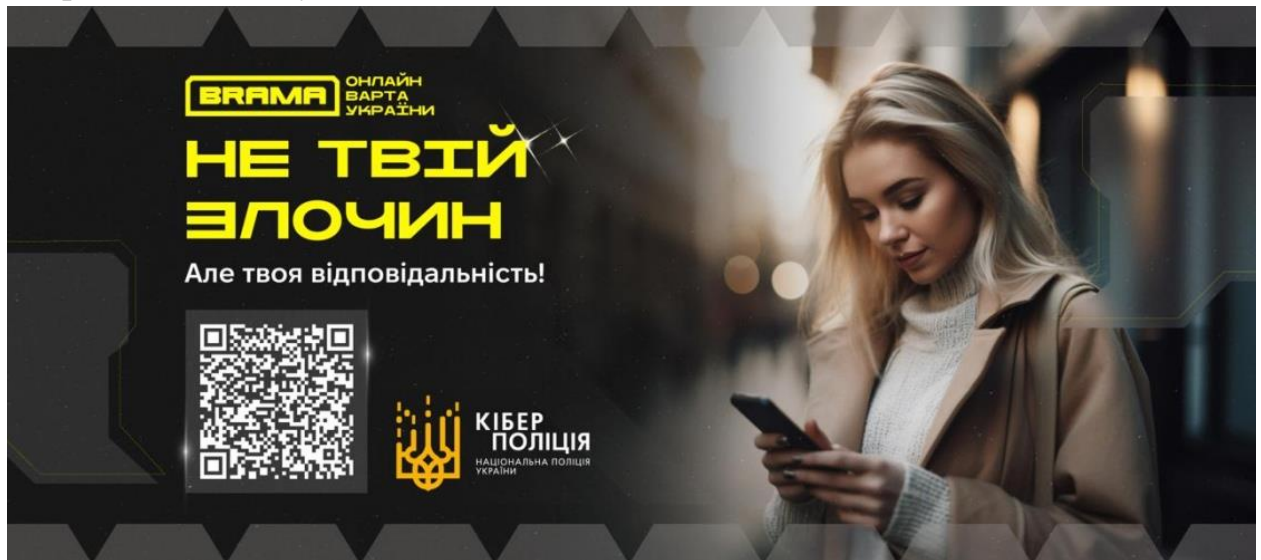


МАТЕРІАЛИ ІНФОРМАЦІЙНОЇ КАМПАНІЇ ПО ПРЕВЕНТИВНІЙ ДІЯЛЬНОСТІ З ПРОТИДІЇ ОНЛАЙН ШАХРАЙСТВ

Дропи: як не стати "грошовим мулом" для шахраїв

Легкі гроші онлайн можуть обернутись тюрмою. Хто такі дропи і як не потрапити в пастку?



Уявіть, вам пише незнайомець у соцмережі або надходить лист на пошту. Пропонують просту віддалену роботу: потрібно лише приймати кошти на свою банківську картку та пересилати їх далі. Обіцяють від 5 000 до 10 000 гривень на місяць, працювати — кілька хвилин на день, досвід не потрібен. Звучить заманливо?

Насправді — це пастка. Саме так шахраї вербують **дропів**, або ж **грошових мулів** — людей, які допомагають їм передавати та “відмивати” вкрадені гроші.

Хто такий дроп?

Дроп — це людина, яка добровільно або через необізнаність погоджується, щоб її банківська карта стала частиною злочинної схеми. Через неї проходять гроші, здобуті шляхом шахрайства, кіберзлочинів, торгівлі наркотиками чи людьми. Головна мета злочинців — **заплутати фінансові сліди**, а дропи — лише інструмент.

Чому це небезпечно?

Дуже часто люди не усвідомлюють, що стають співучасниками злочину. Проте закон не звільняє від відповідальності навіть тих, хто “не знав”.

📌 **Дроп не жертва, а співучасник.**

📌 **Дропів затримують першими.**

📌 **За такі дії загрожують штрафи, конфіскація майна і навіть тюремне ув'язнення.**

Кого найчастіше вербують?

У групі ризику:

- Молодь;
- Студенти та учні;
- Переселенці;
- Люди без стабільного доходу;
- Безробітні та соціально вразливі групи.

Шахраї грають на потребі заробити та обіцяють "золоті гори" — саме тому ця схема настільки небезпечна.

Як розпізнати шахрайську пропозицію?

Ось типові ознаки вербування дропа:

- Потрібно лише “переказувати кошти” — без чітких обов'язків чи посадових інструкцій.
- Немає вимог до освіти або досвіду.
- Спілкування лише онлайн, без особистої зустрічі.
- Пропозиція звучить надто вигідно, щоб бути правдою.
- Вас просять надіслати фото картки, паспорт або навіть передати банківські реквізити.
- “Роботодавець” пише з поштових адрес звичайних поштових операторів, а не з пошти офіційної компанії.

Особливо будьте обережні з так званими “іноземними компаніями”, які не мають офіційного представництва в Україні. Перевірити їхню легальність складніше, і саме через них найчастіше проходять шахрайські операції.

Що робити, якщо ви вже потрапили в пастку?

Якщо ви вже погодилися або підозрюєте, що стали дропом — **не зволікайте**:

1. **Негайно припиніть співпрацю.**
2. **Повідомте в кіберполіцію:** <https://cyberpolice.gov.ua> (можна залишити звернення онлайн).
3. **Зв'яжіться з банком,** картку якого ви використовували.

Як себе захистити?

