ПРАВИЛА БЕЗПЕКИ В ІНТЕРНЕТІ

1. **Бережіть свої таємниці!**

В інформаційному просторі нам часто доводиться вводити свої дані: ПІБ, адресу, дату народження, номера документів. Чи безпечно це?

Персональні дані (ім'я, прізвище, адреса, дата народження, номера документів) можна вводити тільки на державних сайтах або на сайтах для придбання квитків. І тільки в тому випадку, якщо з'єднання встановлюється по протоколу https. Зліва від адреси сайту повинен з'явитися **значок у вигляді зеленого замку** - це означає, що з'єднання захищено.

Реєстрація дитини на сайтах має проходити під керівництвом батьків. Ні в якому разі не можна передавати через мережу дані будь-яких документів і банківських карт. Навіть (і тим більше) якщо хтось про це просить, намагається переконати в тому, що виникла критична ситуація, квапить і повторює, що потрібно терміново надіслати інформацію.

Якщо така ситуація виникла, дитині потрібно відразу зв'язатися з батьками, особливо, якщо їй говорять, що нікому нічого повідомляти не можна і лякають неприємними наслідками. Залякування і спроби попри будь-які обставини одержати відомості говорять про те, що перед вами шахраї.

2. **Будьте анонімним!**

З метою захисту інформації про себе в соціальних мережах (Instagram, Facebook та інші) по можливості не вказуйте свою адресу, дату народження, школу, клас та іншу інформацію, та при реєстрації радимо використовувати очевидний псевдонім замість справжнього ім'я: по ньому має бути зрозуміло, що це не справжнє ім'я.

3. **Не спілкуйся з незнайомцями!**

Є кілька головних небезпек, з якими можна зіткнутися в інтернеті. Вони мало відрізняються від тих, що загрожують нам в реальному житті. Зловмисники тут просто використовують інші засоби.

Булінг. Дитину обзивають або труять в інтернеті - найчастіше без будь-якої причини, «тому що так весело». До жертви можуть причепитися через фотографії в профілі або через публікацію в соцмережах.

Секстинг. Надсилання оголених фото чи відео. Фото часто поширюють отримувачі, що спричиняє кібербулінг, булінг у школі та проблеми при влаштуванні на навчання та роботу.

Кібергрумінг. Налагодження довірливих стосунків із дитиною з метою подальшого сексуального насильства в Інтернеті чи офлайн. Злочинці з усього світу знайомляться у соціальних мережах та онлайн-іграх із дітьми в Україні та вимагають у них робити сексуальні дії перед камерою. Також це може бути підготовкою до злочину в офлайн. (Як приклад - зґвалтування двох підлітків в Одесі у жовтні 2019 після знайомства в Інстаграм).

Сексторшен. Налагодження довірливих стосунків із дитиною з метою отримання інтимних фото чи відео із подальшим шантажем розповсюдити ці матеріали. Основна мета - отримати гроші від дитини чи більш інтимні матеріали для продажу.

Шахраї. Намагаються заволодіти даними користувача або втягнути дитини в небезпечну фінансову авантюру.

Головний засіб захисту від всіх цих загроз - конфіденційність.

Слід обмежити доступ до інформації про всі сторони свого життя. Повідомляти їх можна тільки перевіреним людям: рідним, близьким і людям, які знайомі вам особисто, а не через інтернет. Тих, хто намагається вас якось зачепити чи образити (так званих тролів), потрібно просто ігнорувати. В інших випадках загроз - **негайно припиніть спілкування з незнайомцем та зверніться до вчителя, чи дорослої людини, якій ви довіряєте, батькам/соціальному педагогу/психологу, або зателефонуйте за номером гарячої лінії 116 111, чи зверніться до сервісу з видалення інтимних зображень та служби підтримки (чат-бот) stop-sexting.in.ua.**

На що треба звернути увагу перш ніж вступити в діалог? Що вказує про небезпеку?

- Ви не знайомі з цією людиною в реальному житті;
- Ваш співрозмовник значно перевищує Вас за віком (якщо він використовує свої справжні фотографії);

- У нього немає або дуже мало друзів;
- Співрозмовник про щось просить: сфотографуватися, прислати якісь дані тощо.

