**П’ять речей, які ти можеш зробити, щоб себе від шахраїв захистити:**

1. Будь пильним та обережним;

2. Не перераховуй кошти неверифікованим особам;

3. Уникай фейкових сторінок у соціальних мережах;

4. Не розголошуй свої персональні дані;

**Пам’ятай про 5 фактів**

1. Реальний працівник банку не просить надсилати кошти!

Лише шахраї наполягають на оплаті грошовим переказом пи криптовалютою;

2. Працівнику банку не потрібна інформація про ваш картковий рахунок!

Ніколи не передавай інформацію про свої рахунки тому хто телефонує;

3. Не повідомляй нікому тимчасові паролі, які приходять в смс-повідомленні! Розголошення цієї інформації призведе до втрати коштів.

4. Не переходь за посиланнями!

Не натискай на посилання, які надсилає тобі «працівник банку».

5. Не виконуй ніяких дій у банкомагах чи терміналах. Співробітник банку не надає вказівок щодо проведення маніпуляцій у банкоматах чи терміналах.

**6 ознак фішингового листа**

1. Звернення до вас автоматично згенероване;

2. E-mail адресанта неофіційний;

з. У листі містяться прохання надати персональні дані;

4. Наявні кнопки з гіперпосиланням на фейковий сайт;

5. Додані невідомі вкладення;

6. У тексті присутні граматичні помилки.

**НЕ CTAHЬ ЖЕРТВОЮ**

1. Захисти. Завжди захиіцайте свою особистість. Ніколи ne повідомляйте свою особисту інформацію.

2. Відмов. Довіряйте своїм інстинктам. Якщо ви отримали підозрілий електронний лист, видаліть його. Якщо ви сумнівастеся в правомірності телефонного дзвінка від незнайомця, покладіть трубку.

3. Повідом. Повідомляючи про шахрайство, ви надаете правоохоронним органам інформацію, необхідну для припинення злочинної діяльності шахраїв i запобігання щоб інші не стали жертвами.

Фішинг - (комбінація голосу та SMS) — це атака соціальної інженерїі, ключовою задачею якої є обманом змусити жертв надати конфіденційну інформацію по телефону.

1. **Будьте пильними при** **отриманні дзвінків** **з** **невідомих вам номерів**

2. Не передавайте дані ваших карткових рахунків чи паролю до онлайн банкінгу. Банківські працівники ніколи не запитують таку інформацію.

3. Не довіряйте особі яка телефонує, тільки тому, що вона знає вашу персональну інформацію. Шахраї можуть знайти ii в Інтернеті.

4. Не перераховуйте кошти за проханням особи, яка гелефонує, працівники банку ніколи не попросять вас про це.

Злочинці, які отримують гроші незаконним шляхом, повинні приховувати джерело походження своїх коштів. Вони залучають людей для переказу грошей - дропів! Не беріть участь у вчиненні злочину, не погоджуйтесь отримувати на свої карткові рахунки чи криптогаманці кошти невідомого походження!