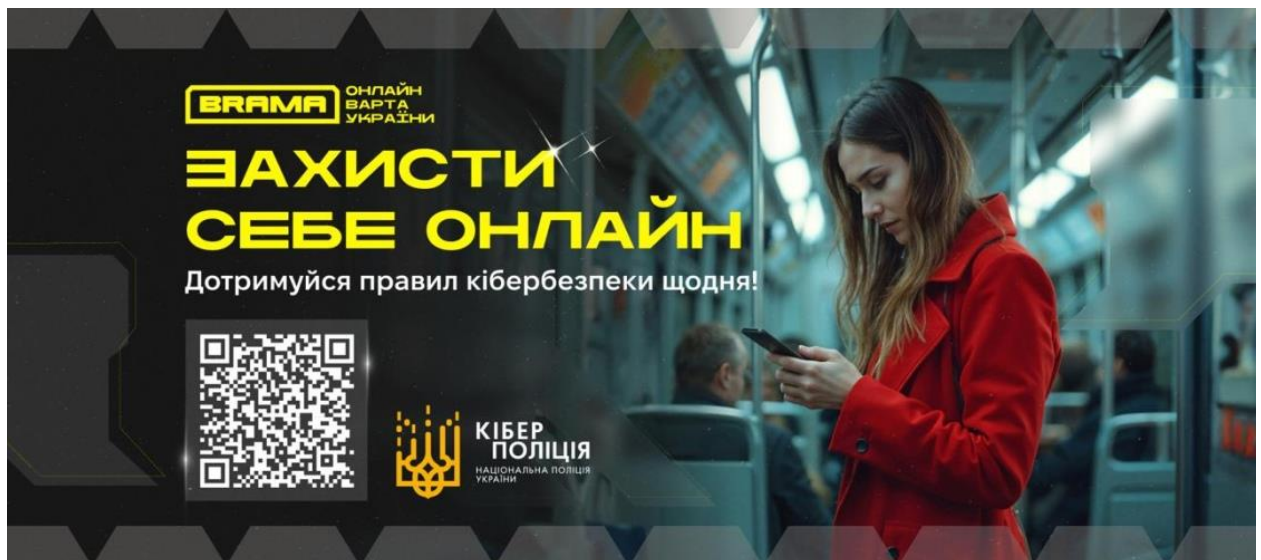
- Завжди перевіряйте, **хто вам пише і яку компанію представляє.**
- Не погоджуйтесь **“просто пересилати гроші”** — це вже привід для підозри.
- Пам'ятайте: **швидкі гроші без зусиль — це майже завжди шахрайство.**

Будьте пильні!

Навіть якщо вам дуже потрібні гроші — не погоджуйтесь на “роботу”, де треба використовувати свої банківські реквізити. Ви ризикуєте свободою заради короткочасного прибутку. Дроп — це не просто випадкова роль. Це — кримінальна відповідальність.

Збір коштів

Отримали повідомлення від знайомої щодо підтримки однієї з бригад ЗСУ, запевнила що сайт установи перевірений яка контролює збір коштів, після відправки коштів отримала повідомлення нецензурного характеру на російській мові.



Розсилання повідомлень начебто від офіційних установ про збір коштів на ЗСУ.

Пам'ятайте:

- ✓ Безпека збереження коштів та користування рахунками починається з Вас.
- ✓ 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.

На замітку:

- *Не довіряй збору без офіційних підтверджень!*
- *Псевдозбори шкодять ЗСУ більше, ніж ворог!*
- *Допомога ЗСУ має бути реальною, а не фейковою!*
- *Кожна гривня має працювати на перемогу, а не на шахраїв!*
- *Лжезбори — злочин проти своєї армії!*

Купівля товару в Інтернеті

Купуючи на сайті дитячі речі, продавець попросив часткову передоплату та надав реквізити для оплати. Після здійснення мною оплати, продавець видалив оголошення, в подальшому зв'язок із продавцем був втрачений, свого замовлення я не отримав, кошти мені не повернулися.



Зловмисники можуть "продавати" в інтернеті товари, яких насправді не існує, за частковою передплатою або повною оплатою наперед.

Пам'ятайте:

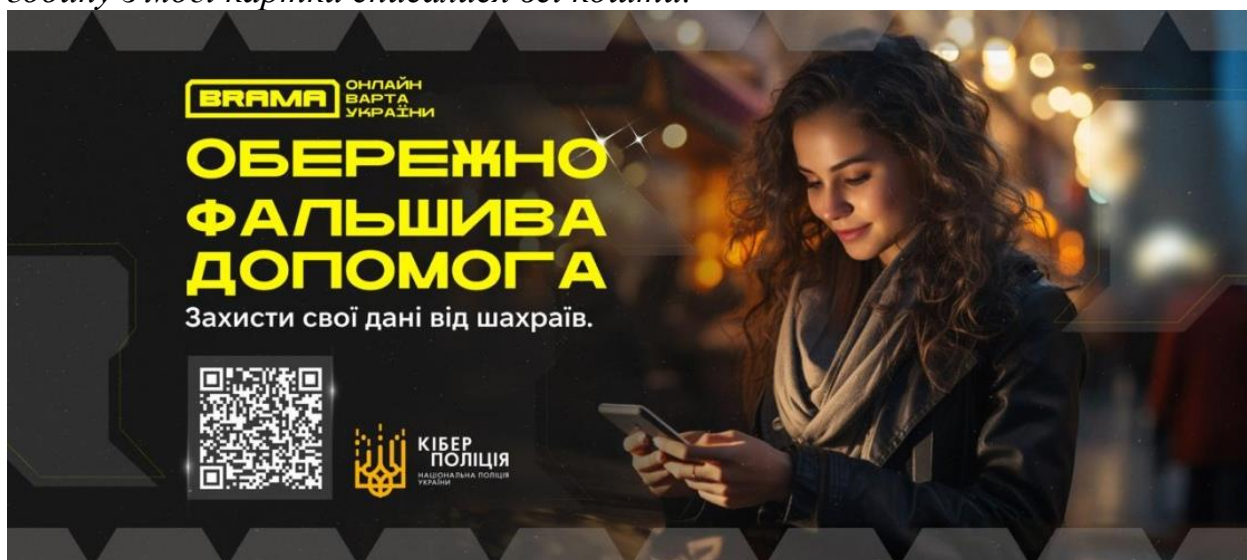
- ✓ Купуйте товари та сплачуйте кошти лише на перевірених сайтах.
- ✓ У разі сумнівів надайте перевагу післяплаті.
- ✓ Для онлайн-шопінгу відкрийте віртуальну картку і переказуйте на неї лише суму грошових коштів, необхідну для подальшої оплати.
- ✓ Перевіряйте правильність назви необхідного сайту (один непомітний символ на панелі адреси може означати, що ви потрапили на фішинговий ресурс).
- ✗ 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.