4. Підходьте зважено до публікацій фотографій!

Правила публікації власних фотографій дуже прості - якщо ви не хочете, щоб вони стали надбанням громадськості, не можна викладати їх в Інтернет і відправляти комусь. Навіть месенджери «вміють» копіювати листування в «хмару», так що ви можете втратити контроль над своїми знімками. Важливо пам'ятати, що ні в якому разі не можна викладати фотографії документів - своїх або чужих. А фото інших людей варто викладати тільки в разі, якщо вони на це згодні.

5. Завжди будьте уважні!

У нас погана новина - видалити нічого не вийде. Все, що попало в мережу, залишиться там назавжди. Як правило, стерти дані з мережі неможливо, бо навіть звичайний месенджер копіює та зберігає дані в хмарі, навіть якщо ви їх видалили з листування.

Єдиний спосіб уникнути витоку інформації - **не ділитися нею.**

6. Не розголошуйте своє місцезнаходження!

Дані геолокації дозволяють всьому світу дізнатися, де ви живете і навчаєтесь, проводите вільний час, в яких акціях берете участь, які шоу та вистави любите, як відпочиваєте. Відстежити місце розташування людини тепер не складає труднощів.

Для дитини це може становити велику небезпеку. Але повністю відключити геолокацію на дитячому телефоні не можна. Батькам корисно використовувати спеціальні програми, щоб знати, де знаходиться дитина.

7. Увага: ігри - небезпека!

Правила безпеки є не тільки в соцмережах і месенджерах. Багато основних загроз може йти від онлайн-ігор. Там дитина навіть більш вразлива, оскільки нею простіше маніпулювати: ігрові об'єкти, членство в командах, внутрішньо ігрові соціальні зв'язки - все це може стати механізмом маніпуляції для шахраїв, педофілів або навіть вербувальників різних екстремістських угруповань. Ось чому в грі потрібно триматися особливо уважно.

8. Навчиться розрізняти фальшиві сайти!

Фішинг - це спосіб виманювати у людини її дані: логін, назву облікового запису та пароль. Відбувається це так: користувачеві надсилають посилання на сайт, дуже схоже на справжню адресу поштового сервісу або соціальної мережі. Як правило, фішери спеціально купують такі домени. Наприклад, для google.com це може бути «googie.com», а для facebook.com - «facebook-com.com».

Зловмисник чекає, коли людина введе логін та пароль на підробленому сайті. Так він дізнається дані, а потім використовує їх для входу в справжній профіль своєї жертви.

9. Тренуйте пам'ять!

Чи цілком безпечно користуватися сервісами, які зберігають паролі? Якщо в профілі міститься дійсно важлива інформація, на жаль, ні. Чому?

- Це зручно, але онлайн-сервіси для зберігання паролів завжди знаходяться під прицілом хакерів та можуть бути зламані.
- Найчастіше жертви дізнаються про це лише через якийсь час, якщо взагалі дізнаються.
- Нерідко такі сайти та сервіси створюються шахраями спеціально для того, щоб збирати паролі.

Паролі повинні бути унікальними. Цифри та спецсимволи значно ускладнюють процес підбору. У соцмережі, месенджери і пошту безпечніше входити через застосунки, а ось в браузерах введення паролів слід уникати. Всі застосунки повинні встановлюватися батьками або під їх контролем.

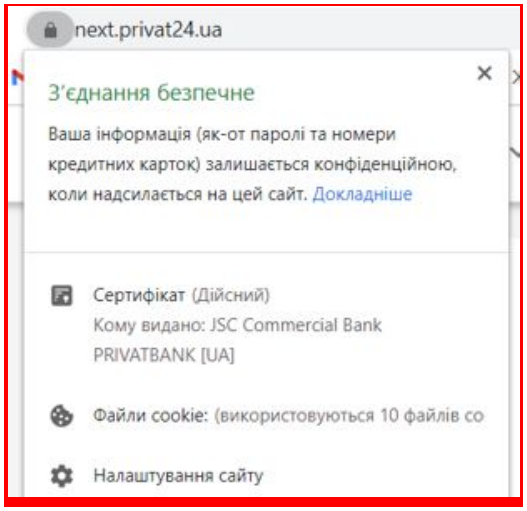
10. Обережно з покупками!

