

ЯК ЗАХИСТИТИ СВОЇ ГРОШІ В ІНТЕРНЕТІ

1

Можливий сценарій злочину

Знайома людина просить позичити грошей в особистому повідомленні в месенджері соціальної мережі. Це може бути хтось, із ким ви давно не спілкуєтесь

Що робити

Зв'язатися з людиною через інший канал (телефоном, поштою, іншим месенджером) і запитати про повідомлення.

Якщо людина не надсилала повідомлення:

- розповісти, що її акаунт зламали
- порадити змінити пароль до месенджера та ввімкнути двофакторну автентифікацію
- попросити повідомити про інцидент Кіберполіцію та CERT-UA



ЯК ЗАХИСТИТИ СВОЇ ГРОШІ В ІНТЕРНЕТІ

2

Можливий сценарій злочину

Повідомлення в месенджері або пост у соцмережах про надання фінансової допомоги, яку може отримати будь-хто. Гроші пропонують нібито від імені державних, міжнародних установ або банків. Повідомлення містить посилання на чат-бот або сайт, де можна дізнатись додаткову інформацію

Що робити

- отримувати інформацію, особливо з приводу фінансових виплат, лише з офіційних джерел
- не переходити за сумнівними посиланнями
- не повідомляти конфіденційної інформації стороннім (дані картки, логін та паролі до онлайн банкінгу тощо)
- якщо ж особисту (персональну) інформацію розголошено, звернутись до банку та заблокувати картку
- у разі підозри шахрайських дій — негайно повідомляти правоохоронні органи



ЯК ЗАХИСТИТИ СВОЇ ГРОШІ В ІНТЕРНЕТІ

3

Можливий сценарій злочину

Повідомлення про евакуаційний рейс
за умови передплати

Що робити

- перевіряти інформацію про евакуаційні рейси, гуманітарні коридори необхідно тільки на офіційних ресурсах
- якщо можливо, обирати післяплату евакуаційних перевезень
- у разі, якщо ви стали жертвою шахрайства, заповніть форму на сайті кіберполіції

<https://ticket.cyberpolice.gov.ua/>



ЯК ЗАХИСТИТИ СВОЇ ГРОШІ В ІНТЕРНЕТІ

4

Можливий сценарій злочину

Продаж в інтернеті неіснуючих товарів за передплатою

Що робити

- купуйте та сплачуйте лише на перевірених сайтах, у разі сумнівів, надайте перевагу післяплаті
- для онлайн-шопінгу відкрийте віртуальну картку і переказуйте на неї лише суму, необхідну для оплати
- не повідомляйте нікому термін дії картки, CVV та PIN-код
- у разі купівлі на платформі оголошень обговорюйте деталі угоди тільки в чаті цієї платформи та не переходьте у сторонні месенджери
- перевіряйте правильність назви необхідного сайту: один непомітний символ на панелі адреси може означати, що ви потрапили на фішинговий ресурс



ЯК ЗАХИСТИТИ СВОЇ ГРОШІ В ІНТЕРНЕТІ

5

Можливий сценарій злочину

Псевдопокупець запитує реквізити картки для оплати за товар на дошці оголошень і називає час здійснення переказу.

У зазначений час напарник зловмисника під виглядом працівника служби безпеки банку телефонує і повідомляє, що для зарахування грошей необхідно активувати платіжну картку. Він диктує потерпілим реквізити підконтрольних рахунків, видаючи їх за коди активації картки

Що робити

- не повідомляйте стороннім даних картки або даних, 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, і уточніть інформацію
- якщо стали жертвою злочину в інтернеті, заповніть форму на сайті кіберполіції:
<https://ticket.cyberpolice.gov.ua/>



ЯК ЗАХИСТИТИ СВОЇ ГРОШІ В ІНТЕРНЕТІ

6

Можливий сценарій злочину

Розсилення повідомлень начебто від офіційних установ про збір коштів на підтримку ЗСУ тощо

Що робити

- переказуйте гроші лише через офіційні фонди, благодійні організації або людям, яких ви знаєте особисто чи яким довіряєте
- не переходьте за сумнівними посиланнями
- не вказуйте на сторонніх ресурсах даних вашої банківської картки



ЯК ЗАХИСТИТИ СВОЇ ГРОШІ В ІНТЕРНЕТІ

7

**Куди та як повідомляти
про злочинців (фото, посилання
на ресурс, аудіо, відео тощо)?**

**Адміністрації месенджера –
про користувачів, які порушують закон**

Telegram

Натисніть на повідомлення → оберіть
Повідомити → опишіть причину (якщо фішинг –
Інше → Фішинг)

WhatsApp

Натисніть на повідомлення і кілька секунд
утримуйте → оберіть у правому верхньому
кутку три крапки → натисніть Поскаржитись

**Кіберполіцію, якщо стали жертвою
злочину в інтернеті:**

<https://ticket.cyberpolice.gov.ua/>

**CERT-UA – про фішинг, зловмисне ПЗ,
кібератаки**

cert@cert.gov.ua

