viber тощо)
- Онлайн-форуми, чати та дошки оголошень
- Електронна пошта
- Спільноти онлайн-ігор

Проте небезпека кібербулінгу не обмежується лише кіберпростором. Приниження і насильство, що почалось в інтернеті, може вийти офлайн і перетворитися на приниження чи переслідування в реальному світі. Бо мета «реального» булінгу та віртуального однакова — образити, принизити, залякати.

ЩО РОБИТЬ КІБЕРБУЛІНГ ТАКИМ ШКІДЛИВИМ?

Більшість форм є **публічними** – багато людей можуть побачити і, таким чином, примножити приниження жертви.

Швидко **поширюється і «віруситься».** Особливо це стосується випадків, коли булер використовує меми жорстоко висміюючи жертву або розповсюджуючи наклеп.

Буває **важко уникнути**, особливо якщо цькування відбувається на публічному майданчику. Кібербулінг легко може одночасно охопити величезну аудиторію і проявитись будь-де і будь-коли.

Анонімність кривдника або використання ним чужої віртуальної особистість. Це також ускладнює притягнення до відповідальності.

Кібербулінг морально легший за реальний. У віртуальному просторі агресор не бачить реакції жертви (тільки екран комп'ютера чи телефона), і рішитися на моральні порушення йому легше.

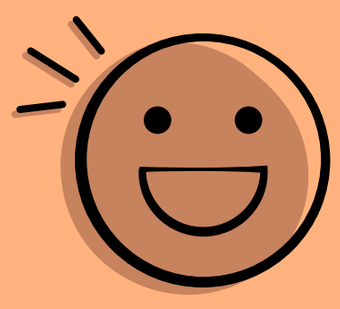
Видалення кібербулінгу **може бути важким процесом**, адже образливі і принизливі тексти, фото і відео легко копіюються і репостяться.

Жертві **ніде не можна сховатися**, бо навіть коли людина іде з онлайну, вона знає і розуміє, що процес цькування там може продовжуватися. Людині може здаватися, що кривдники її переслідують постійно і навіть вдома вона не почувається у безпеці.

Через соціальні мережі та спільноти в інтернеті **поширення будь-якої інформації відбувається блискавично.** Один клік – і принизливі фото, відео, відфотошоплені фейкові зображення, чутки сягають величезної кількості адресатів. Потрапивши до інтернету, інформація залишається там надовго та може з'являтись на різних ресурсах. Це справжній рай для того, хто цькує інших, тобто вдається до кібербулінгу.

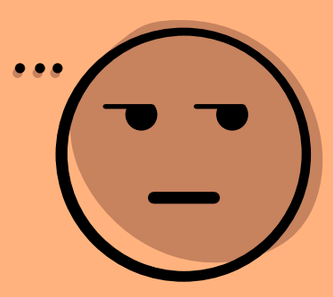
Так кіберагрессори, не прикладаючи суттєвих зусиль, можуть цілодобово залякувати своїх жертв, створюючи в них ілюзію повного контролю їхнього життя і поведінки. Підлітки, що стали жертвами булінгу, часто не розповідають про це, бо відчувають свою провину за те, що сталося, бояться, що будуть покарані за «донос» або погіршиться ставлення до них з боку дорослих чи друзів. Це захоплює агресора, укріплює його відчуття безкарності і його методи стають більш жорстокими і наносять все більшої шкоди жертві.

КІБЕРБУЛІНГ ШКОДИТЬ РІЗНИМИ СПОСОБАМИ



Ментально

Жертва кібербулінгу відчуває смуток, пригніченість, навіть злість через те, що почувається безглуздому становищі. Це з часом виснажує. Відчуття того, що з тебе насміхаються або переслідують, може заважати ділитися пережитим, шукати допомоги або намагатися іншими способами боротися з проблемою. Це відбивається на навчанні: зникає цікавість до знань, складніше стає впоратися із завданнями і, навіть, просто примусити себе взятись за якісь справи.



Емоційно

Незважаючи на те, що у цькуванні винуватий тільки агресор, жертви кібербулінгу переживають відчуття сорому. Емоційне виснаження призводить до втрати цікавості до речей і занять, які раніше викликали захопленняі і приносили задоволення. З іншого боку, стає складно контролювати емоції і найменші проблеми призводять до агресії і конфліктів: з друзями, батьками, вчителями.

Фізично

Емоційні та ментальні негаразди впливають на фізичний стан. Так, може з’являтись відчуття втоми і поряд із ним проблеми зі сном (безсоння). Нерідко спостерігаються такі симптоми, як біль у животі, м’язах, головний біль.

У КРАЙНІХ ВИПАДКАХ КІБЕРБУЛІНГ МОЖЕ ПРИЗВЕСТИ НАВІТЬ ДО СПРОБ СУЇЦИДУ

Що робити тим, хто став об’єктом кібербулінгу?

Найголовніше – **не замикатись у собі і шукати підтримки.** Дуже важливо пам’ятати, що насильство (у тому числі в інтернеті) ніколи не буває виправданим і **завжди винен той, хто його чинить.** Проблемою треба поділитись і шукати шляхи її вирішення разом із тими людьми, яким **довіряєш.**

Іноді кривдник відступає, коли не отримує реакції на перші закиди. Не варто витрачати час і зусилля на сперечання, виправдування і взагалі на відповіді на образливі коментарі. Хоча це й складно, треба спробувати ігнорувати образи, адже у випадку із тролінгом і флеймінгом збільшення кількості коментарів – одна із цілей, яку переслідують кривдники. Крім того, виплескуючи негативні емоції (у тому числі спровоковані) у соціальну мережу, ми несемо і помножуємо негатив далі.