На замітку:

- *Передплата може коштувати втрати всього!*
- *Купуючи онлайн, не сплачуй наперед!*
- *Сумніваєшся в продавці? Краще відмовся!*
- *Фейковий товар = фейковий продавець!*
- *Онлайн-шопінг потребує уваги: перевір усе двічі!*

Надання фінансової допомоги

Надійшло повідомлення від ООН про надання фінансової допомоги кожному громадянину України, в якому потрібно перейти за посиланням для подачі заяви, перейшов за посиланням, заповнив анкету, дивне було питання про мої банківські реквізити, але і на нього я дав повну відповідь. Після чого через годину з моєї картки списалися всі кошти.



Вам може надійти повідомлення в месенджері або пост у соцмережах про надання фінансової допомоги, яку може отримати будь-хто. Ця схема так званий фішинг*.

**Фішинг- метод соціальної інженерії, коли дії правопорушника передбачають отримання (виманювання) правопорушниками у держателів платіжних карток їхніх реквізитів та іншої конфіденційної інформації шляхом імітації діяльності у кіберпросторі державних соціальних програм, компаній, банків-емітентів з використанням неголосових засобів комунікації під різними приводами.*

Гроші пропонують нібито від імені державних, міжнародних установ або банків.

Повідомлення зазвичай містить посилання на чат-бот або сайт, де нібито можна дізнатись додаткову інформацію.

Пам'ятайте:

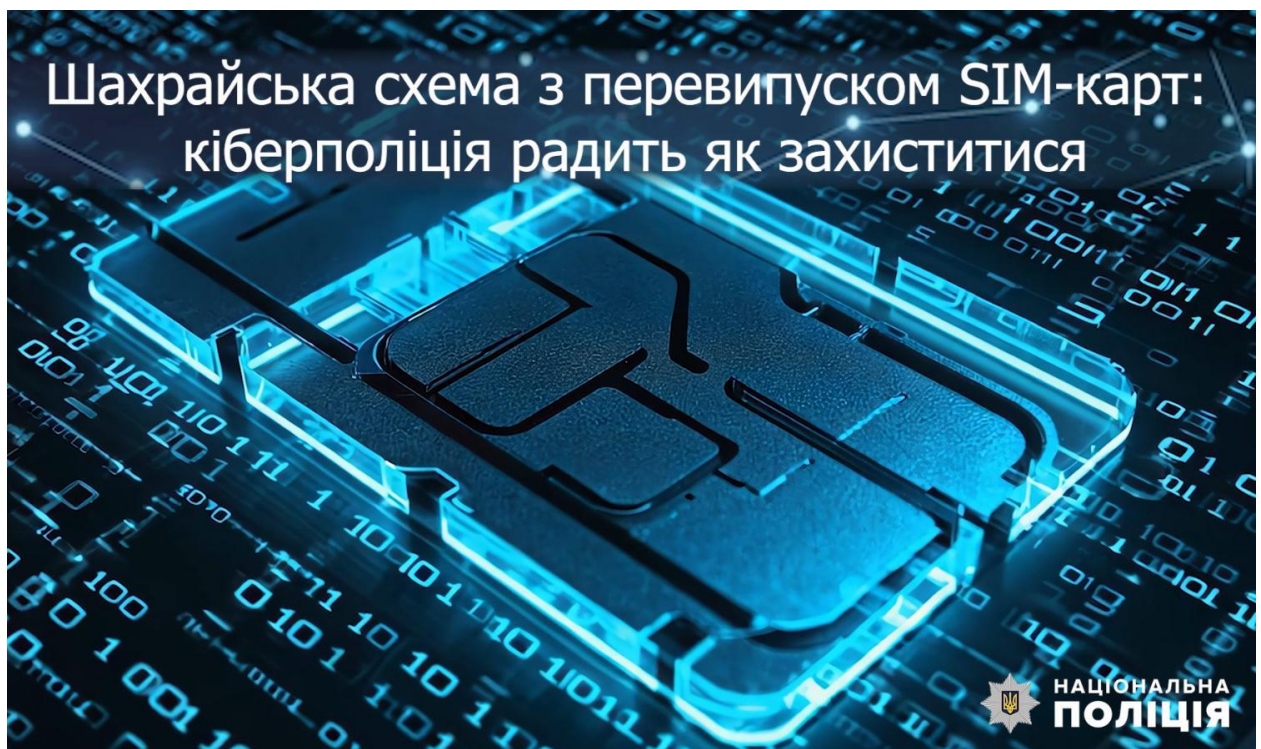
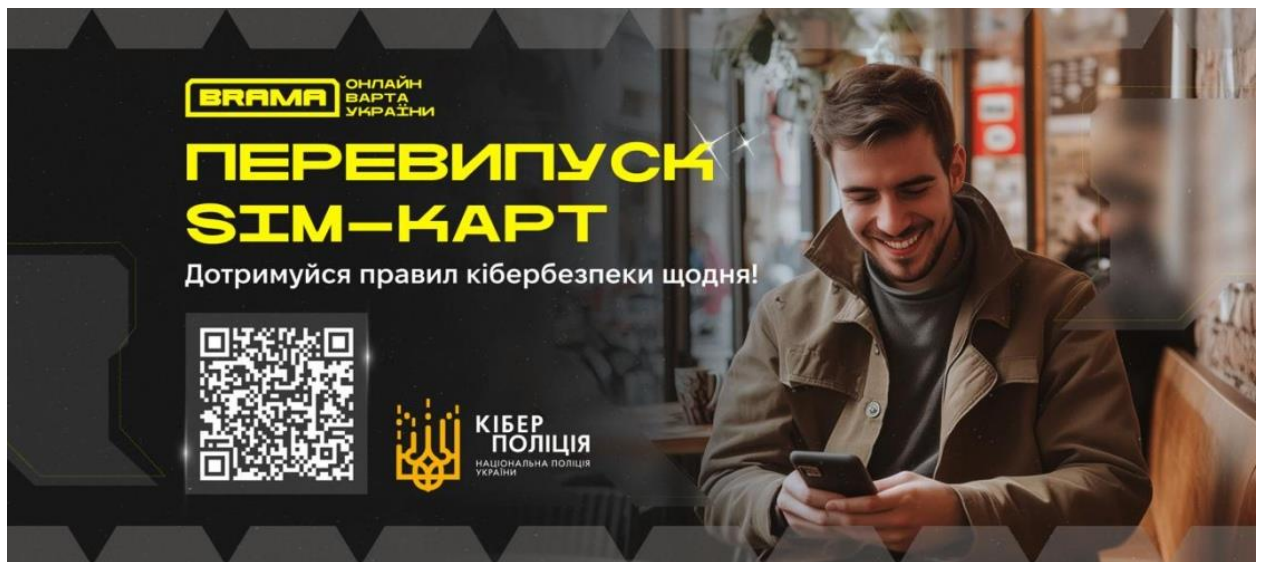
- ✓ Потрібно отримувати інформацію, особливо з приводу фінансових виплат, лише з офіційних джерел.
- ✓ Якщо ж особисту (персональну) інформацію розголошено, потрібно звернутись до банку та заблокувати картку.
- ✓ Якщо підозрюєте шахрайство – негайно повідомляйте правоохоронців.
- ✗ Ніколи не переходьте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

