День безпеки в Інтернеті

Ця міжнародна календарна подія виникла за сприянням організації Insafe починаючи з 2004 року. Вона відзначається щорічно у другий день другого тижня лютого, тобто 9 лютого.

Цей день проводиться з метою залучити до дій кожного та кожну, хто відіграє свою роль у створенні кращого Інтернету для всіх, зокрема, наймолодших користувачів. Більш того, це запрошення для всіх до поважливого онлайнового спілкування задля забезпечення найкращого цифрового досвіду.

Подія ця дозволяє зробити акцент на позитивному використанні технологій і вивчити роль, яку ми всі граємо в цілях сприяння створенню кращої і більш безпечної онлайн-спільноти. Воно служить закликом для молодих людей, батьків, вихователів, вчителів, соціальних працівників, співробітників правоохоронних органів, підприємств, політиків і широких верств суспільства, щоб об'єднатися з метою сприяння та створення найбільш позитивного і кращого інтернету.

Якщо раніше треба було говорити з дітьми про їх безпеку поза домом тощо, то вже давно має сенс застерігати їх від негараздів під час перебування в інтернеті.

Інформаційна безпека стосується захисту життєво важливих інтересів людини (і більш глобально – суспільства, держави). Неправдива, неповна, невчасна інформація може нанести шкоду. Особливо вразливі у цьому контексті діти. Вони можуть не знати, яку інформацію можна викладати в мережу, а яку не варто. Інколи школярі не можуть правильно зреагувати на матеріали з мережі з різних причин. Робота у цьому напрямку для вчителів та батьків дуже важлива. Безконтрольний доступ до інтернету може мати негативні наслідки для дитини.

Типи загроз

1. Стосуються особистої безпеки:

- Ознайомлення з порнографічними матеріалами, ненормативною лексикою, інформацією суїцидального характеру, расистського, ненависницького чи сектантського змісту.
- Загроза отримання недостовірної чи неправдивої інформації.
- Формування залежності (ігрової, комп'ютерної, інтернет).
- Спілкування з небезпечними людьми (збоченці, шахраї, грифери).
- Залучення до виконання протиправних дій (хакерство, порушення прав та свобод інших).

2. Стосуються безпеки інших.

- Матеріали, існування та використання яких може стати причиною посягання на безпеку оточуючих (наприклад, інформація про створення вибухівки).
- Свідоме та несвідоме введення в оману інших.
- Вчинення протиправних дій, що тягнуть за собою відповідальність згідно з чинним законодавством.
- Кібербулінг — свідоме цькування та приниження, передусім однолітків.

3. Стосуються загрози витоку персональної інформації:

- Розголошення персональної та конфіденційної інформації (прізвища, імена, контакти, секретні дані кредитних карток, номери телефонів).
- Загроза зараження ПК вірусами різної категорії.
- Небезпека завантаження програм зі шкідливими функціями.

Це найбільш поширені типи загроз, з якими може зіштовхнутися дитина в інтернеті, викладаючи чи переглядаючи сумнівну інформацію.

Основні правила безпечної роботи в інтернеті, про які варто сказати дітям

1. Не давайте нікому своїх паролів.
2. Не надавайте особистої інформації поштою чи в чатах без гострої на те потреби.
3. Не реагуйте на непристойні та грубі коментарі, адресовані вам.
4. Повідомляйте про ситуації в інтернеті, які вас непокоять (погрози, файли певного місту, пропозиції).
5. Відмовляйтесь від зустрічей з випадковими людьми, з якими познайомились в онлайні.
6. Не діліться своїми фото з незнайомцями.
7. Не повідомляйте інформацію про кредитки батьків (номер картки, термін дії та таємний код).
8. Не викладайте фото квитків, на яких видно штрих-код чи QR-код.
9. Не скачуйте та не встановлюйте невідомі програми за посиланнями, навіть якщо їх надали друзі.
10. Встановлюючи перевірені програми, контролюйте, щоб на ПК не додались небажані програми.
11. Не переглядайте інформацію за невідомими посиланнями (друзі, які ними діляться можуть не підозрювати про загрозу).
12. Не відкривайте листи-спам, вони можуть містити віруси.