Важливо розуміти: доречно ігнорувати поодинокий негатив, часто в результаті цього кібербулінг на початковій стадії і зупиниться. Щоб не дратуватись, можна відключити сповіщення месенджера на якийсь час, перевести телефон у режим «не турбувати». Пауза в спілкуванні руйнує взаємопідсилювані автоматизми кібербулінгу, особливо якщо він мотивований втечею булерів від нудьги та не супроводжується булінгом у реальному житті. **Якщо ж булер не припиняє агресію – блокувати.** Так само блокувати треба підозрілу людину, або тих, хто залякує. Для цього у всіх соціальних мережах є опція «заблокувати».

Крім того, **у соціальних мережах є центри безпеки.** Прочитайте, як ви можете поскаржитись на принизливу чи образливу публікацію і робіть це у випадку необхідності. Також можна заборонити людям відзначати себе в записах і на фотографіях. Якщо сервіс, на якому стався випадок кібербулінгу, модерований – не треба соромитись скаржитись модераторам. Якщо образлива інформація розміщена на сайті, варто зробити запит адміністратору щодо видалення цієї інформації.

Булінг, у тому числі у цифровому середовищі, **це правопорушення**, за яке передбачена відповідальність. Але, щоб правоохоронні органи змогли виконувати свою функцію, їм будуть необхідні докази. Такими доказами можуть бути збережені посилання на пости чи сторінки, де розміщена неправдива інформація і скріншоти (або роздруківки) таких матеріалів. Не виключено, що у випадку, коли справа дійде

до розслідування, зловмисник пробуватиме «підчистити» історію.

Тому докази варто зберігати заздалегідь. Потурбуйтесь, щоб на скріншоті або записі екрану було видно адресу сторінки (посилання), соціальну мережу (або сайт), де були розміщені образливі пости, дату та час публікації і автора. Якщо кривдником є хтось із класу, такі матеріали будуть підставою для того, щоб до порушника вжила заходів адміністрація школи. Для правоохоронців треба буде зберегти докази систематичного булінгу (тобто такого, що стався два і більше разів).

Про випадки кібербулінгу у класі чи школі треба повідомляти адміністрацію школи. Директор, завуч та інші уповноважені особи зобов'язані не лише реагувати на такі випадки, але й ставити до відома поліцію. За багатьма школами закріплені шкільні офіцери поліції. До них теж варто звернутись за допомогою.

Від особистих негативних наслідків, які спричиняє кібербулінг, може допомогти «**цифровий детокс**». Обмежте на деякий час користування соціальними мережами. Переключіть свою увагу, займіться іншими справами. Разом з батьками буває корисним навіть змінити номер телефону чи створити нові сторінки у соціальних мережах, про які повідомити тільки тих людей, до яких є довіра. У нагоді стане візит до психолога чи дзвінок на «гарячу лінію». **(Деякі корисні контакти дивись на останній сторінці цієї брошури).**

Обов'язково варто розповісти батькам, якщо агресором є незнайома людина і є підозра, що зловмиснику відомі адреса, школа, гуртки, секції і подробиці звичайного розпорядку дня.

Якщо погрози є досить серйозними, стосуються життя або здоров'я, то ви маєте право на захист з боку правоохоронних органів. Так само треба повідомляти поліцію, якщо повідомлення булера містять порнографічні матеріали.

ЩО РОБИТИ ТИМ, ХТО СТАВ СВІДКОМ КІБЕРБУЛІНГУ?

Виступити проти булера. У соціальних мережах можна по-різному дати зрозуміти, що такі дії оцінюються негативно. Крім того, булер може сприймав мовчання як підтримку і нарощувати агресію. Важливо самим при цьому не вдаватись до агресії. Те, що ви з кимось не погоджуєтесь, не дає вам права бути грубим або ображати інших.

Підтримати жертву. Це варто робити як особисто, так і в публічному віртуальному просторі. Для публічного простору найкраще підходить форма підтримки, з якої зрозуміло, що ви вважаєте що кібербулінг – це погано. Цим Ви надаєте емоційну підтримку, так необхідну жертві і водночас виступаєте проти булера.

Поскаржитись на образливий пост. Центри безпеки соціальних мереж так влаштовані, що збільшення кількості скарг пришвидшує реагування на них.

Повідомити дорослим про факт некоректної поведінки в кіберпросторі. Особливо, якщо ви стали свідком не одноразової агресії, а систематичного цькування жертви.

