STOP sextинг

Академія Української Преси

ПРИВАТНІСТЬ ДИТИНИ В ІНТЕРНЕТІ

Як приватне залишати приватним в інтернеті? Адже постійно ми висвітлюємо інформацію про власне життя, робочі моменти, наші роздуми та вподобання. Також кожного дня спілкуємось з друзями, рідними чи колегами через соціальні мережі. І такі, на перший погляд, звичні речі можуть стати причиною викрадення приватних даних.

НА ЩО ВАЖЛИВО ЗВЕРТАТИ УВАГУ, КОЛИ МИ ВИКОРИСТОВУЄМО ІНТЕРНЕТ, ЩОБ ЗБЕРЕГТИ ПРИВАТНІ ДАНІ?

САЙТИ

Рекомендовано зберігати в закладах браузера сайти та платформи, якими ми найчастіше користуємось, наприклад, платформа для оплати покупок в інтернеті (як то Приват24) чи головні сторінки соціальних мереж. Зловмисники дуже часто роблять копії популярних сайтів, де викрадають приватні дані користувачів. В самій адресі сайту може бути лише маленька зміна, яку ми можемо не помітити.

ДОДАТКИ

Так само злочинці створюють фейкові додатки, які ззовні виглядають ідентично до справжніх. Важливо завантажувати додатки лише з перевірених сайтів та дивитись по кількості завантажень й на коментарі.

ПОСИЛАННЯ

Часом в приватні повідомлення чи у групові чати надсилають різні посилання. Частина з них може бути направлена на збір приватної інформації чи мати вірусне походження. Тож, якщо ви не очікуєте від людини ніякі посилання, то перед тим як відкрити невідомий лінк перепитайте, що там знаходиться і для чого людина його надіслала.

ПОВІДОМЛЕННЯ

Повідомлення типу “Ви виграли приз, подзвоніть по вказаному номеру/надішліть ваші дані”, “Готові надати вам кошти для ваших потреб, подзвоніть нашому оператору”, “За цим посиланням є вся інформація про тебе, перейди” та схожі тексту використовують злочинці для отримання приватних даних людини.

ПЕРЕВІРКА ЗАПИТІВ

Якщо у соціальних мережах хтось зі знайомих написав приватне повідомлення чи пост про термінову потребу, наприклад, в грошах. Перед тим, як надсилати кошти, перетелефонуйте чи напишіть в іншій мережі цій людині для перевірки чи запит дійсно правдивий, чи акаунт був взломаний шахраями.

ЯК ДОРОСЛИМ ТА ДІТЯМ ЗАХИСТИТИ СВОЮ ПРИВАТНІСТЬ В МЕРЕЖІ?

- Не додавайте у друзі в соціальних мережах тих, кого не знаєте в житті.
- Закрийте акаунт у соціальній мережі, щоб користувачі, які не в списку друзів, не могли бачити інформацію на сторінці.
- Скрийте приватну інформацію про себе: номер мобільного телефону та електронну пошту, щоб користувачі не могли бачити це на вашій сторінці.
- Не переходьте по посиланнях, в яких ви не впевнені, навіть, якщо хтось зі знайомих відправив це.
- Не публікуйте у соціальних мережах ваші родинні плани щодо майбутньої відпустки чи поїздки за місто.
- Якщо подаєтесь на волонтерські чи навчальні проєкти, то додатково дізнайтесь, хто організатор цього, чи є сайт, чи є відгуки про програми.
- Не публікуйте паролі від соціальних мереж - ні на власній сторінці, ні в приватних повідомленнях.
- Не вказуйте геолокацію в той час, коли ви там знаходитесь. Наприклад, якщо ви поїхали з рідними у відпустку, то краще виставляти фото та вказувати локацію по поверненню звідти.
- Створюйте пароль, який буде містити літери та цифри, як великого розміру, так і маленькі.
- Не використовуйте один і той самий пароль на різних платформах.
- Видаляйте зі смартфона всі додатки, якими не користуєтесь.

Ви можете разом з дитиною розглянути ці пункти та переглянути, чи ваші приватні акаунти відповідають цим правилам захисту приватності в інтернеті. Якщо ні, то моете спільно змінити налаштування, паролі, переглянути список друзів та переконатись, чи дійсно ви всіх знаєте на своїй сторінці і дитина - на своїй.

ЯКА ВІДПОВІДАЛЬНІСТЬ ДОРОСЛИХ ЗА ПРИВАТНІСТЬ ДИТИНИ В ІНТЕРНЕТІ?

Доволі часто батьки та освітяни використовують фотографії з зображенням дітей для власних постів, для публікацій навчального закладу чи певних подій. Так, з однієї сторони це про висвітлення важливих урочистостей, про спогади про певний моменти. Але поруч з цим це також про порушення приватності дитини та можливий вплив на її майбутнє.
На що важливо звернути увагу, коли ми публікуємо фото чи відео за участі дитини?

Впевніться, що дитина одягнена, виглядає пристойно - не запачканий одяг чи частини тіла, дитина чиста.

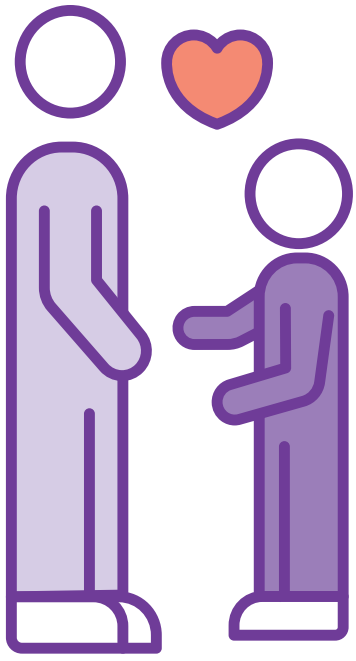
Перевірте, чи на задньому фоні немає ніякої приватної інформації (номеру школи, записаних на дошці телефонів, прикмет по яким легко розпізнати місце навчання чи проживання тощо).

Не варто публікувати смішні фото дитини, навіть, якщо це здається кумедним. Оскільки все, що ми публікуємо в мережі, назавжди там залишається. І через роки така фотографія дитини може стати причиною кібербулінгу в дитячому колективі.

Не вказуйте геолокації у постах.

Подумайте чи не нашкодить така публікація приватності чи репутації дитини зараз чи в майбутньому.

Запитайте у дитини чи згодна вона на розміщення таких матеріалів про неї. Якщо так, оберіть фото чи відео разом.



Пам'ятайте, що коли ми фізично знаходимось у безпечному для нас місці (у власній кімнаті, на робочому місці чи поруч з рідними), то нам може здаватись, що в інтернеті ми також в безпеці у цей час. Але злочинці не втрачають шанс знайти нових жертв для своїх махінацій. Тож, важливо попіклуватись, щоб використання інтернету для нас та наших дітей був максимально безпечним.

#stop_sextинг - найбільший в Україні освітній проєкт щодо захисту дітей в інтернеті. Отримав премію Глобального договору ООН та загалом навчив більше ніж 500 000 дітей та батьків. В межах інформаційної компанії торкнувся мільйонів українських родин та створив першу тематичну консультаційну гарячу лінію.

Посилання на проєкт #stop_sextинг

Сайт: https://stop-sexting.in.ua/

Instagram https://www.instagram.com/stopsexting.ua

Facebook https://www.facebook.com/stopsextingua/

Для дітей та підлітків:

TikTok https://www.tiktok.com/@stopsexting.ua

2022