На замітку:

- *Допомога без перевірки — крок у шахрайську пастку!*
- *Міжнародна допомога? Спочатку переконайся, що це реально!*
- *Фейкові установи полюють на твої гроші!*
- *Чи варто довіряти посиланню з повідомлення?*

Перевипуск SIM-карт

Одна з небезпечних злочинних махінацій – перевипуск sim-картки без відома власника. Отримавши контроль над вашим номером, зловмисники можуть отримати доступ до банківських рахунків, оформити кредити на ваше ім'я, а також зламати електронні облікові записи та використати їх для зловмисних цілей.



Таким чином, втрата власної sim-картки — це не лише побутові незручності, а й серйозна загроза фінансовій безпеці та приватності громадян. Тому важливо знати, як протидіяти таким атакам і які кроки здійснити у разі підозри на зловмисні дії.

Шахраї використовують методи соціальної інженерії, фішингові сайти тощо, щоб змусити людину передати необхідні дані або виконати необхідні дії.

Злочинці навіть можуть навмисно телефонувати жертві з різних номерів, щоб потім використати ці ж номери для підтвердження перевипуску sim-картки.

Як убезпечити себе

1. Будьте обережні з дзвінками від нібито представників мобільного оператора. Якщо вам телефонують із проханням надати код підтвердження або особисті дані, не передавайте інформацію та одразу завершіть розмову. У разі сумнівів самостійно зателефонуйте до свого оператора за офіційним номером.
2. Якщо підозрюєте, що вашу карту хочуть перевипустити - негайно зверніться до служби підтримки мобільного оператора. Повідомте про підозрілу активність та заблокуйте віддалений перевипуск sim-карти.
3. Перервіть “ланцюжок” шахрайських дзвінків. Якщо вам телефонують із підозрілими пропозиціями чи проханням передзвонити - відразу зателефонуйте своїм знайомим або родичам – це дозволить розірвати можливий шахрайський механізм.
4. Забороніть віддалений перевипуск sim-картки. У налаштуваннях мобільного оператора або через контактний центр можна активувати функцію, що дозволяє перевипуск sim-картки лише при особистому візиті до офіційного магазину та з пред’явленням паспорта.
5. Використовуйте унікальний номер для фінансових операцій. Бажано мати окремий номер телефону для банківських операцій, який не зазначається у відкритому доступі, зокрема в оголошеннях чи для соціальних мереж, чи месенджерів.
6. Розгляньте можливість переходу на контрактне обслуговування або прив’язку передплаченого номера телефону до паспорта. Така форма підключення забезпечує вищий рівень безпеки, оскільки перевипуск sim-карти можливий лише за особистої присутності та пред’явлення документа.

Також ви можете звернутися до свого мобільного оператора й дізнатися про інші додаткові заходи безпеки (наприклад, підтвердження зміни sim-картки через відеоверифікацію або перевірку за паспортом), і попросити увімкнути їх. Зауважте, що деякі оператори можуть стягувати додаткові кошти за подібні послуги.

