ДОДАТКОВІ МАТЕРІАЛИ ІНТЕРНЕТ-КОНФЕРЕНЦІЇ «НА УРОК»

На Урок
освітній проект

БЕЗПЕЧНЕ ІНТЕРНЕТ-СЕРЕДОВИЩЕ

ПОРАДИ, ЯК ГОВОРИТИ З ДІТЬМИ ПРО НЕБЕЗПЕКУ В ІНТЕРНЕТІ

2022
ОСВІТНІЙ ПРОЕКТ «НА УРОК»
https://naurok.com.ua

Поради школярам, як уникнути небезпеки в інтернеті

Для учасників конференції ми підготували перелік потенційних загроз для підлітків у мережі та практичні поради, які допоможуть їх оминути.

Загроза №1. Шахрайство

1.1. Фішинг (отримання доступу до логінів, паролів, банківських даних)

Як уникнути:

- використовуйте сайти, в яких встановлено захищене з'єднання за протоколом https (зліва від адреси сайту має бути значок у вигляді зеленого замку);
- перевіряйте на сайті реальні відомості про авторів та їхні контактні дані;
- не вводьте дані банківських карток на сумнівних сайтах (cvc/cvv-код, термін дії, номер картки);
- не передавайте та не викладайте у вільний доступ конфіденційну інформацію (дані облікового запису, адресу місця проживання, відомості про документ, що підтверджує особу);
- за можливості вимикайте геолокацію.

1.2. Сумнівні інтернет-продажі (підроблені Інтернет-магазини, спільноти у соціальних мережах, дошки рекламних оголошень)

Як уникнути:

- перед здійсненням покупки перевірте відомості про правовстановлюючі документи, наявність угоди на використання та обробку персональних даних, адресу фактичного розташування, дані про споживчі властивості товару;
- не повідомляйте свої персональні дані та не переказуйте кошти стороннім особам, які не є представниками продавця;
- не продавайте особисті речі (вироби, творчі роботи, одяг та ін.) через неспеціалізовані інтернет-сайти, соціальні мережі тощо.

1.3. Збори коштів на «благодійність» (лікування, харчування, покупка медикаментів чи обладнання, допомога тваринам)

Аби переконатися, що ваша допомога досягне адресата:

- проаналізуйте історію групи у соціальних мережах (кількість підписників, періодичність розміщення постів про проведення благодійних акцій);
- перевірте, чи існують аналогічні групи, спрямовані на підтримку цього ж об'єкта (іноді шахраї роблять сторінку-клон з метою перехопити частину відвідувачів спільноти з гарною репутацією);
- зв'яжіться з адміністраторами групи для уточнення деталей, поставте якомога більше запитань, що дозволять визначити їхню причетність до збору коштів;
- спробуйте зв'язатися з родичами/представниками особи, для якої організовано збирання коштів;
- без обговорення з дорослими не переказуйте гроші малознайомій людині, з якою спілкувалися лише в режимі онлайн (які б причини не називав співрозмовник).

1.4. Вірусний контент (вимога здійснити переказ коштів для відновлення доступу до вашого персонального комп'ютера)

Як уникнути:

- не відкривайте та не зберігайте підозрювані файли;
- не переходьте за небезпечними посиланнями, не приймайте будь-які сумнівні угоди;
- встановіть та своєчасно оновлювайте спеціальні захисні програми та фільтри для захисту комп'ютера;
- використовуйте ліцензійне програмне забезпечення з актуальними оновленнями;.
- з обережністю завантажуйте програмні продукти з файлообмінних мереж і торентів.

1.5. Інформація про легкий заробіток для підлітків

Найчастіше така робота пов'язана із залученням школярів до шахрайських чи злочинних схем (наприклад, для розповсюдження наркотичних засобів).

Як уникнути:

- аналізуйте будь-які «привабливі» оголошення на адекватність;
- перевіряйте інформацію про роботодавця, уникайте анонімних пропозицій;
- з'ясовуйте конкретний зміст та умови підробітку;
- пам'ятайте, що за легку роботу жоден роботодавець не розплачуватиметься великою сумою грошей;
- не долучайтеся до видобутку віртуальної криптовалюти. Цей вид заробітку несе загрозу для вашого здоров'я та суттєво збільшує ризик пожежі у зв'язку з перевантаженням електромережі житлового будинку.