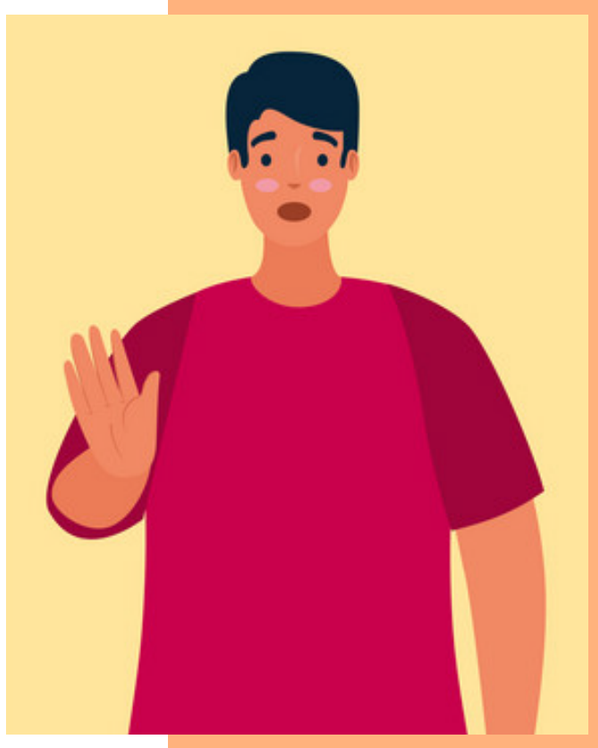
ЗАКОНОДАВЧИЙ ЗАХИСТ

В Україні вже на сьогодні включені до законодавства норми, що регулюють правопорушення, пов'язані саме з кібербулінгом. Так, адміністративна відповідальність передбачена:

Ст. 173-4 Кодексу України про адміністративні правопорушення (КУпАП) «**Булінг (цькування) учасників освітнього процесу**». За цією статтею можна притягнути до відповідальності булерів, які діють у школі. Санкція статті передбачає **штраф від 50 до 100 неоподатковуваних мінімумів доходів громадян (від 850 до 1700 грн) або громадські роботи на строк від 20 до 40 годин.** Якщо порушення вчинене групою осіб або повторно протягом року після накладення адміністративного стягнення, це тягне за собою штраф від 100 до 200 неоподатковуваних мінімумів доходів громадян (від 1700 до 3400 грн) або громадські роботи на строк від 40 до 60 годин. Якщо ці діяння вчинені **малолітніми або неповнолітніми особами** віком від 14 до 16 років, **штраф накладають на батьків** або осіб, які їх замінюють (від 850 до 1700 грн, або громадські роботи на строк від 20 до 40 годин). Діяння, передбачене ч. 2 цієї статті (тобто вчинене групою осіб або повторно протягом року), вчинене малолітньою або неповнолітньою особою віком від 14 до 16 років, тягне накладення штрафу на батьків або осіб, які їх замінюють, від 100 до 200 неоподатковуваних мінімумів доходів громадян або громадські роботи на строк від 40 до 60 годин.

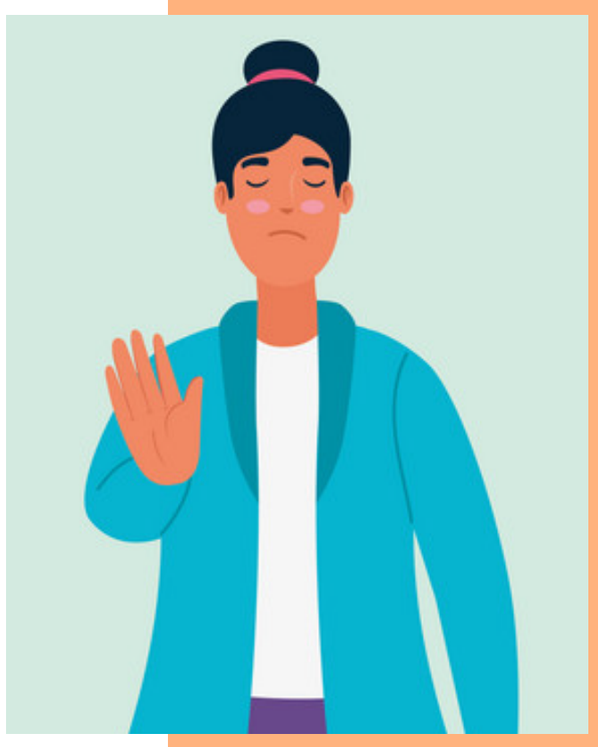
Неповідомлення керівником закладу освіти уповноваженим підрозділам органів Національної поліції України про випадки булінгу (цькування) учасника освітнього процесу **карається штрафом від 850 до 1700 грн або виправними роботами на строк до 1 місяця з відрахуванням до 20% заробітку.**

ЯК ПОПЕРЕДИТИ ВИНИКНЕННЯ НЕБЕЗПЕЧНИХ СИТУАЦІЙ У ІНТЕРНЕТІ?



Не поширюйте у відкритому доступі та у переписці із людьми, з якими ви знайомі тільки віртуально, **свої особисті дані**, такі як: номер телефону, адреса, дані батьків, паспортні дані.

Наші публікації у соціальних мережах **можуть бути справжнім скарбом для зловмисників**, що полюють за чужими профілями. Подумайте, чи може незнайома людина, використовуючи те, про що ви пишете чи фотографуєте, отримати доступ до вашого акаунту.



Пам'ятайте про **чутливі дані**. До них належить медична інформація, дані про сексуальну орієнтацію і гендерну ідентичність, стан здоров'я, статеве життя, дані про те, чи була особа жертвою якихось видів насильства, дані про етнічну, релігійну приналежність і ще багато чого. Особливо якщо це дані про інших людей. Розповсюджуючи їх у відкритому доступі можна ненавмисно стати співучасником кіберправопорушення.

Якщо ви натрапили на образи, переслідування, бачите щось підозріле, не треба закриватися і вирішувати це самостійно. **Не треба боятися поділиться цим** із сім'єю, друзями, близькими людьми. Не відмовляйтеся від підтримки та **шукайте допомогу**. Особливо у дорослих.

Якщо ви стали свідком кібербулінгу або насильства, **не проходьте повз.** Пропонуйте свою допомогу жертві і активно виступайте проти таких випадків публічно.