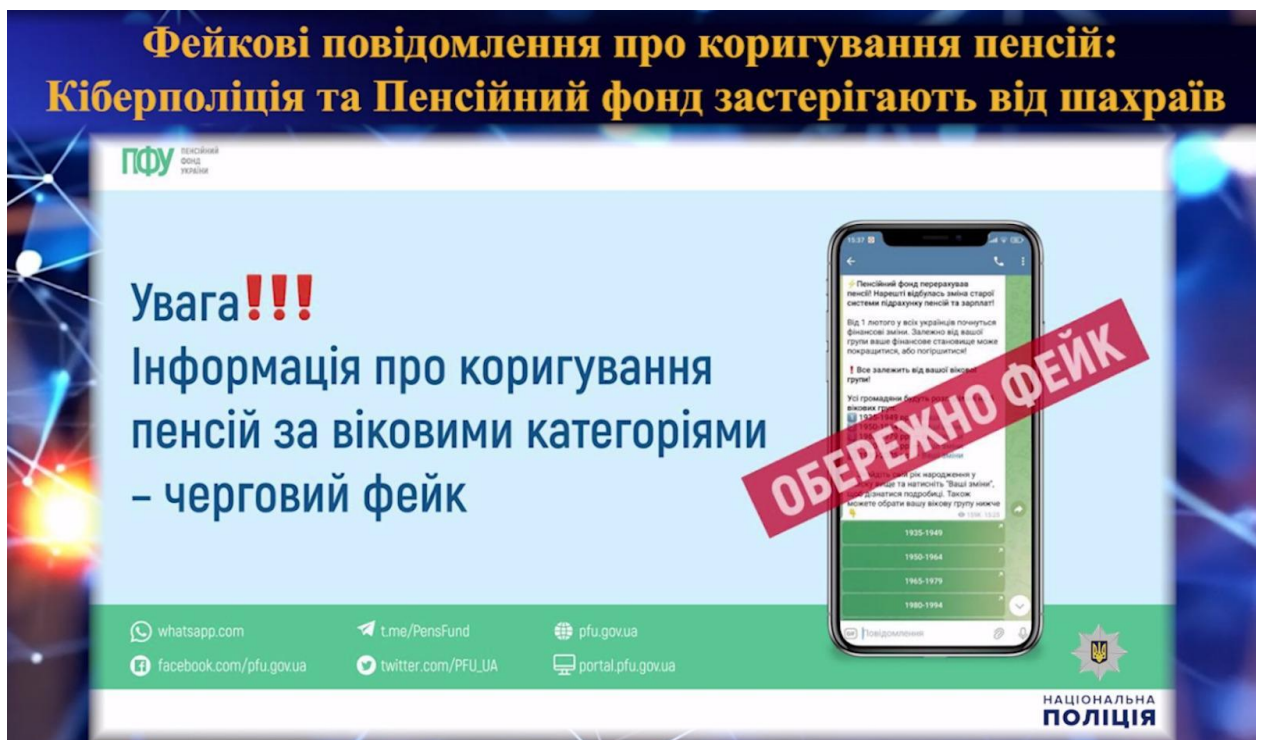
Що робити, якщо стали жертвою шахраїв

- негайно зверніться до мобільного оператора та повідомте про перевипуск sim-картки без вашого відома. Попросіть тимчасово заблокувати номер.
- При підозрі, що шахраї отримали доступ до банківського акаунту – зв'яжіться з банком та заблокуйте картки та онлайн-доступ.
- Перевірте доступ до своїх облікових записів у соціальних мережах та електронній пошті. Якщо є підозра на злам - змініть паролі.
- Якщо шахраї отримали доступ до ваших акаунтів - повідомте про це друзям та знайомим, щоб вони не потрапили у пастку шахраїв (наприклад, якщо шахраї будуть просити гроші від вашого імені).
- Зверніться до правоохоронних органів із заявою про шахрайство або подайте електронне звернення до кіберполіції за посиланням <https://ticket.cyberpolice.gov.ua>.

Пам'ятайте, що головна лінія захисту – ваша пильність. Дотримання базових правил безпеки може допомогти уникнути фінансових втрат та захистити приватність вашого життя.

Підвищення пенсії

Зловмисники розповсюджують у соціальних мережах та месенджерах неправдиву інформацію про нібито нові правила нарахування пенсійних виплат. Шахраї видають себе за представників ПФУ та пропонують заповнити «офіційну анкету» на підконтрольних сайтах.



Звертаємо вашу увагу: такі повідомлення є фейковими! Вони не мають жодного відношення до діяльності Пенсійного фонду України та створені виключно з метою введення громадян в оману.

Як працює шахрайська схема?

Зловмисники публікують оголошення з гучними заголовками та посиланням на підроблений сайт, стилізований під офіційний ресурс. Аферисти закликають пенсіонерів терміново заповнити анкету, використовуючи методи соціальної інженерії. У результаті громадяни, не підозрюючи обману, вводять свої особисті та банківські дані на сторонніх ресурсах, які одразу стають відомі зловмисникам і можуть бути використані у шахрайських схемах.

Як не стати жертвою?

- **Довіряйте лише офіційним джерелам** – усі зміни щодо пенсійних виплат публікуються передусім на вебпорталі Пенсійного фонду України за посиланням www.pfu.gov.ua та його офіційних сторінках у соціальних мережах.
- **Перевіряйте посилання** – офіційні сайти державних установ завжди мають домен **gov.ua**.
- **Не переходьте за підозрілими посиланнями** – навіть якщо їх надіслали знайомі, адже їхні акаунти могли бути зламані.
- **Не розголошуйте свої персональні дані** – Фонд не вимагає вводити конфіденційну інформацію через анкети у месенджерах.
- **Попередьте рідних та близьких** – шахраї часто орієнтуються на людей поважного віку, тому важливо вчасно розповідати їм про можливу загрозу.

Позичити гроші

Я отримав повідомлення в телеграм від свого знайомого, який просить позичити кошти на зазначений номер картки в повідомленні, я без вагань здійснив переказ коштів, після зателефонував цьому знайомому – виявилось, що шахраї зламали його телеграм.



Знайома людина просить позичити грошей в особистому повідомленні в месенджері соціальної мережі. Це може бути хтось, із ким ви давно не спілкуєтесь, але є ризик, що сторінку людини зламали шахраї.

Знайомою людиною може бути друг, родич, колега тощо. Вона надсилає Вам особисте повідомлення в месенджер*, у т.ч. соціальної мережі.

**Месенджер — це безкоштовний мобільний додаток для обміну повідомленнями, який використовується для обміну миттєвими повідомленнями, обміну фотографіями, відео, аудіозаписами та для групових чатів. Приклади месенджерів: viber, whats app, telegram, messenger facebook, direct instagram та ін.*

Та просить Вас позичити їй грошей (зазвичай, перерахувати на вказану нею банківську картку чи поповнити рахунок номеру мобільного телефону). Це може бути хтось, із ким ви давно не спілкуєтесь чи навпаки, спілкуєтесь дуже часто. Головне, у цьому випадку Ви повинні завжди пам'ятати те, що, можливо, акаунт* месенджеру чи соціальної мережі* цієї людини зламали шахраї (підпорядкували собі управління акаунтом) та від імені вашого знайомого просять у вас гроші.

**Акаунт — обліковий запис людини у якійсь системі реєстрації та інформація пов'язана з таким записом.*

**Соціальна мережа — це сервіс (інтернет майданчик) для підтримки соціальних зв'язків в Інтернеті. Важливим елементом соцмережі є контент (зміст, інформація), створений користувачами (власниками акаунтів у даній мережі).*

Якщо дійсно таке трапилося, то дії даних осіб називаються шахрайством. Шахрайство — це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою.

Відповідальність за вчинення шахрайства регулюється ст. 190 Кримінального кодексу України та передбачена від штрафу у розмірі двох тисяч неоподатковуваних мінімумів доходів громадян до дванадцяти років позбавлення волі з конфіскацією майна, в залежності від суми завданого збитку та кількості осіб, які вчинюють шахрайські дії.

