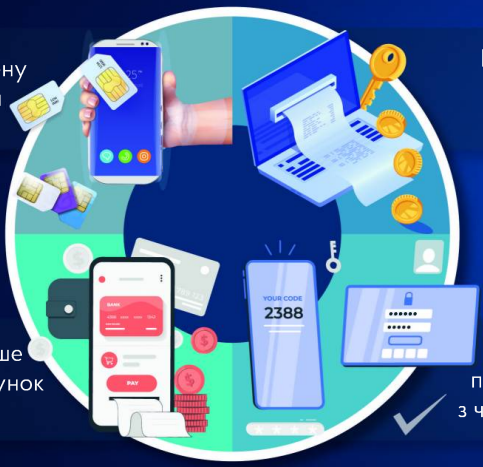
КІБЕР ПОЛІЦІЯ
НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ

ПОДБАЙ ПРО ЗАХИСТ БАНКІВСЬКОГО РАХУНКУ

Заборони віддалену заміну SIM-картки

Візьми за звичку перегляд історії транзакції



Використовуй лише офіційний застосунок свого банку

Не проводь платіжні операції з чужих пристроїв

Не повідомляй нікому:

- PIN-код, CVV та термін дії картки
- коди з SMS, що можуть використовуватися для підтвердження транзакцій
- пароль від онлайн-банкінгу

Для платежів в Інтернеті краще мати окрему картку і встановити ліміти на оплату в Інтернет

ПОСТРАЖДАВ ВІД ЗЛОЧИНУ В ІНТЕРНЕТІ?

0 800 505 170

https://ticket.cyberpolice.gov.ua

КІБЕР ПОЛІЦІЯ
НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ

ФІШИНГ

Ігноруй підозрілі посилання

Не переходь на сторонні ресурси, навіть якщо посилання надіслав друг у соцмережі

За ним може ховатися вірус або фішинговий сайт

Фішингові сайти можуть бути:

- маркетплейсами
- банками
- платформами оголошень
- сервісами обміну валют
- службами доставки

та взагалі будь-якими сайтами, де користувачі вводять свої конфіденційні дані, зокрема дані банківських карток

- купуючи на платформах оголошень, обговорюй деталі угоди тільки в чаті цієї платформи та не переходь у месенджери: туди шахраї можуть надсилати фішингові посилання
- купуй та плати лише на перевірених сайтах
- не переходь за рекламою у додатках та іграх
- не вводь конфіденційні дані на сторонніх ресурсах
- завжди уважно перевіряй URL-адресу, адже будь-які неточності можуть означати, що ти потрапив на фішинговий сайт

ПОСТРАЖДАВ ВІД ЗЛОЧИНУ В ІНТЕРНЕТІ?

0 800 505 170

https://ticket.cyberpolice.gov.ua

КІБЕР ПОЛІЦІЯ
НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ

ЯК МІНІМІЗУВАТИ РИЗИКИ ВИТОКУ ДАНИХ?

- Створюй надійні, складні паролі та не використовуй однаковий пароль для кількох ресурсів
- Вмикай двофакторну аутентифікацію всюди, де є така можливість

не переходь за сумнівними гіперпосиланнями

перевіряй правильність URL-адреси необхідного сайту

не вводь конфіденційні дані на незнайомих сайтах

створюй резервні копії

завантажуй програми та додатки лише з офіційних джерел

вчасно встановлюй оновлення операційної системи

Якщо ти став жертвою витоку даних, терміново звертайся:

ПОСТРАЖДАВ ВІД ЗЛОЧИНУ В ІНТЕРНЕТІ?

0 800 505 170

https://ticket.cyberpolice.gov.ua

КІБЕР ПОЛІЦІЯ
НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ

ЯК ДІЯТИ У РАЗІ ВИКРАДЕННЯ АБО ВТРАТИ ҐАДЖЕТУ?

- Зателефонуй на гарячу лінію оператора та заблокуй SIM-картку
- Заверши усі активні сеанси у облікових записах

Чимшвидше зміни паролі до:

- Облікових записів «Apple ID» та «Google»
- Соціальних мереж
- Месенджерів
- Електронних скриньок
- Онлайн банкінгу

Не ігноруй повідомлення системи підтримки сервісів, у яких ти зареєстрований та які використовувалися на втраченому пристрої

Ці повідомлення можуть містити **інформацію про сторонній вхід до** облікового запису або про спроби такого входу

Налаштуй скрізь, де це можливо, **двофакторну автентифікацію**

Залежно від ситуації, заблокуй **пристрій або зітри з нього всі дані.** Для цього слідуй інструкціям з офіційних вебресурсів виробника втраченого пристрою

Якщо ти став жертвою крадіжки, терміново звертайся до поліції на лінію 102

ПОСТРАЖДАВ ВІД ЗЛОЧИНУ В ІНТЕРНЕТІ?

0 800 505 170

https://ticket.cyberpolice.gov.ua

ПО ТЕЛЕФОНУ НЕ МОЖНА:

1

ВРЯТУВАТИ БЛИЗЬКУ ЛЮДИНУ З БІДИ

2

РОЗБЛОКУВАТИ БАНКІВСЬКУ КАРТКУ

3

ВИГРАТИ ЗНАЧНУ СУМУ ГРОШЕЙ АБО АВТОМОБІЛЬ

ПРОТЕ, ПО ТЕЛЕФОНУ МОЖНА СТАТИ ЖЕРТВОЮ ШАХРАЇВ!

НАЦІОНАЛЬНА ПОЛІЦІЯ ПОПЕРЕДЖАЄ!

Якщо до вас телефонують під цими приводами — припиняйте розмову та негайно звертайтесь на лінію **102**