З метою протидії та попередження вчинення онлайн-шахрайства шляхом підвищення рівня обізнаності населення про шахрайські схеми до Вашої уваги інформація, надана відділом протидії кіберзлочинцям в Сумській області Департаменту кіберполіціі Національної поліції України:

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

1. Будь пильним та обережним.
2. Не перераховуй кошти не верифікованим особам.
3. Уникай фейкових сторінок у соціальних мережах.
4. Не розголошуй свої персональні дані.
5. Ознайомся з шахрайськими схемами [тут.](https://mriya.social/projects/stopfraud/)

**З вами зв’язався працівник банку?**

**Пам’ятай про 5 фактів:**

1. Реальний працівник банку не просить надсилати кошти! Лише шахраї наполягають на оплаті грошовим переказом чи криптовалютою.
2. Працівнику банку не потрібна інформація про ваш картковий рахунок! Ніколи не передавай інформацію про твої 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 тoбi «працівник банку».
5. Не виконуй ніяких дій у банкоматах чи терміналах. Співробітник банку не надає вказівок щодо проведения маніпуляцій у банкоматах чи терміналах.

**6 ознак фішингового листа:**

1. Звернення до вас автоматично згенероване.
2. E-mail адресанта не офіційний.
3. 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 захищай свою особистість. Ніколи не повідомляй свою особисту інформацію.
2. Відмов. Довіряй своїм інстинктам. Якщо ти отримав підозрілий електронний лист, видали його. Якщо ти сумніваєшся в правомірності телефонного дзвінка від незнайомця, поклади трубку.
3. Повідом. Повідомляючи про шахрайство, ти надаєш правоохоронним органам інформацію, необхідну для припинення злочинної діяльності шахраїв i **запобігання** **щоб** **інші** нe **стали** жертвами. ФІШИНГ – (комбінація голосу та SMS) — це атака соціальної інженерії, ключовою задачею якої обманом **змусити**жертв надати конфіденційну інформацію› по телефону.
4. Будьте пильними при отриманні дзвінків з невідомих вам номерів.
5. Не передавайте дані ваших карткових рахунків чи паролю до онлайн банкінгу. Банківські працівники ніколи не запитують таку інформацію.
6. Не довіряйте особі яка телефонує,  тільки тому, що вона знає про вас персональну інформацію. Шахраї можуть знайти її в Інтернеті.
7. Не перераховуйте кошти за проханням особи, яка телефонує, працівники банку ніколи не попросять вас про це.

Злочинці, які отримують гроші незаконним шляхом, повинні приховувати a6o відмивати 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!

[ЯК НЕ ВТРАТИТИ ГРОШІ. ПОРАДИ НА САЙТІ](https://mriya.social/projects/stopfraud/)

[ШАХРАЇ ПОЛЮЮТЬ ЗА ГРОШИМА. ЯК НЕ СТАТИ МІШЕННЮ?](https://mriya.social/projects/stopfraud/)

[ЗНАЙШОВ ТОВАР ЗА ПІВЦІНИ? ТЕБЕ ЗНАЙШЛИ ШАХРАЇ!](https://mriya.social/projects/stopfraud/)

[ЗНАЙОМИЙ ПРОСИТЬ В БОРГ? НАПИШИ ЙОМУ…](https://mriya.social/projects/stopfraud/)

[ТЕЛЕФОНУЄ ПРЕДСТАВНИК БАНКУ? ЯК ЙОГО ПЕРЕВІРИТИ?](https://mriya.social/projects/stopfraud/)

[РОДИЧ ПОТРАПИВ У БІДУ? ШАХРАЇ ЧЕКАЮТЬ І ТЕБЕ!](https://mriya.social/projects/stopfraud/)