Головне правило інтернет-покупок таке: доступ дитини до грошей повинен бути обмеженим і перебувати під контролем батьків. Основні фінансові втрати зазвичай відбуваються через телефон. Необхідно підключити послуги блокування платного контенту, не класти багато грошей на рахунок дитячого телефону і контролювати витрати. Всі інші платежі повинні узгоджуватися з батьками та відбуватися тільки під їх наглядом.

Всі сервіси, які приймають гроші, повинні мати значок замку, при натисканні на який ви побачите повідомлення про захищене з'єднання.

Якщо такого значка немає, краще не користуватися сторінкою. Втім, навіть його наявність стовідсоткової гарантії не дає.

Як приклад Ви можете бачити скріншот (сайту Приват24) - захищеного з'єднання з веб банкінгом.



11. Перевіряйте інформацію!

Перевірка інформації - досить складний процес, і навіть дорослі люди далеко не завжди справляються з цим. Є кілька формальних ознак того, що Ви потрапили на сайт, якому не варто вірити беззастережно. Це кричущі заголовки, велика кількість реклами або якщо читача, який натиснув на новину, перекидає кудись далі.

Щоб перевірити інформацію, яку ви отримали в інтернеті, дотримуйтесь наступних рекомендацій:

- пошукайте ще два-три джерела, бажано також на інших мовах;
- знайдіть першоджерело і задайте собі питання: «Чи можна йому довіряти?»;
- перевірте, чи є в мережі інші думки та факти, які спростовують або підтверджують сказане.

Якщо потрібно дізнатися якийсь факт або з'ясувати, що означає незрозумілий термін, можна звернутися до «Вікіпедії». Там рідко можна зустріти зовсім відверту нісенітницю, але сліпо довіряти відкритій цифрової енциклопедії не варто (навіть в ній попадаються помилки).

12. Попіклуйся за хмару!

Наскільки надійні сховища, на кшталт “Диск” від Google, і чи можна там без побоювання зберігати документи та інші файли? Фахівці кажуть, що хмарне сховище є надійним місцем зберігання інформації та

рекомендують насамперед використовувати для резервного копіювання. Але слід зазначити, що потрібно його надійно захистити зі сторони користувача, а саме встановити надійний пароль та увімкнути додатковий захист з використанням двох кроків входу, наприклад: пароль та код з смс повідомлення.

13. Слідуй мережному етикету!

Людство тільки вчиться спілкуватися в мережі, але правила гарного тону тут нічим не відрізняються від тих, яких потрібно дотримуватися в реальному світі. Не ображайте інших та не будьте нав'язливим, не дозволяйте своїм негативним емоціям виходити з-під контролю, пишіть грамотно.

Як і в житті, в мережі нам доводиться бувати в різних спільнотах, і правила спілкування можуть відрізнятися. Ввічлива людина, потрапивши в незнайоме суспільство, перш за все спробує дізнатися його особливості. Десь прийнято спілкуватися на «Ви», а десь - на «ти», десь смайли доречні, а десь - ні. Є компанії, де вітається використання мережного сленгу, а є такі, де його просто не зрозуміють або вважатимуть Вас безграмотним.

Втім, існують правила, актуальні для будь-яких спільнот:

- не відходьте від теми розмови: «флуд» вважається одним з головних «гріхів» в мережі;
- не ігноруйте питання співрозмовника, крім явного тролінгу або образ - подібну бесіду потрібно негайно припинити;
- ніколи не беріть участь в цькуванні: булінг в мережі нічим не відрізняється від реального та однаково небезпечний і для жертви, і для агресора.

14. Головний секрет безпеки в мережі інтернет.

Не потрібно робити в інтернеті нічого, що ви не стали б робити в фізичному світі. Різниця між віртуальною і реальною дійсністю мінімальна. Що стосується батьківської поведінки, в мережі вона теж не повинна відрізнятись від поведінки «в офлайні».

Від дитини не можна домогтися покори шляхом заборон і жорсткого контролю. Однак і відчуття вседозволеності в інтернеті теж бути не повинно. Разом вчіться вести безпечний спосіб життя, як реального, так і віртуального.