Не перетворюйтесь самі **на агресора**. Так, образи викликають сильні емоції, але чи варто керуватись ними? У випадку із тролінгом ви не лише граєте на руку тролю, але й ризикуєте викликати на себе інші форми кібербулінгу.

Проте, поведінка, що убезпечує від агресії в інтернеті, це лише частина того, що можна зробити для вибудовування безпечного віртуального простору.

Подбати про свою систему кібербезки варто і на рівні вживання різноманітних засобів захисту своїх профілів і акаунтів, а також впроваджуючи **корисні звички кібергігієни.**

Одною з **центральних небезпек**, з якими ми стикаємось у інтернеті, є отримання неправомірного **доступу до акаунтів у соціальних мережах** та в інтернет-сервісах, таких як електронна пошта або онлайн магазин ігор. З одного боку, «зламавши» акаунт зловмисник отримує доступ до нашої особистої інформації і може використати її для агресії, спрямованої на нас же. З іншого – крадіжка чужої віртуальної особистості дозволяє цькувати інших, просити від чужого імені гроші, розсилати спам чи шкідливе програмне забезпечення, а також видобувати із особистої переписки з друзями інформацію, за допомогою якої шкодити нашим друзям і знайомим. Крім того, особиста інформація, яку ми зберігаємо у приватних акаунтах, **може бути використана для переслідувань у реальному світі.**

ЧОМУ КІБЕРБЕЗПЕКА ВАЖЛИВА?

Більшість сервісів, якими ми користуємося щодня, управляється через Інтернет: від розрахунків банківськими картками до електричних мереж, які живлять наші міста. Кіберзахист дозволяє їм функціонувати як слід – це оборонна стіна, яка стримує кібератаки. Кібератаки можуть мати різні мотиви: від політичних до фінансових, включаючи розважальні. Отже, державні органи і бізнес докладають багато зусиль у побудову надійних систем кіберзахисту. Втім, захист приватних акаунтів і комп'ютерів так само є важливим, адже за висновками безпекової компанії Check Point, 49% організацій не можуть виявити атаку, якщо вона відбувається через особистий пристрій співробітника. Такі атаки полягають у викраденні даних, що надалі можуть стати джерелом для того, аби отримати інформацію для агресора, кібершпигуна чи для інших злочинних намірів. Отже, злам приватного акаунта може призвести до вразливості більшої і важливішої системи.

Щоб розуміти, які навички перебування в інтернеті працюватимуть на користь захисту від зловмисників, треба розуміти, як саме можуть нападати на наші акаунти і профілі мисливці за даними.

Якими можуть бути кібератаки?

ЗАЛЯКУВАННЯ

Також спосіб відомий як шахрайські програми, програми, які вводять в оману, шахрайські сканери – заплутують жертв, змушуючи повірити, що їм загрожує небезпека. Наприклад, ви можете отримати повідомлення, що ваш пристрій заражений вірусом, проте насправді це буде лише спливаюче вікно, а от гроші, які вимагаються – справжніми.

ПІДБІР ПАРОЛІВ

Іноді для того, щоб підібрати пароль до акаунту, зловмисникам не потрібно напряму контактувати із людиною. Так, маючи вкрадену базу паролів з якогось сервісу, шахраї можуть отримати доступ до інших акаунтів, де користувач використав той самий пароль.

Підібрати пароль (або відповідь на секретне питання щоб встановити новий пароль) іноді можна, використовуючи інформацію з відкритих джерел. Ім'я домашнього улюбленця, дата народження, дружнє прізвисько і ще багато особистих подробиць можна знайти, просто полиставши публікації людини і її друзів у соціальній мережі. Не найкраща ідея використовувати такі дані для захисту доступу до свого акаунту.

ШКІДЛИВІ ПРОГРАМИ

Шкідливе програмне забезпечення – це будь-які шкідливі програми, які використовують дані користувача для власної вигоди. Вони можуть атакувати ваш комп'ютер рекламою або працювати як клавіатурні шпигуни, які фіксують кожне натиснення клавіш клавіатури. Існують також програми-вимагачі, які заражають пристрій і шифрують всі його дані. Якщо жертва нападу хоче знову отримати доступ до даних на своєму пристрої, їй доведеться заплатити викуп.

ПСИХОЛОГІЧНІ МАНІПУЛЯЦІЇ (СОЦІАЛЬНА ІНЖЕНЕРІЯ)

У кібератаках активно використовують психологічні маніпуляції – сукупність прийомів, які змушують нас робити те, що хоче зловмисник. Це загальний термін, який включає фішинг, вішинг, кетфішинг, претекстинг і таке інше.

Найбільш популярні - **фішингові атаки**, коли шахраї використовують будь-яку форму зв'язку (електронну пошту, повідомлення в месенджерах, чатах) для виловлювання інформації. Такі повідомлення мають вигляд ідентичний до повідомлень із надійних джерел: організації, знайомі вам люди. Від людини хочуть, щоб вона перейшла за посиланням (як правило, на фальшиву сторінку, за допомогою якої надалі вкрадуть дані) або завантажила вкладення (скоріш за все це буде шкідливе програмне забезпечення) або ввела свої дані на сайті (і там їх використають як хочуть зловмисники). Популярні також різновиди фішингу: **смішинг та вішинг**, в яких використовується телефонний зв'язок: розсилаються СМС (у тому числі з підроблених номерів телефонів) або виманюються дані під час спілкування по телефону. Часто такі атаки супроводжуються методом **претекстінгу**, коли зловмисник видає себе за особу, відому потенційній жертві, або представника кол-центру, технічної підтримки тощо, і, щоб викликати довіру, повідомляє співрозмовнику якусь інформацію про нього (наприклад, прізвище, адресу, дату народження тощо). При типі атаки «**привид**» зловмисник використовує підроблену особистість і вимагає доступу до даних. Метод «**емоційної бурі**» використовують ті, хто розсилає так звані «WOW- повідомлення» ніби то від імені друзів і знайомих у соцмережах, месенджерах. Це гра на природній цікавості та емоційності користувачів. Як правило це короткі повідомлення типу «Подивись, це ти?» або «Двивсь, що знайшла», зміст яких має спонукати перейти за посиланням у тілі повідомлення.

