Разом заради кращого Інтернету

БЕЗПЕКА В ІНТЕРНЕТІ

День безпечного інтернету

У другий вівторок лютого у світі відзначають День безпечного Інтернету (Safer Internet Day).

Суспільство звернуло увагу на цю проблему 17 років тому, коли мережа стала не просто системою комунікації, а й каналом розповсюдження ворожого та шкідливого, а дуже часто жахливого контенту.

День безпечного Інтернету запровадили мережі Insafe та INHOPE за підтримки Європейської комісії для просування безпечного та позитивного використання цифрових технологій, особливо, дітьми й молоддю.

В Україні День безпечного Інтернету відзначається з 2009 року за підтримки "Майкрософт Україна". Цього дня проводяться різноманітні конференції, круглі столи, "прямі лінії" за участю експертів, спрямовані на популяризацію механізмів безпечної роботи в мережі, обговорюються питання інтернет-етики, загроз протизаконного контенту, а також ведуться дискусії та діалоги з пошуку компромісу між ефективністю та безпечністю використання Інтернету з урахуванням української специфіки.

На фоні інформаційної політичної боротьби всі чомусь забувають, що сьогодні в першу чергу безпечний Інтернет потрібен саме для дітей. Адже нові покоління фактично народжуються зі смартфонами в руках. А батьківський недогляд чи байдужість до того, що саме шукає дитина в мережі та що вона може там побачити – становить величезну загрозу. Дитина може стати жертвою емоційно-психічного нападу чи насилля, що призведе до жахливих наслідків.

За інформацією ООН, 70,6% користувачів Інтернету 15-24 років піддаються небезпеці залякування та переслідувань.

10 правил безпечного користування Інтернетом

1. Використовуйте надійний пароль – комбінуйте букви, цифри та інші символи.
2. Не вірте всьому, що читаєте – завжди перевіряйте достовірність джерела.
3. Не викладайте особисту інформацію про себе, своїх рідних, друзів і знайомих в Інтернеті.
4. Не ховайтеся за анонімністю екрану комп'ютера. Не кажіть того, що не могли б сказати людині в обличчя.
5. Подумайте двічі, перш ніж поширити будь-яку інформацію. Як і в житті, потрібно думати про наслідки того, що говориш.
6. Не поширюйте в Інтернеті контент незаконного або непристойного змісту.
7. Переконайтеся, що ваш профіль у соціальній мережі закритий від сторонніх (перевірте налаштування безпеки).
8. Додавайте "у друзі" тільки тих, кого дійсно знаєте: навіть якщо це друзі ваших друзів, але особисто ви не знайомі, краще зайвий раз перестрахуватися.
9. Вашим друзям слід питати вашого дозволу, перш ніж завантажувати фотографії з вами або позначати вас на фотографіях в соціальних мережах. Не бійтеся сказати їм про це, і самі теж дотримуйтесь цього правила.
10. Не переходьте за посиланнями, прикріпленим в імейл-повідомленнях – безпечніше вводити адресу в рядок браузера самому.

Діти в інтернеті

Проблема безпеки дітей в мережі Інтернет вже не здається Україні такою далекою. Ніхто не може заперечити, що на сьогоднішній день вона постала особливо гостро.

Відомо, що підлітки у період заниженої самооцінки шукають підтримки серед своїх друзів, а не у родинному колі. Старші підлітки, бажаючи незалежності, мають потребу ототожнювати себе з певною групою й схильні порівнювати цінності своєї сім'ї та своїх товаришів.

Що роблять підлітки в онлайні

В онлайні підлітки завантажують музику, використовують обмін миттєвими повідомленнями, електронну пошту та грають в он-лайнові ігри. За допомогою пошукових серверів підлітки знаходять інформацію будь-якого змісту та якості в мережі Інтернет. Більшість підлітків реєструються у приватних чатах та спілкуються на будь-які теми, видаючи себе за дорослих. Хлопці в цьому віці надають перевагу всьому, що виходить за межі дозволеного: брутальний гумор, насильство, азартні ігри, еротичні та порно сайти. Дівчатам, які мають занижену самооцінку, подобається розміщувати провокаційні фото, вони схильні на фривольні розмови, видаючи себе за дорослих жінок, в результаті чого стають жертвами сексуальних домагань.