Пам'ятайте:

☒ 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 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 можуть знайти її в інтернеті).

На замітку:

- *Друзі не просять грошей у месенджерах — перевір двічі!*
- *Чужий акаунт може стати шахрайським інструментом!*
- *Не поспішай допомагати онлайн — це може бути пастка!*
- *Переконайся, що це дійсно твій знайомий!*
- *Позичати в мережі — ризик втратити більше!*

Продаж товару в Інтернеті

Купив собі новий телефон, попередній виставив на продаж на одній із дошок оголошень. Мені телефонує покупець, просить реквізити для оплати та каже що зробить повну оплату наперед що б уникнути комісії накладеного платежу при доставці Новою поштою. Одразу ж мені телефонує невідомий номер, представляється працівником банку і намагається вивідати у мене платіжну інформацію по моїй картці під приводом зарахування мені коштів від юридичної особи. Після чого з моєї картки списалися всі кошти.



Псевдопокупець може запитати реквізити картки для оплати за ваш товар на дошці оголошень і назвати час здійснення переказу або щось подібне.

У цей час напарник зловмисника під виглядом працівника служби безпеки банку може зателефонувати вам і сказати, що для зарахування грошей необхідно вчинити якусь дію, наприклад "активувати платіжну картку".

Таким чином шахраї будуть намагатися вивідати у вас реквізити та інші дані по вашому рахунку.

Пам'ятайте:

- ☒ 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.

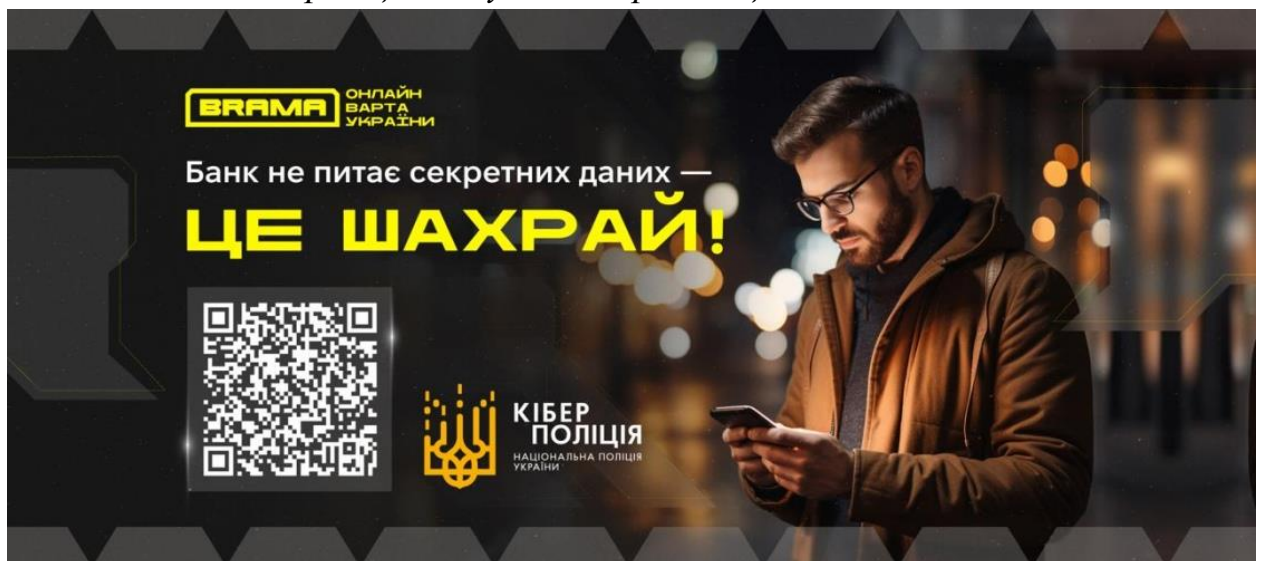
- ✓ Безпека збереження коштів та користування рахунками починається з Вас.

На замітку:

- *Твоя безпека — твої секрети. Не розголошуй дані!*
- *Служба банку не питає паролів та кодів!*
- *Телефонний "покупець"? Можливо, це шахрай!*
- *Ніколи не активуй фейкові платежі!*
- *Шахраї працюють у парі — будь напготові!*

Телефонують зі служби безпеки банку

Перебуваючи в транспорті отримала дзвінок від працівника банку, який повідомив що з мого рахунку намагаються зняти кошти та перевести на сумнівну картку, терміново необхідно назвати номер своєї картки, термін дії та код для ідентифікації та зупинки транзакції.



Телефонують з банку під виглядом працівників і виманюють реквізити карти, код (або від імені державних установ чи операторів мобільного зв'язку)

Пам'ятайте:

- ✓ Безпека збереження коштів та користування рахунками починається з Вас.
- ✓ Використовуйте під час будь-яких операцій у мережі "Інтернет" чи онлайн-оплаті послуг лише інтернет-карти, на які переказуйте кошти з основного рахунку в сумі, яка необхідна для оплати або переказу! Не дайте змоги шахраям заволодіти реквізитами до основного рахунку та викрасти кошти.
- ✓ Ніколи не розміщуйте об'яви в мережі "Інтернет" з вказанням фінансового номеру. Шахраї, отримавши цю інформацію, можуть звернутись до оператора мобільного зв'язку та здійснити його перевипуск, отримати доступ до

інтернет-банкінгу та заволодіти коштами. Якщо ви виявили, що сімкартка з якоїсь причини заблокована, мерщій зверніться до найближчого відділення банку та заблокуйте карткові рахунки. Краще їх потім розблокувати, аніж залишитись без коштів.

✓ Використовуйте контрактну основу надання послуг мобільним оператором, тоді шахраям буде важко перевипустити ваш фінансовий номер.

✓ Використовуйте послугу код-пароллю на перевипуск або блокування сімкарт, який знаєте лише ви та мобільний оператор, бо, не маючи цієї інформації, шахрай не досягне злочинної мети.

✗ Працівник банку ніколи не зателефонує до клієнта та не буде випитувати реквізити карти, термін дії, CVV код та 3ds підтвердження, він запросить вас до відділення банку.