QUID PRO QUO

(Шахрайство із техпідтримкою) це ситуації, коли шахраї видають себе за співробітників відділу інформаційних технологій чи іншого постачальника технічних послуг і під виглядом супроводження якоїсь операції (зміни пакету послуг, налаштування доступу, усунення технічних труднощів тощо) і надають вказівки жертві, виконуючі які, отримують доступ до, наприклад, телефонного номеру чи банківського рахунку.

АТАКА ЧЕРЕЗ ПРИМАНКУ

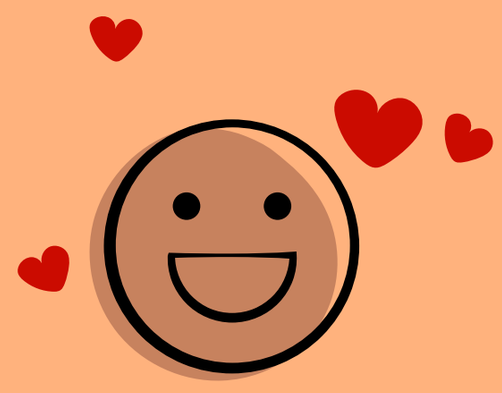
Примушує користувачів віддавати свої дані взамін на обіцянку якоїсь винагороди. Винагорода може бути будь-якою: від обіцянки грошей чи призу до віртуальних «винагород», таких як гороскоп, результат тесту тощо. Отримали повідомлення типу «я йду з гри, зайди сюди забери з мого акаунту потрібне» - будьте певні, що посилання фальшиве і через кілька хвилин ви втратите доступ до свого профілю.

РОМАНТИЧНІ АФЕРИ

Романтичні афери здійснюють з **фальшивих акаунтів** або крадених профілів. Трохи неймовірних історій, брехні про те, чому неможна використати своє фото на аватарці і далі спочатку обережні, а потім все наполегливіші прохання про «допомогу». Довіра зростає, а от наша безпека тане.

СУМІСНИЦТВО/ЗАДНІЙ ХІД

Популярний тип атаки, коли авторизована особа надає іншому доступ до обмеженої зони. «Можна я з твого акаунту подивлюсь, що робиться у когось?» може бути виправданим цілком обґрунтованою на перший погляд причиною. Так само як і «підтверди, що це я, бо забула пароль до профілю». А от наслідки крадіжки даних чи дії з-під чужого акаунту – дуже різними.



Попри різноманіття методів соціальної інженерії їх об’єднує **одна мета:** жертва надає доступ до своїх даних самостійно, внаслідок омани або маніпуляцій. Втім, є низка ознак, за якими **атаки** з використанням соціальної інженерії **можна розпізнати.**

Одна з них — **погана граматика та правопис або, навпаки, занадто офіційна лексика.** Ще однією помітною ознакою є почуття терміновості, яке зловмисники намагаються створити для зменшення пильності жертви. Тут у діло ідуть емоційні слова типу «терміново», спеціально виділені дати (час) або фразу типу «залишилось лише Х годин». Будь-який запит щодо конфіденційних даних також має викликати підозру: авторитетні компанії ніколи не просять відправити їм паролі або інші особисті дані електронною поштою або текстовими повідомленнями.

Одне з ключових правил для ідентифікації атаки з використанням соціальної інженерії – увага до джерела повідомлення. Якщо ви отримали лист на електронну пошту, уважно роздивиться адресу. Офіційні повідомлення не приходять із скриньок безкоштовних поштових сервісів. Крім того, фальшива електронна адреса може маскуватись під «солідним» іменем користувача. Витратьте хвилинку і подивиться саме на адресу. Схожа на офіційну? Погугліть офіційні адреси (вони є на сайтах в розділі «контакти»). Все ще підозріло? Запитайте у служби підтримки. За схожимиправилами варто перевіряти повідомлення у месенджерах ніби від друзів. Спробуйте зв'язатись альтернативним способом (через інший месенджер або зателефонувати). Не зайвим буде репитати у спільних знайомих, чи отримували вони дивні повідомлення також. При фішингу як правило використовують масову розсилку абсолютно однакових повідомлень. Це – одна з ознак, що від імені вашого друга з вами спілкується хтось інший.

Від **шкідливих вкладень у розсилці захищають якісні антивірусні програми**. Не забувайте їх оновлювати. Ніколи не слід відкривати одразу вміст додатків або переходити за посиланням. Якщо мова йде про пересланий файл, краще його зберегти і перевірити, чи це справді текстовий документ, а не програма, яка самостійно запуститься на вашому гаджеті. Багато браузерів і поштових клієнтів має функцію попереднього перегляду. Достатньо навести мишкою на вкладення (не клікати!) і подивитись, чи справді вам надіслали те, на що ви очікуєте.

