ЯК УБЕЗПЕЧИТИ СЕБЕ ВІД ШАХРАЇВ?

1. **Не використовуй в якості паролів своє прізвище чи день народження** — нехай це буде щось на 10-16 символів, з використанням великих та малих літер, усіляких значків на кшталт #$% та цифр.

2. **Для кожного свого акаунту придумай окремий пароль**, а щоб не заплутатися в них — використовуй менеджер паролів.

3. **Не нехтуй двофакторною аутентифікацією** (підтвердженням входу в акаунт через номер телефону, мейл або через введення спеціального коду).

4. **Вчасно оновлюй операційну систему** та застосунки, використовуй антивіруси.

5. **З обережністю надавай застосункам дозволи** до особистої інформації (наприклад, програмі з прогнозом погоди точно не потрібна камера або твої документи).

6. **Створюй резервні копії важливих даних** — вручну або налаштуй гаджети робити це автоматично.

7. **Перевіряй в пошуковику лінки**, за якими переходиш, особливо надіслані від незнайомих відправників. Якщо це посилання на магазин чи сервіс (особливо на оплату) — перевіряй правильність написання назви та звідки надіслано лінк.

8. Також **з обережністю переходь за скороченими посиланнями і QR-кодами**, адже в них може бути зашитий шкідливий контент.

9. **Використовуючи відкриті мережі WiFi, не передавай через них чутливі дані** — адресу, дані карток, паролі, скріни документів. Для подібних операцій використовуй мобільний інтернет або виконуй їх вдома, із захищеною мережею.

10. **Для додаткового захисту** даних можна використовувати **VPN-технології**, але обирай лише перевірені програми.

ДОДАТКОВО

Відео, які допоможуть тобі краще запам'ятати правила кібербезпеки 👉 https://cutt.ly/seedZiRr

Інтерактивна гра для застосування нових знань 👉 https://game.shotam.info

Більше правил кібергігієни

CRDF GLOBAL · НКЦК · МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ · ВСЕУКРАЇНСЬКА ШКОЛА ОНЛАЙН · ОСВІТОРІЯ · КИЇВ ЦИФРОВИЙ