✗ Не повідомляйте нікому тимчасові паролі, які приходять в смс-повідомленні. Розголошення цієї інформації призведе до втрати коштів.

✗ Співробітник банку ніколи не буде телефонувати та розповідати про якісь псевдошахрайські операції по рахунку, він просто заблокує картковий рахунок і ви будете змушені звернутись до відділення банку для з'ясування обставин.

✗ Співробітник банку ніколи не запропонує встановити програми для віддаленого керування рахунками (Тімв'ювер, АніДеск та ін...).

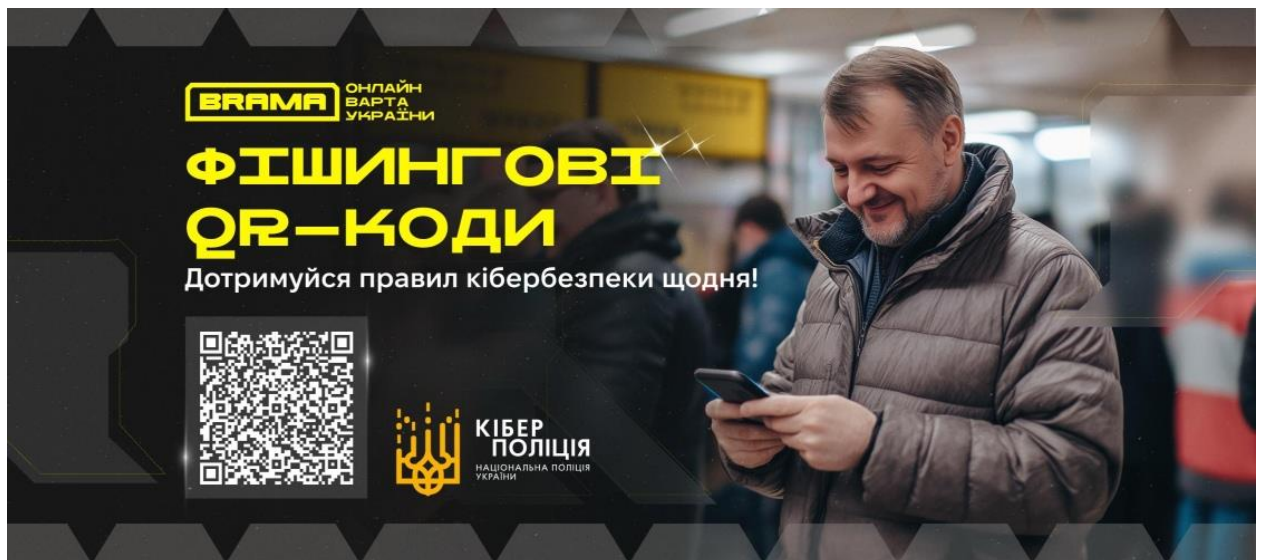
✗ Не виконуйте ніяких дій у банкоматах чи терміналах за вказівкою співробітника банку (проведення маніпуляцій у банкоматах чи терміналах)

На замітку:

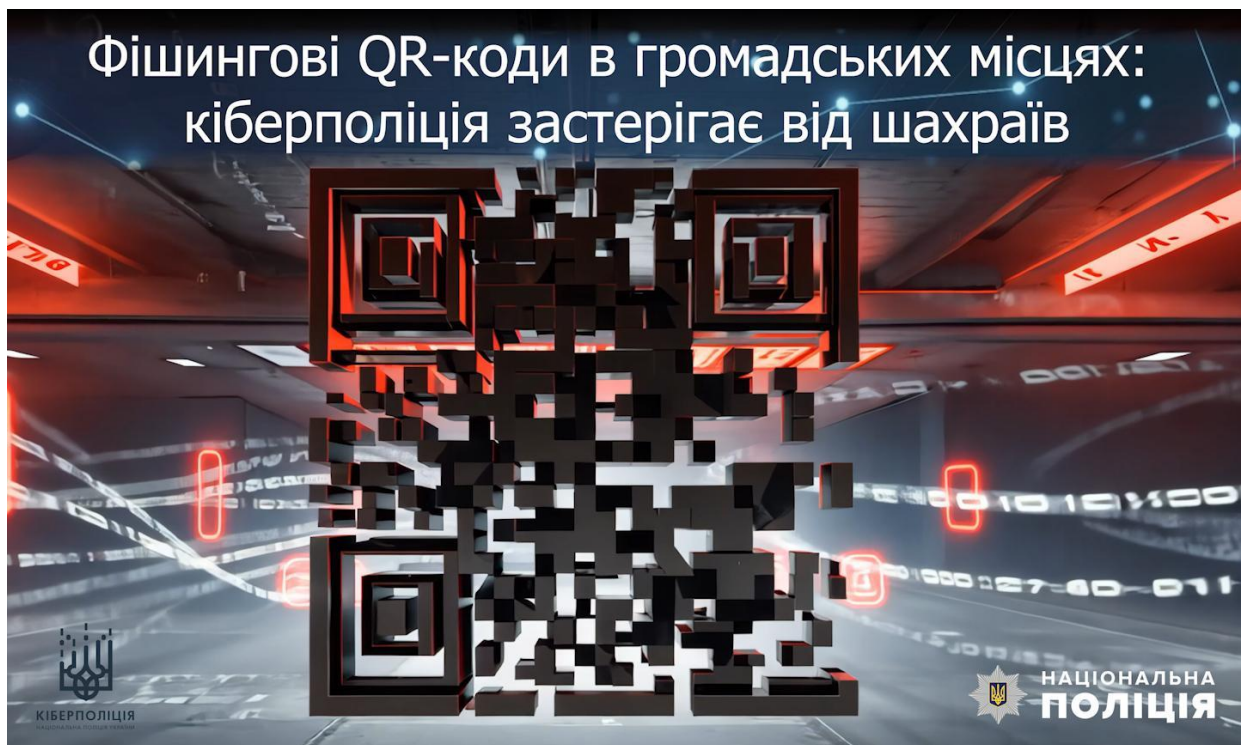
- *Банк не питає секретних даних — це шахрай!*
- *Телефонний дзвінок — ще не доказ, що це банк!*
- *Коди й паролі — це твої гроші. Бережи їх!*
- *Шахрай намагається дізнатися більше — зупини це!*
- *Банківські дані — це твоє приватне життя. Захисти його!*

Фішингові QR-коди в громадських місцях: кіберполіція застерігає від шахраїв

В Україні знову активізувалася шахрайська схема, пов'язана з підміною QR-кодів у загальнодоступних місцях. Зловмисники використовують фішингові сайти, щоб отримати дані банківських карт громадян.