Завжди з недовірою ставтесь до **посилань**, які ведуть на сторінку, де просять ввести **особисті дані**. Краще окремо зайти на сайт компанії чи сервісу, адже фальшиві сторінки часто відрізняються дуже непомітними деталями.

Не слід також забувати і про сповіщення про такі небезпеки друзів чи членів сімей. **Завжди повідомляйте людей**, з чийого акаунту ви отримуєте підозрілі повідомлення. Те саме варто зробити, якщо ви помітили підозрілу активність у себе у профілі чи стикнулись із явною роботою шкідливого програмного забезпечення із свого гаджету чи втратою доступу до власного профілю у якомусь з інтернет-сервісів.

Якщо ж ви таки стали жертвою кібератаки, заснованої на соціальній інженерії – ніколи не платіть викуп. Повідомляйте про інцидент поліцію.

БАЗОВІ ПРАВИЛА КІБЕРГІГІЄНИ

Слідкуйте за інформацією про нові методи кібератак. Про них пишуть у соціальних мережах – варто лише підписатись на відповідні канали, наприклад, кіберполіції, проектів, присвячених кібербезпеці.

Перш ніж натиснути – аналізуйте. Більшість кібератак використовує маніпулятивні техніки, коли емоції переважають над розумом. Нічого не трапиться, якщо ви вікриєте вкладення або перейдете за посиланням на кілька хвилин пізніше.

Переконайтесь у безпечності платформи чи людини, з якими ви взаємодієте. Як це зробити – описано вище.

Регулярно перевіряйте свої акаунти і **видаляйте ті, якими ви не користуєтесь.** Час від часу доречно гуглити себе або шукати по своєму імені і прізвищу у соціальних мережах, а також використовувати пошук по фото (за допомогою сервісу пошуку по зображенням google або інших, наприклад, https://tineye.com чи подібних). Зловмисники іноді крадуть фото зі сторінок, створюють профілі під іншими іменами і таким чином вводять в оману ваших друзів, які думають, що це – ваш запасний профіль під іншим іменем.

Використовуйте лише найновіші версії програмного забезпечення і вчасно їх оновлюйте. Оновлення програмного забезпечення часто містять виправлення вразливостей безпеки, якими можуть скористатися злочинці.

Не використовуйте піратські копії програмного забезпечення. Сама програма цілком може бути чистою, а от файл, за допомогою якого ви «обходите» захист виробника, цілком може бути вірусом чи шпигунською програмою. Як альтернативу варто пошукати безкоштовне програмне забезпечення чи онлайн-сервіси або використати можливість підписки на місяць, наприклад.

Уникайте використання застосунків російських розробників: ВК, Одноклассники, Яндекс.Браузер, 1С, Mail.ru та інші – росіяни можуть їх відслідковувати. Перед завантаженням обов'язково перевіряйте інформацію про те, хто розробник та власник застосунка, чи не заборонений він в Україні.

Обачливо ставтесь до банерів чи спливаючих вікон.

Перевіряйте, чи слід довіряти персональну інформацію будь-якому ресурсу.

Створюйте резервні копії даних. Для Android це можна робити на гугл-диску (Google Drive), для iPhone – у сервісі iCloud. Налаштувати резервне копіювання можна також на хмарних сервісах Dropbox, OneDrive.

Завжди використовуйте антивірус. Його так само треба вчасно оновлювати. Ідеальний варіант – за допомогою функції автоматичного оновлення.

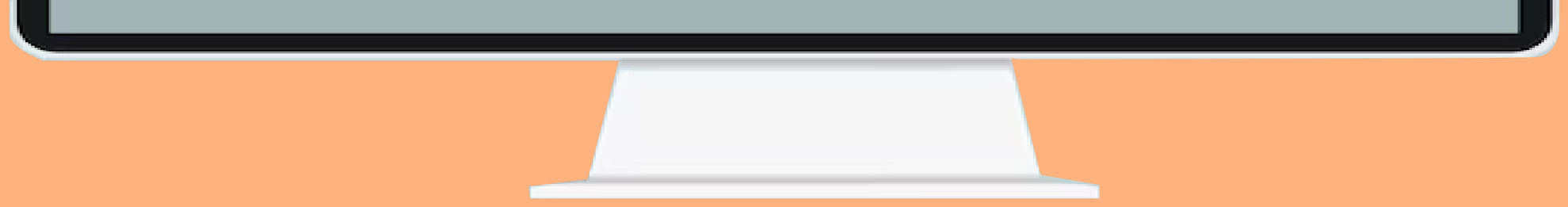
Впроваджуючи ці базові принципи, ви легко вживатимете інші засоби, щоб протистояти різним типам кібератак.

ВИКОРИСТОВУЙТЕ НАДІЙНІ ПАРОЛІ

Більшість ваших пристроїв та облікових записів захищається за допомогою паролів. **Ненадійні паролі – легка здобич** для ворожих хакерів і шахраїв. Зверніть увагу: саме паролі у множині. Людина, що використовує один і той же, навіть дуже складний пароль для різних сервісів – справжній подарунок для зловмисників.

Замініть паролі в соцмережах та на всіх сайтах, де може бути ваша персональна інформація, **на надійніші та регулярно їх змінюйте**. Так само варто час від часу перевіряти паролі на витік. Сучасні операційні системи та антивіруси теж мають таку функцію перевірки. Не нехтуйте, якщо ви отримуєте такі повідомлення і змінюйте паролі.

