

ПАМ'ЯТАЙТЕ:



ПРОСЯТЬ ПОЗИЧИТИ ГРОШЕЙ В ЕЛЕКТРОННОМУ ПОВІДОМЛЕННІ?

✓ Зв'язатися з людиною через інший канал (телефоном, поштою, іншим месенджером).

Якщо людина не надсилала 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" карти.

✓ 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 сплачуйте 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 правомірності 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.