Шахраї підмінюють QR-коди на офіційних інформаційних табличках або просто розміщують їх в громадських місцях. Скануючи такі коди, користувачі потрапляють на підроблені сайти, що імітують реальні онлайн-сервіси. У результаті зловмисники можуть отримати доступ до банківських даних і викрасти кошти.



Найчастіше такі випадки трапляються у місцях, де люди активно використовують QR-коди для швидких оплат: під час паркування, оплати громадського транспорту, входу на заходи чи здійснення благодійних внесків.

Візуально відрізнити якісно підроблений код від справжнього дуже складно, тому головна порада – завжди перевіряти адресу сайту перед введенням будь-яких конфіденційних даних.

Щоб уберегтися від шахраїв, варто дотримуватися кількох правил:

- скануйте QR-коди лише з надійних джерел – уникайте кодів, розміщених на випадкових наклейках, листівках або рекламних оголошеннях.
- перед скануванням перевіряйте наклейку – звертайте увагу на можливі сліди підробки (додатковий шар, нерівні краї, інший шрифт).
- використовуйте функцію попереднього перегляду посилання – більшість смартфонів дозволяють побачити URL перед переходом.
- завжди звертайте увагу на веб-адресу після переходу за QR-кодом – навіть якщо сайт виглядає переконливо, будь-які відмінності в домені можуть бути ознакою шахрайства.
- Перевіряйте наявність захищеного з'єднання (https://) – якщо сайт не має сертифіката безпеки, вводити на ньому будь-яку інформацію небезпечно.
- Не вводьте банківські дані на невідомих сайтах та без необхідності.
- Якщо ви виявили підозрілий QR-код – повідомте адміністрацію закладу, службу підтримки або правоохоронні органи.
- Використовуйте віртуальні або тимчасові картки для онлайн-платежів – це допоможе уникнути значних фінансових втрат у разі витоку фінансових даних картки.

Якщо ви стали жертвою шахрайства - негайно зверніться до банку для блокування картки та подайте електронне звернення до кіберполіції за посиланням <https://ticket.cyberpolice.gov.ua>.

Фішингові посилання

Популярність маркетплейсів серед українців зростає, що створює поле діяльності для шахраїв. Одна з найпоширеніших схем аферистів – фішингові посилання, які імітують вигляд маркетплейсів та мають на меті виманити дані банківських карток.



Як захистити себе від фішинг-афери на маркетплейсах: поради для українців

Популярність онлайн-торгівлі в Україні зростає з кожним роком, і маркетплейси стають основними майданчиками для покупок. Але з цим приходять і нові загрози, зокрема, шахрайські схеми, спрямовані на виманювання особистих даних та грошей у користувачів. Однією з найбільш поширених схем є фішингові посилання, що імітують вигляд популярних маркетплейсів.

Що таке фішинг і як він працює?

Фішинг — це шахрайська практика, коли зловмисники намагаються отримати конфіденційну інформацію користувача, наприклад, логіни, паролі чи дані банківських карток. Для цього вони створюють фальшиві веб-сайти, які виглядають схожими на справжні платформи, такі як маркетплейси. Відвідавши таке посилання, користувачі можуть випадково ввести свої персональні дані або оплатити покупку через небезпечний ресурс.

Як розпізнати фішинг?

✅ **Перевірте URL-адресу.** Офіційні сайти маркетплейсів мають правильні та безпечні доменні імена (наприклад, "rozetka.ua" або "olx.ua"). Якщо ж у посиланні присутні сумнівні символи, додаткові цифри чи літери, або якщо адреса виглядає трохи зміненою, наприклад, "roz3tka.ua" або "olx.com.ua", це може бути ознакою фішингу.

✅ **Перевірте дизайн сайту.** Фальшиві сайти часто виглядають схоже на оригінальні, але зазвичай мають низьку якість графіки, помилки у тексті або незвичну структуру. Якщо ви помітили подібні недоліки, краще покинути сайт.

✅ **Звертайте увагу на розсилки.** Легітимні маркетплейси зазвичай не просять вводити особисту інформацію через електронну пошту або месенджери. Якщо ви отримали таку вимогу, будьте обережні.

✅ **Перевірка через офіційний сайт або додаток.** Якщо вам здається, що з вами зв'язуються з офіційного маркетплейсу, краще зайти на сайт або відкрити додаток через перевірений канал, а не за посиланням у листі чи повідомленні.

❌ **Остерігайтеся підозрілих повідомлень.** Якщо ви отримали листи або повідомлення через соцмережі з посиланнями на "подарунки" чи "знижки", це може бути спробою заманити вас на фальшивий сайт. Часто такі повідомлення містять заклики терміново ввести дані або здійснити оплату.

Як захистити себе від фішингу?

✅ **Використовуйте двофакторну автентифікацію.** Більшість сучасних маркетплейсів пропонують додаткові засоби безпеки, такі як SMS-коди або підтвердження через додаток. Це знижує ризик несанкціонованого доступу до вашого акаунту.

✅ **Перевіряйте покупку через додаток чи офіційний сайт.** Не вводьте платіжні дані на сторонніх сайтах. Завжди використовуйте лише перевірені ресурси.

✅ **Слідкуйте за оновленнями безпеки.** Переконайтеся, що ваш браузер та операційна система оновлені до останніх версій. Це допоможе захистити вас від багатьох онлайн-загроз.

✅ **Будьте обережні з публічними Wi-Fi мережами.** Уникайте здійснювати покупки чи вводити особисті дані, коли підключені до незахищених мереж.

❌ **Не довіряйте занадто гарним пропозиціям.** Якщо якась пропозиція здається надто вигідною, щоб бути правдою, швидше за все, це пастка.