Згенерувати надійний пароль допомагають менеджери паролів – це спеціальні застосунки, які зберігають ваші паролі в зашифрованому вигляді, і вам не доведеться запам'ятовувати всі складні комбінації, а лише пароль від самого застосунку. Використовувати менеджери паролів можна як на комп'ютерах, так і на смартфонах. Радимо надавати перевагу програмам відомих розробників (**1Password, Bitwarden, KeePass тощо**). У будь-якому разі перед встановленням перевіряйте репутацію продукту, знайомтеся з відгуками з точки зору безпеки. Пошукайте, чи не було повідомлень про виявлені вразливості.



Додатковим захистом і підсиленням надійності паролю є двофакторна аутентифікація – це звичайна двоетапна перевірка при вході в акаунт. Налаштуйте її. Тоді при спробі зламу ви отримаєте SMS-повідомлення з проханням підтвердити вхід в акаунт (або кодом, який треба ввести). Лиш зверніть увагу, що зловмисники можуть пробувати «виманювати» у вас цей код. Він не призначений, щоб передавати його службі підтримки. Виключно для того, що підтвердити вхід на самій платформі інтернет-сервісу.

Встановлюйте паролі для розблокування пристроїв і доступу до сім-картки. **Замініть стандартний PIN-код до SIM-карти.**

ПЕРЕВІРТЕ СВОЇ ПАРОЛІ НА НАДІЙНІСТЬ

1 не містять поширених поєднань букв і слів; символів, що повторюються або йдуть один за одним (0000, 1111, abc123); вашого імені, прізвища, дати народження; імені, прізвища або дати народження ваших батьків, дітей, чоловіка або дружини та іншої інформації, якає про вас у відкритому доступі.

2 натомість містять спеціальні символи, цифри, великі та малі літери в кількості понад 8, а також слова, яких немає в українській чи англійській, і, бажано, в інших мовах теж.

3 створені за допомогою сервісу генерування паролів.

4 використовуються тільки в одному сервісі (на кожен сервіс чи поштову скриньку – свій унікальний пароль).

5 не зберігаються у вас на смартфоні або ноутбуці в нотатках чи на наліпці на вашому ноутбуці. До речі, камери телефонів постійно удосконалюються і, цілком можливо, що така записка потрапить у кадр селфі і надалі – у відкритий доступ у мережу.

6 регулярно змінюються та істотно відрізняються від минулого пароля, що використовувався на цьому ж сервісі.

7 їх не знають ваші рідні, друзі, кохані, колеги.

Як безпечно завантажувати й використовувати застосунки та файли

Кіберзлочинці постійно вигадують нові способи для обману користувачів через шкідливі застосунки та програми. Завантажити безкоштовний фільм, гру чи музику – завжди є ризик інфікування шкідливим програмним забезпеченням. А мета зловмисників – отримати доступ до вашої особистої інформації.

Як зазначено вище, **безпечніше віддавати перевагу ліцензійному програмному забезпеченню**, завантажуючи його із перевірених джерел - офіційних сайтів або з ліцензованих носіїв. У ліцензійних програм є ще одна перевага – своєчасне автоматичне оновлення. Розробники, що випускають програми, завжди дуже уважно слідкують за виявленими атаками і вразливостями програм, оперативно реагують на виявлені проблеми та постійно працюють над покращенням своїх безпекових протоколів.

Обираючи безкоштовну альтернативу платним програмам, так само треба звертати увагу на джерело завантаження, адже безкоштовні програмні продукти так само розповсюджуються через офіційні сайти, а їх розробники дбають про безпеку. Завантаження файлів і застосунків із невідомих джерел (особливо, якщо це анонімні сервіси для обміну файлами) завжди ризиковане з точки зору «підхопити» шкідливе програмне забезпечення. Як альтернативу піратським програмам варто розглядати онлайн-сервіси. Відомі онлайн-сервіси так само вживають безпекових заходів і не допускають, щоб через них шкодили користувачам.

Корисною безпековою звичкою є **завжди перевіряти завантажені файли антивірусом**, а ще краще: налаштувати автоматичну перевірку у програмі.

Контролюйте дозволи, які запитує програма чи застосунок під час встановлення. Не всім застосункам для роботи необхідний доступ до вашої геолокації чи персональної інформації. Запит на доступ до великої кількості даних, як і до даних чи функцій телефона, які очевидно не пов'язані із призначенням застосунку (наприклад, застосунок «ліхтарик» точно не взаємодіє з фото), є приводом для того, щоб поцікавитись, чи є він безпечним.

БЕЗПЕЧНІ НАЛАШТУВАННЯ БРАУЗЕРІВ ТА МЕСЕНДЖЕРІВ

Зменшити кількість потенційних контактів зі шкідливим програмним забезпеченням та ризик випадково перейти за небезпечним посиланням, а також зменшити кількість небажаних повідомлень можна за допомогою правильних налаштувань браузерів та месенджерів.

Завжди вказувати місце для завантаження.

У налаштуваннях телефону треба обрати заборону встановлення застосунків з неперевірених джерел та автоматичного завантаження файлів, а для браузера – увімкнути функцію «щоразу запитувати про місце зберігання файла перед завантаженням» або аналогічну. У такому разі, навіть якщо ви випадково перейдете за посиланням, яке автоматично розпочинає процес завантаження, він не розпочнеться, поки ви не підтвердите це. Тож у вас буде можливість ще раз подумати, чи варто це робити. Для Chrome це можна зробити у розділі налаштувань «Завантажені файли», Firefox - Файли і програми, Opera – Завантаження.