Цікаві цифри (за матеріалами досліджень компанії "Київстар")

78% українських дітей старше 6 років користуються інтернетом;

24% батьків не знають про те, що їхні діти виходять в інтернет через мобільні телефони;

9% батьків не підозрюють, що їхні діти виходять в інтернет через мобільні телефони батьків;

8% батьків не знають, що їхні діти відвідують інтернет-клуби;

27% дітей зізналися, що в інтернеті з ними контактували незнайомці, 30% з них пішли на контакт;

28% висилали фото віртуальним знайомим;

7% ділилися в інтернеті інформацією про сім'ю.

Безпека в Інтернеті: що потрібно знати

Від соціальних мереж – до онлайн-банкінгу: сьогодні Інтернет проник у наше життя і діяльність. Окрім комп'ютерів та ноутбуків, ми підключаємо до Інтернету все – мобільні телефони, планшети, холодильники, телевізори й багато інших портативних пристроїв. Саме тому дуже важливо знати якомога більше про безпеку у Всесвітній мережі.

Необхідно віднайти правильні способи захисту нашого приватного життя, коли ми перебуваємо онлайн.

Багато хто думає, що безпека в Інтернеті – це ілюзія, і бути захищеним зараз неможливо, адже веб-сайти збирають конфіденційну інформацію так тонко, що ми навіть не знаємо що саме їм відомо. Це, можливо, й так, але ця невпевненість – ще одна причина, щоб зберегти свою приватність та уникнути витоку персональних даних в Інтернет.

Чи є щось, що ми можемо зробити, аби бути більш захищеним коли займаємося серфінгом в Інеті, крім того, що не показувати свої паролі, або не надавати забагато особистої інформації?

Які загрози існують для дітей в Інтернеті?

- **Фі́шинг** — вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказування або обміну валюти, інтернет-магазинів.

Шахраї використовують усілякі виверти, які найчастіше змушують користувачів самостійно розкрити конфіденційні дані – наприклад, посилаючи електронні листи із пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт в Інтернеті, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів.

- **Грумінг** – входження в довіру до дитини з метою її схилення до якого-небудь брутального поводження, в тому числі і в сексуальному плані.

Злочинці найчастіше встановлюють контакти з підлітками в чатах або на форумах. Зазвичай вони добре обізнані із захопленнями сучасної молоді і без особливих зусиль підтримують бесіди. Вони знаходять співрозмовників, які чимось засмучені або шукають підтримки, співчувають їм, потім пропонують перейти в більш відокремлене віртуальне місце спілкування. Поступово втягують їх в обговорення інтимних питань. Потім пропонується зустрічі в реальному світі.

Які загрози існують для дітей в Інтернеті?

- **Кардинг** – вид шахрайства, при якому проводиться операція з використанням банківської картки або її реквізитів, не ініційована або не підтверджена її власником.

- **Тролінг** – розміщення в Інтернеті провокаційних повідомлень з метою викликати конфлікти між учасниками, образи, марнослів'я тощо.

Тролі - персонажі, які свідомо провокують нас на негативні реакції і знижують рівень комфорту нашого перебування в мережі. Це може відбуватися як в блогах, так і в соціальних мережах або в соціальних медіа – в будь-якій ситуації, де виникає мовна взаємодія.
Тролінг є грубим порушенням мережевого етикету.

- **Мобінг** - психологічні утиски, переважно групові, що включають у себе постійні негативні висловлювання, постійну критику.

Мобінг виражається в різних формах, і розвиток Інтернету породило чергову – мобінг в соціальних мережах.
За наслідками мобінг в Інтернеті нічим не відрізняється від реального життя. Інтернет-мобінг навіть більш небезпечний, оскільки, якщо раніше діти, які зазнавали утисків однокласників, могли хоча б вдома уникати цих проблем, то зараз цей тиск дитина відчуває постійно. Збільшується він тим, що Інтернет робить мобінг відкритим для всього світу. Дитина отримує ярлик жертви в очах тих, хто не повинен знати про цькування.

Кібербулінг

❑ **Кібербулінг –** це «цькування онлайн», що передбачає жорстокі дії з метою дошкулити, нашкодити, принизити людину з використанням інформаційно-комунікаційних засобів: мобільних телефонів, електронної пошти, соціальних мереж, форумів, блогів, онлайн-відеоігор.

8 типів кібербулінгу:

1. Флеймінг – найбільш емоційні та жорстокі репліки, які агресор приносить жертви на «публіці»: на форумах або у чатах. Улюблений інструмент знущання так званих «тролів».

2. Нападки – це регулярні висловлювання провокатора, які виснажують жертву. зображення можна спостерігати в ігровому товаристві – у чатах онлайн ігор.

