



**КІБЕР
ПОЛІЦІЯ**
НАЦІОНАЛЬНА ПОЛІЦІЯ
УКРАЇНИ

Використовуйте складний пароль

Зокрема, такий що:

- * містять не менше 8 символів;
- * містять літери, цифри та спеціальні символи;
- * не містять персоніфікованої інформації (дати народження, номерів телефонів, номерів та серій документів, автотранспорту, банківської картки, адреси реєстрації тощо);
- * не використовуються в будь-яких інших акаунтах.





КІБЕР
ПОЛІЦІЯ
НАЦІОНАЛЬНА ПОЛІЦІЯ
УКРАЇНИ

Використовуйте лише ліцензійні програми

та інші програмні продукти.
Своєчасно і систематично їх оновлюйте.

Користуйтеся антивірусним програмним забезпеченням з технологією евристичного аналізу





**КІБЕР
ПОЛІЦІЯ**
НАЦІОНАЛЬНА ПОЛІЦІЯ
УКРАЇНИ

Здійснюйте **регулярне резервне копіювання даних, зберігайте резервні копії на зовнішніх носіях інформації** (SDD, HDD тощо) та налаштуйте функцію «**відновлення системи**».



**КІБЕР
ПОЛІЦІЯ**
НАЦІОНАЛЬНА ПОЛІЦІЯ
УКРАЇНИ

Уникайте використання інтернет-банкінгу

електронних платіжних систем,
введення автентифікаційних даних
під час доступу до інтернету

**через загальнодоступні
(незахищені) безпроводові
мережі**

(в кафе, барах, аеропортах та інших
публічних місцях.)



**КІБЕР
ПОЛІЦІЯ**
НАЦІОНАЛЬНА ПОЛІЦІЯ
УКРАЇНИ

Не переходьте за сумнівними посиланнями

Зазвичай інфіковані листи надходять електронною поштою. Не варто відкривати документи або посилання, які містяться у листі, якщо відправник незнайомий, або ж посилання викликають сумніви



Не переходьте за сумнівними посиланнями

Разом з ними Ви
можете завантажити вірус

Для завантаження необхідних
файлів використовуйте перевірені
офіційні ресурси





**КІБЕР
ПОЛІЦІЯ**
НАЦІОНАЛЬНА ПОЛІЦІЯ
УКРАЇНИ

**Не підключайте флешки та
зовнішні диски,
не вставляйте CD та DVD
тощо у ваш комп'ютер**

якщо ви не довіряєте повністю їх
джерелу

Існують техніки зламування
комп'ютера, що спрацьовують ще до
того, як ви відкриєте файл на флешці
і задовго до того, як ваш антивірус
його просканує



КІБЕР
ПОЛІЦІЯ
НАЦІОНАЛЬНА ПОЛІЦІЯ
УКРАЇНИ

Під час користування інтернет-ресурсами (інтернет-банкінгом, соціальними мережами, системами обміну повідомленнями, новинами, онлайн-іграми)

не відкривайте підозрілі посилання (URL), особливо ті, що вказують на веб-сайти, які ви зазвичай не відвідуєте



**КІБЕР
ПОЛІЦІЯ**
НАЦІОНАЛЬНА ПОЛІЦІЯ
УКРАЇНИ

Переконайтеся у правильності назви необхідного сайту

Один непомітний символ у назві сайту на панелі адреси може означати, що Ви потрапили не на оригінальний ресурс, а на фішинговий сайт



КІБЕР
ПОЛІЦІЯ

НАЦІОНАЛЬНА ПОЛІЦІЯ
УКРАЇНИ

Перевірте невідомий номер на сайті Кіберполіції

Якщо на Ваш номер телефону надійшло СМС сумнівного змісту, перевірте цей номер на сайті Кіберполіції у розділі «Стоп фрод»

Можливо, шахраї вже є у базі кіберполіції.

Також у цьому розділі можливо перевірити банківську картку та посилання на сумнівний сайт

Зателефонуйте у банк та заблокуйте картку

Якщо гроші зникли з рахунку,
телефонуйте у банк з проханням
заблокувати картку та відмінити
переказ коштів

Використовуйте післяплату

Обирайте післяплату

Це унеможливить шанси шахраїв
заволодіти Вашими коштами



**КІБЕР
ПОЛІЦІЯ**

НАЦІОНАЛЬНА ПОЛІЦІЯ
УКРАЇНИ

Що таке https:// і навіщо він?



HTTPS це лише HTTP з активованим шифруванням SSL/TLS

шифрується лише канал

даних між браузером користувача та веб-сервером

HTTPS на вебсайті не гарантує, що власники не шахраї

лише сайтам з сертифікатом EV

Ви можете цілком довіряти

існує три види SSL сертифікатів:

- 1 засвідчено домен (DV)
- 2 засвідчено організацію, що володіє доменом (OV)
- 3 проведено поглиблену перевірку організації, що володіє доменом (EV)

Як захистити персональну інформацію?



зберігайте електронні
фотокопії документів
(паспортів, нотаріальних
свідоцтв та доручень тощо)

**лише на шифрованих
або зовнішніх дисках**

активуйте

двофакторну аутентифікацію

всюди, де є можливість

вчасно встановлюйте

оновлення операційної системи

Як безпечно користуватися криптовалютою?

використовуйте лише **відомі онлайн-сервіси** крипто-бірж та крипто-гаманців

не використовуйте **крипто-біржі як крипто-гаманці**

кодові фрази та паролі мають **бути надійними та складними**

завжди робіть **резервні копії гаманців**

значні суми безпечніше зберігати в офлайн крипто-гаманцях