Більшість популярних месенджерів дозволяє обмежити коло спілкування і доступ до вас з боку невідомих абонентів.

У месенджері **Telegram** рекомендується застосовувати двоетапну перевірку (пам’ятайте про цнікальний пароль) та встановити наступні налаштування:

Хто може бачити номер телефону

НІХТО Усі

Хто може знайти за номером

Мої контакти Усі

Хто може бачити фото та відео мого профілю

Мої контакти Усі

Хто може додавати посилання на мій обліковий запис під час надсилання моїх повідомлень

Мої контакти Усі

Хто може бачити мої відвідини

НІХТО Усі

Хто може мені телефонувати

Мої контакти /НІХТО Усі

У розділі “Виклики” для Peer-to-peer слід також встановити значення – Мої контакти (це параметр, який дозволяє отримувати або не отримувати вашу IP-адресу користувачам, які вам телефонують)

Хто може додавати мене до чатів

Мої контакти Усі

Аналогічні налаштування доступні для **WhatsApp**

Налаштування > Обліковий запис > Двоетапна перевірка > Увімкнути

Востаннє в мережі

НІХТО Усі

Фото профілю

Мої контакти Усі

Групи

Мої контакти Усі

Крім того, у WhatsApp корисно вимкнути автоматичне завантаження до фотоальбому надісланих зображень.

У месенджері **Viber** за допомогою параметру «Виклики і повідомлення» варто активувати опцію «**Блокування невідомих абонентів**». Вкладку “Конфіденційність” налаштуйте таким чином: встановіть тумблер навпроти “**Автоматична перевірка на спам**” зніміть тумблер навпроти “Одноранговий зв’язок” встановіть тумблер навпроти “Запити” Контролюйте, хто може додавати вас у групи – перейдіть в “**Настройка додавання в групи**” і поставте галочку навпроти “Мої контакти”. Також зніміть тумблер навпроти “Пропонувати друзів”.

Зверніть увагу на функції “Запит ваших даних” і “Видалити ваші дані” та перегляньте, які саме дані про вас зберігаються на серверах Viber. **Відключіть опції** “Збирати аналітику”, “Дозволити персоналізацію контенту” та “Дозволити служби точної геолокації”.

Браузери, які і інші програми, потребують регулярного оновлення, а також можуть стати безпечнішими за допомогою деяких налаштувань. Про те, як увімкнути контроль за файлами, що завантажуються, йшлось вище. Нижче – це кілька корисних налаштувань для популярних браузерів.

Один із найпопулярніших браузерів – **Chrome** надає можливість увімкнути опцію «Покращений захист» у розділі «Безпечний перегляд», а також опцію «Завжди використовувати безпечне з’єднання».

Firefox у розділі «Приватність браузера» містить корисні опції «Блокувати небезпечний і шахрайський вміст» та «Увімкнути HTTPS-режим у всіх вікнах». Так браузер не лише заважатиме запуску шахрайського коду, але й попереджатиме про потенційні небезпеки на підозрілих сайтах.

Аналогічно у браузері **Opera** можна активувати опцію «Увімкнути захист від шкідливих сайтів та завжди використовувати безпечні з’єднання».

Куди звертатись за допомогою?

Державні органи та громадські організації надають різноманітну допомогу тим, хто потерпає від зловмисників в інтернеті.

Національна дитяча «гаряча» лінія для дітей та молоді. Професійні психологи і юристи Національної дитячої «гарячої» лінії допоможуть розібратися зі складнощами й вирішити будь-яку твою проблему, в тому числі, пов'язану з цькуванням в онлайні.

0 800 500 225

116 111 **БЕЗКОШТОВНО**

Telegram: @CHL116111
Instagram: @childhotline_ua
Facebook: @childhotline.ukraine

(можна телефонувати на Telegram канал)

Безкоштовний номер: 0 800 500 225 або короткий номер: 116 111 (безкоштовно з усіх мобільних). **Лінія є анонімною та конфіденційною.** Через періодичні перебої в роботі електропостачання можуть бути труднощі із електронним зв'язком, втім фахівці лінії залишаються на зв'язку за допомогою електронних каналів консультування поданих вище.

УГСПЛ. Docudays UA спільно з Українською Гельсінською спілкою з прав людини (УГСПЛ) **пропонують кваліфіковану юридичну допомогу дітям та/чи батькам дітей, які опинились у ситуації кібербулінгу.** Якщо Ви страждаєте від постійних образ в Інтернеті; Ваш аккаунт зламали та поширили особисті дані; чи Ви наразилися на інші небезпеки в мережі — звертайтеся по правову допомогу. **Телефони київської приймальні УГСПЛ: (044) 383 9519, 094 928 6519. Працює в будні з 10:00 до 18:00.** Мешканці інших регіонів України за цими самими номерами можуть дізнатися адреси найближчих до них приймалень УГСПЛ, куди можна звернутися по допомогу.

Поліція. Можна звернутися до поліції за номером 102 (цілодобово).

Правова допомога. Якщо потрібна правова допомога чи порада, звертайтеся до найближчого місцевого центру чи бюро правової допомоги, дізнавшись контакти на сайті **legalaid.gov.ua. Можна зателефонувати та проконсультуватися у фахових юристів, як поводитися, щоб бути в безпеці: 0 800 213 103. Номер працює цілодобово — безкоштовно в межах України.**