1. Використовуй надійний пароль для акаунтів: із великими та маленькими літерами, цифрами, символами.
2. Намагайся не поширювати особисті дані (повне ім'я, домашню адресу, паролі) в інтернеті.
3. Завантажуй програми тільки з офіційних сайтів.
4. Не переходь за підозрілими посиланнями.
5. Встанови антивірусну програму на всі гаджети.
6. Пам'ятай: коли ти ділишся фото або відео, то втрачаєш контроль над ними.
7. Не пиши та не публікуй нічого, про що не хочеш, аби дізнався весь світ.
8. Якщо тебе хтось ображає, скажи про це батькам.
9. Коли ділишся своїм домашнім завданням, обирай режим «Доступне тим, у кого є посилання».
10. Не спілкуйся з тими, кого не знаєш у реальному житті.

🤦‍♂️ «Твій пароль змінено, дані викрадено, доступ до облікового запису втрачено. Йди вчи основи кібербезпеки»

Погодься, неприємно було б отримати таке повідомлення після входу на якийсь сайт. Ризик отримати «вітання» від хакерів та кіберзлочинців зростає ледь не щодня. Як же не втратити доступ до акаунтів та захистити персональні дані?

Зберігай та поширюй наші поради 👇

1. Регулярно оновлюй програмне забезпечення. З часом воно стає більш вразливим для кіберзлочинців. Старе ПЗ зламати легше. Радимо використовувати ліцензійне ПЗ: так більше шансів на безпеку системи.
2. Встановлюй складні паролі та не забувай їх змінювати. Використай великі-малі літери, цифри, спецсимволи. Роби різні «ключі» до різних даних, сторінок, пошти. Змінювати паролі варто кожні декілька місяців.
3. Використовуй двофакторну аутентифікацію, де це можливо. Насамперед в онлайн-банкінгу.

4. Створюй резервні копії важливих документів на незалежному сервері. Так буде легше зберегти дані у разі їх витоку, блокування системи, втрати доступу до початкової системи, у якій зберігалися ці дані.
5. Не переходь за незнайомими посиланнями, не завантажуй незнайомі файли. Хакери закинули наживку й чекають, щоб завантажити тобі вірус чи додаток. Так можна не тільки викрасти дані, а й погіршити роботу пристрою.
6. Не використовуй публічні мережі Wi-Fi для передачі важливої інформації. Широкий доступ до таких мереж практично нівелює захист.
7. Створюй окрему віртуальну картку для платежів в мережі Інтернет. Це обмежить доступ до даних, які пов'язані з банківським рахунком.
8. Не публікуй у соцмережах важливу приватну інформацію: геотеги, номери телефонів, email. Не рятує навіть функція «для найближчих друзів».
9. Не вставляй знайдену флешку чи інший носій інформації у свій пристрій. Віруси на ній можуть залишити спеціально. Знайди пристрій, який для цього не шкода.