Загроза №2. Сумнівний контент

2.1. Недостовірна, фейкова інформація

Як уникнути:

- користуйтеся офіційними енциклопедіями та словниками. Якщо є потреба звернутися до «Вікіпедії», пам'ятайте – навіть там трапляються помилки;
- не завантажуйте інформацію з неперевірених джерел, наприклад, з банку рефератів. Зазвичай якісна робота, на яку витрачено суттєвих інтелектуальних зусиль, не розміщується у вільному доступі для загального користування;
- звертайте увагу на дотримання авторських прав (відомості про автора та посилання на джерела інформації)
- розпізнавайте «жовті» сайти, яким не варто беззаперечно вірити. Серед їхніх формальних ознак – кричущі заголовки, велика кількість реклами або перенаправлень на інші сайти;
- шукайте два-три джерела, бажано й іншими мовами. Перевіряйте, чи є в мережі інші думки та факти, які спростовують чи підтверджують той чи інший факт.

2.2. Deepfake (підроблене відео)

Цей механізм передбачає створення відео шляхом заміщення обличчя однієї людини на обличчя іншої. Аби не стати об'єктом такого неправдивого відео, не варто розміщувати велику кількість фотографій у соціальних мережах.

2.3 Контент, що формує спотворене враження про успішність

У мережі є велика кількість постів, де користувачі викладають фотографії дорогого відпочинку, гарних місць, брендових речей тощо. Проводячи паралель зі своїм повсякденним життям, діти намагаються прагнути до такого ж формату успішності, що не завжди відповідає фінансовим можливостям родини.

Аби цього уникнути, варто розуміти, що:

- окремі пости у соціальних мережах інколи не відбивають повну картину реального життя.
- фотографії, що викладаються в соціальні мережі, можуть ретельно редагуватися за допомогою сучасних програм;
- можуть використовуються чужі зображення для створення власного контенту.

Загроза №3. Небезпечний контент

Зйомка контенту, пов'язаного з небезпекою для життя та здоров'я (збройний конфлікт, вибух, екстремальні захоплення («руфінг», «скайуокінг», «зачепінг»), заклик до фізичної розправи з учителями, батьками, однокласниками)

Ці захоплення представляють смертельну небезпеку, а використання гаджету лише збільшує ризик оступитися, втратити рівновагу або не помітити загрозу.

Як уникнути:

- формуйте культуру особистої безпеки. Вона полягає у готовності захистити себе та оточуючих від несприятливого впливу, загроз та небажаних наслідків;
- у разі виникнення небезпечних ситуацій подбайте, в першу чергу, про свою та безпеку інших людей;
- пам'ятайте, що публікації з загрозами фізичного насилля - не жарти, й можуть тягнути за собою кримінальну відповідальність.

Загроза №4. Секстинг (онлайн-листування інтимного характеру, надсилання інтимних фото або відео) та онлайн-грумінг (встановлення дорослими дружніх та довірливих відносин з неповнолітніми)

Як уникнути:

- під час створення профілю у соціальних мережах максимально уникайте прив'язки до «фізичного» світу. Не можна вказувати детальну інформацію про себе (адресу проживання, дату народження, номер телефону та адресу електронної пошти, місце навчання тощо);
- створюйте унікальні паролі за допомогою літер, цифр та спецсимволів;
- будьте обережні у спілкуванні, якщо ви: не знайомі з цією людиною у реальному житті; ваш співрозмовник явно дорослiший за вас; у нього немає або дуже мало друзів у соцмережі;
- не публікуйте на своїй сторінці у соціальній мережі відверту фотографію або навіть кадр із натяком на відвертість з метою зібрати більше «лайків», привернути увагу хлопця чи дівчини;
- не надсилайте інтимні фотографії незнайомцям навіть після довгих умовлянь;
- якщо ви стали жертвою секстингу, потрібно звернутися до дорослих. Вони допоможуть зв'язатися з адміністрацією ресурсу та повідомити, що персональні дані неповнолітнього розміщено у відкритому доступі. Якщо таке звернення не допоможе, варто звернутися за юридичною допомогою;
- категорично відмовляйтеся від пропозицій зустрітися з незнайомими людьми.

Загроза №5. Негативні наслідки спілкування у мережі

Як уникнути:

1. Не ображайте інших.
2. Не будьте нав'язливими.
3. Не дозволяйте своїм негативним емоціям виходити з-під контролю.
4. Пишіть грамотно.
5. Дізнавайтеся про особливості спілкування у новій спільноті (використання смайлів, сленгу тощо)
6. Не привертайте увагу за рахунок епатажу.
7. Не відходьте від теми розмови («флуд» вважається одним із головних «гріхів» у мережі).
8. Не ігноруйте запитання співрозмовника, крім явного тролінгу чи образ (у цьому разі спілкування потрібно негайно припинити).
9. Ніколи не беріть участь у цькуванні. Віртуальний булінг нічим не відрізняється від реального й однаково небезпечний і для жертви, і для агресора.
10. Не соромтеся розповідати вчителям та батькам про загрози, отримані через Інтернет. У цьому разі шанс гідно вийти з неприємної ситуації значно зростає.