3. Наклеп – провокатор розширює неправдиву та принизлив інформацію про свою жертву.

4. Самозванство – агресор використовує інформацію про іншу людину (паролі до облікових записів у соціальних мережах та блогах), щоб від її імені дошкуляти іншим користувачам.

5. Ошукання – крадіжка конфіденційних даних за власними цінами або на замовлення третіх осіб.

6. Відчуження – демонстраційне ігнорування людини: видалення з чатів, груп, додавання до чорного списку друзів тощо.

7. Кіберпереслідування – найнебезпечніший різновид інтернет-мобінгу. За допомогою інформації яку жертву викладає в мережі, злодій переслідує її, щоб скоїти напад, побити або зґвалтувати.

8. Хепіслепінг – фільмування реальних нападів або знущання для публікації в інтернеті. Внаслідок появи хепіслепінгу з'явилося інше поняття – буліцид, що означає загибель жертви внаслідок булінгу.

Як запобігти кібербулінгу?

✓ Контролюй поширення своєї особистої інформації та налаштуй приватність у власних акаунтах.

✓ Перевіряй усе що надсилаєш знайомим і незнайомим людям, та бублікуєш в Інтернеті, за допомогою запитання-тесту «Біл-борд».

✓ Додавай у «друзі» тільки реально знайомих безпечних людей.

✓ Критично стався до інформації знайденої в Інтернеті, та перевіряй її за допомогою декількох джерел.

ЗАХИСТ ДІТЕЙ ВІД СЕКСУАЛЬНОГО НАСИЛЛЯ В ІНТЕРНЕТІ

Сексуальне насилля онлайн – один з викликів, який стоїть перед батьками та педагогами. Діти можуть стикатись із сексуальним насилля в Інтернеті у формах секстингу, кібергрумінгу та сексторшену.

Секстинг – це надсилання інтимних фото чи відео з використанням сучасних засобів зв'язку. Діти можуть надсилати такі матеріали як знайомим, так і не знайомим їм у реальному житті людям. Матеріали подібних переписок можуть бути оприлюднені, що часто призводить до кібербулінгу та цькувань дитини у школі.

Кібергрумінг — це процес комунікації із дитиною в Інтернеті, під час якого злочинці налагоджують довірливі стосунки з дитиною з метою сексуального насильства над нею у реальному житті чи онлайн. Вони можуть змушувати дітей виконувати певні сексуальні дії перед камерою. Злочинці свідомо будують своє спілкування з дитиною так, аби викликати в неї теплі почуття та довіру, показати, що вона цінна та унікальна. Вони можуть прикидатися однолітками дитини, пропонувати роботу моделлю, дарувати подарунки тощо.

Сексторшен – налагодження довірливих стосунків із дитиною в Інтернеті з метою отримання приватних матеріалів, шантажування та вимагання додаткових матеріалів або грошей.

Увага: якщо дитина стала жертвою секстингу, кібергрумінгу чи сексторшену, необхідно звернутися до поліції.

Як забезпечити безпеку дітей в мережі Інтернет

- Розміщуйте комп'ютери з Internet-з'єднанням поза межами кімнати вашої дитини.
- Поговоріть зі своїми дітьми про друзів, з яким вони спілкуються в он-лайні, довідайтесь як вони проводять дозвілля і чим захоплюються.
- Цікавтесь які веб сайти вони відвідують та з ким розмовляють.
- Вивчіть програми, які фільтрують отримання інформації з мережі Інтернет, наприклад, Батьківський контроль в Windows*.
- Наполягайте на тому, щоб ваші діти ніколи не погоджувалися зустрічатися зі своїм он-лайновим другом без Вашого відома.
- Навчіть своїх дітей ніколи не надавати особисту інформацію про себе та свою родину електронною поштою та в різних реєстраційних формах, які пропонуються власниками сайтів.
- Контролюйте інформацію, яку завантажує дитина (фільми, музику, ігри, тощо).
- Цікавтесь чи не відвідують діти сайти з агресивним змістом.
- Навчіть своїх дітей відповідальному та етичному поводженню в он-лайні. Вони не повинні використовувати Інтернет мережу для розповсюдження пліток, погроз іншим та хуліганських дій.
- Переконайтеся, що діти консультуються з Вами, щодо будь-яких фінансових операції, здійснюючи замовлення, купівлю або продаж через Інтернет мережу.
- Інформуйте дітей стосовно потенційного ризику під час їх участі у будь-яких іграх та розвагах.
- Розмовляйте як з рівним партнером, демонструючи свою турботу про суспільну мораль.