

Кіберполіція попереджає:

Війна в Україні стала підґрунтям для поширення шахрайських схем, заснованих на вразливому емоційному стані та зловживанні довірою громадян. Зловмисники здатні обдурити дітей, пенсіонерів та намагаться розчинитись у просторах інтернету, не залишивши слідів злочину.

Понад 60% українців не можуть безпечно користуватися інтернетом, часто вони потрапляють на гачки аферистів та добровільно віддають гроші. У групах ризику люди похилого віку та діти. Але шахраям вдається обдурити навіть досвідчених користувачів інтернету.

При цьому кмітливість шахраїв виходить за рамки вже добре знайомих українцям афер, тож з'являються нові способи ошукування.

Департамент кіберполіції Національної поліції України розповідає про найпоширеніші схеми шахрайства та основні правила безпеки, які допоможуть викрити аферистів.

ПАМ'ЯТАЙТЕ:

**ПРОСЯТЬ ПОЗИЧИТИ ГРОШЕЙ В ЕЛЕКТРОННОМУ ПОВІДОМЛЕННІ?**

- ✓ Зв'язатися з людиною через інший канал (телефоном, поштою, іншим месенджером).
- ✓ Якщо людина не надсилає повідомлення: Розповісти, що її акаунт зламали.
- ✓ Порадити змінити пароль до месенджера та увімкнути двофакторну аутентифікацію.
- ✓ Попросити повідомити про інцидент Кіберполіцію та CERT-UA.
- ✗ Не довіряйте особі, яка телефонує, тільки тому, що вона знає про вас персональну інформацію.

**ШАХРАЇ НАМАГАЮТЬСЯ ВИВІДАТИ У ВАС РЕКВІЗИТИ ТА ІНШІ ДАНІ ПО ВАШОМУ РАХУНКУ**

- ✗ Не повідомляйте стороннім особам інформацію по картці або дані, що можуть бути використані для підтвердження платежів.
- ✗ Не виконуйте жодних операцій з "верифікації" картки.
- ✓ У разі сумнівів – телефонуйте до банку за телефоном, вказаним на звороті картки та уточніть інформацію.
- ✓ Безпека збереження коштів та користування рахунками починається з Вас.

**В ІНТЕРНЕТІ Є У ПРОДАЖУ ТОВАРИ, ЯКИХ НАСПРАВДІ НЕ ІСНУЄ**

- ✓ Купуйте товари та сплачуєте кошти лише на перевірених сайтах.
- ✓ У разі сумнівів надайте перевагу післяплаті.
- ✓ Для онлайн-шопінгу відкрийте віртуальну картку і переказуйте на неї лише суму грошових коштів, необхідну для подальшої оплати.
- ✓ Перевіряйте правильність назви сайту.
- ✗ Нікому не повідомляйте термін дії картки, CVV та PIN-код.
- ✗ При купівлі на платформі оголошень обговорюйте деталі угоди тільки в чаті цієї платформи – НЕ переходьте в сторонні месенджери.

**ОТРИМАЛИ ПОВІДОМЛЕННЯ ПРО НАДАННЯ ФІНАНСОВОЇ ДОПОМОГИ**

- ✓ Потрібно отримувати інформацію лише з офіційних джерел.
- ✓ Якщо ж персональну інформацію розголошено, потрібно звернутись до банку та заблокувати картку.
- ✓ Якщо підозрюєте шахрайство – негайно повідомляйте правоохоронців.
- ✗ Ніколи не переходьте за сумнівними посиланнями.
- ✗ Не повідомляйте конфіденційну інформацію стороннім особам (дані картки, логіни та паролі до онлайн банкінгу, тощо).

**РОЗСИЛАННЯ ПОВІДОМЛЕНЬ НАЧЕБТО ВІД ОФІЦІЙНИХ УСТАНОВ ПРО ЗБІР НА ЗСУ**

- ✓ Переказуйте гроші лише через офіційні фонди, благодійні організації або людям, яких ви знаєте особисто і яким довіряєте.
- ✗ Не переходьте за сумнівними посиланнями.
- ✗ Не вказуйте на сторонніх ресурсах дані ваших банківських карток.
- ✗ Довіряйте своїм інстинктам. Якщо ви отримали підозрілий електронний лист, смс-повідомлення – видаліть його. Якщо ви сумніваєтеся в правдивості телефонного дзвінка від незнайомця, покладіть трубку.

**ШАХРАЇ МОЖУТЬ СКОРИСТАТИСЯ ТВОЇМ ПАСПОРТОМ, ЗРОБИВШИ ТЕБЕ «ДРОПОМ»**

- ✓ Не передавай свої документи стороннім — на твоє ім'я можуть оформити кредити чи фірму.
- ✗ Не погоджуйся на «роботу» з використанням документів — це шахрайство.
- ✗ Не оформлюй рахунки чи кредити для інших.
- ✗ Не ведись на обіцянки легкої наживи — за це можна потрапити до в'язниці.
- ✓ Якщо отримав підозрілу пропозицію — звернись до поліції.



ТЕЛЕФОНУЮТЬ З БАНКУ ПІД ВИГЛЯДОМ ПРАЦІВНИКІВ І ВИМАНЮЮТЬ РЕКВІЗИТИ КАРТИ, КОД...

- ✓ Ніколи не розміщуйте об'яви в мережі "Інтернет" з вказанням фінансового номеру.
- ✓ Використовуйте контрактну основу надання послуг мобільним оператором, тоді шахраям буде важко перевипустити ваш фінансовий номер.
- ✗ Працівник банку ніколи не зателефонує до клієнта та не буде випитувати реквізити карти, термін дії, CVV код, вчинити дії у банкомату, він запросить вас до відділення банку.
- ✗ Не повідомляйте нікому тимчасові паролі, які приходять в смс-повідомленні.

Не дай їм виграти! Зупинимо шахраїв разом!

Повідом!

Повідомляючи про шахрайство, <https://ticket.cyberpolice.gov.ua/> ви надаєте правоохоронним органам інформацію, необхідну для припинення злочинної діяльності шахраїв та запобігаєте подальшому вчиненню шахрайських дій по відношенню до інших громадян.



**КІБЕР
ПОЛІЦІЯ**
НАЦІОНАЛЬНА ПОЛІЦІЯ
УКРАЇНИ

BRAMA

ОНЛАЙН
ВАРТА
УКРАЇНИ

**ЗАХИСТИСЬ ВІД
ШАХРАЇВ
РАЗОМ ІЗ НАМИ**



**КІБЕР
ПОЛІЦІЯ**
НАЦІОНАЛЬНА ПОЛІЦІЯ
УКРАЇНИ

<https://stopfraud.gov.ua/>