Інформаційна кампанії з платіжної безпеки #ШахрайГудбай!

Друзі, розпочинається новий етап інформаційної кампанії з платіжної безпеки #ШахрайГудбай. Її організаторами є Національний банк України, Департамент кіберполіції Національної поліції України і Державна служба спеціального зв'язку та захисту інформації України.

Мета кампанії – поліпшити обізнаність громадян та нагадати їм про основні правила безпеки під час безготівкових розрахунків, особливо в інтернеті.

У 2025 році кількість шахрайських операцій із платіжними картками, за якими були зазнані збитки, зменшилася на 5% порівняно з 2024 роком — до 256 тисяч випадків. Водночас сума збитків від таких операцій збільшилася майже на чверть — до 1,4 млрд грн.

Це свідчить про те, що, попри зменшення кількості випадків, масштаб втрат від шахрайства зростає. Тема платіжного шахрайства залишається актуальною та зумовлює необхідність системної просвітницької роботи серед населення.

Найпопулярнішим методом шахрайства з платіжними картками в Україні, як і в усьому світі, традиційно залишається соціальна інженерія, коли люди самостійно, не підозрюючи підступу, повідомляють шахраям свої персональні дані, реквізити карток, коди підтвердження чи паролі для здійснення платежів.

Поліпшення знань щодо безпечного користування платіжними картками та інтернет-банкінгом допоможе громадянам уберегтися від шахрайських пасток у віртуальному просторі.

Під час кампанії ми будемо говорити про те:

- як уберегтися від шахрайства під виглядом державних послуг;
- як уникнути інвестиційного шахрайства;
- як перевіряти сайти, чат-боти, на яких користувачі вводять свої платіжні дані;
- як безпечно купувати в інтернеті;
- як захистити свій фінансовий номер телефону;
- як уникнути найпоширеніших схем шахрайства;
- як випадково не стати співучасником злочину та не потрапити в пастку шахраїв під час пошуку роботи;

Кампанія триватиме до кінця року у всіх регіонах України. До кампанії долучилося близько 80 партнерів.

Також у нас є сайт, на якому можна знайти багато цікавої та корисної інформації: https://promo.bank.gov.ua/stopfraud/.

Слідкуйте за нашими публікаціями та дізнавайтеся більше про те, як захистити свої фінанси!

Інформаційна кампанія #ШахрайГудбай реалізується за підтримки Європейського Союзу в рамках проєкту «Подальше наближення регуляторної бази до законодавства Європейського Союзу та міжнародних стандартів на фінансових ринках в Україні» (FINMAR).

#ШахрайГудбай

Фінансова піраміда — це шахрайська схема, у якій кошти учасників не генеруються в результаті реальної діяльності, а перерозподіляються між вкладниками.

Ознаками фінансової піраміди є:

• обов'язковий вступний внесок;

• декларування прибутку без реальної діяльності;

• здійснення виплат за рахунок нових учасників;

• те, що немає прозорої бізнес-моделі.

Після зменшення припливу нових коштів функціонування такої схеми припиняється, більшість учасників зазнає збитків.

Як працює фінансова піраміда?

Спочатку перші вкладники отримують виплати, що створює довіру та стимулює масове залучення нових учасників. Коли нових грошей стає менше, схема припиняє діяльність і більшість інвесторів втрачає кошти.

Сучасні фінансові піраміди маскуються під:

• криптовалютні або трейдингові проєкти ("ШІ-бот торгує за вас");

• green-energy ініціативи ("інвестиції в сонячні ферми");

• ШІ-стартапи ("алгоритм прогнозує ринок");

• e-commerce-моделі ("оренда складів Amazon" або "пасивний дохід від онлайн-продажів");

• GameFi або заробіток у метавсесвіті (ігри з обіцянкою доходу);

• інвестиційні клуби та платформи пасивного доходу;

• навчальні або менторські програми.

Форма змінюється. Механіка — ні.

Пам'ятайте: якщо прибуток залежить не від реального бізнесу, а від припливу нових учасників, то це – фінансова піраміда.

Перевіряйте інформацію в офіційних джерелах і не приймайте рішення під тиском.

У разі виявлення ознак інвестиційного шахрайства рекомендуємо невідкладно звернутися до правоохоронних органів, зокрема шляхом подання електронного звернення до кіберполіції: https://ticket.cyberpolice.gov.ua.

Більше інформації — на сайті #ШахрайГудбай: https://promo.bank.gov.ua/stopfraud/.

#ШахрайГудбай

Шахраї активно використовують тему складання іспитів у сервісних центрах МВС. Обіцяють “допомогу”, “гарантований результат” або “без черги”. Такі пропозиції поширюють у фейкових акаунтах у соціальних мережах під виглядом сервісних центрів МВС. На перший погляд, це здається швидким рішенням в отриманні посвідчення водія.

Як це працює?

Вам пропонують швидко отримати посвідчення водія.

Для цього просять переказати гроші на приватну картку, також можуть просити надіслати копії документів.

Після цього:

- гроші зникають;
- “посередник” більше не відповідає;
- жодного впливу на іспит він не мав.

Щоб здаватися переконливими, шахраї використовують у своїх акаунтах та групах:

- назву сервісного центру МВС із конкретним номером;
- справжні фото з офіційних ресурсів сервісних центрів МВС;
- фейкові відгуки “клієнтів”, які нібито отримали офіційне посвідчення водія;
- графік роботи та офіційні номери телефонів сервісних центрів МВС.

Не переказуйте гроші незнайомим особам.

Жоден сервісний центр МВС не продає посвідчення водія онлайн.

 Пам’ятайте: у сервісних центрах МВС немає платних “допомог” чи “прискорень”.

Єдиний шлях – скласти іспит офіційно.

Водійські документи видаються за єдиним для всіх алгоритмом.

Щоб отримати посвідчення водія, потрібно:

- вивчити правила дорожнього руху за самопідготовкою або в автошколі;
- скласти теоретичний іспит у ТСЦ МВС;
- пройти практичне навчання в автошколі;
- скласти практичний іспит в сервісному центрі МВС. Лише після цього посвідчення водія видається особисто власнику в руки після пред’явлення документа, що посвідчує особу.

Пам’ятайте! Персональні дані та копії документів зловмисники можуть використати в інших шахрайських схемах, у тому числі щоб оформити кредити або зламати акаунти. Тому не варто передавати персональні дані стороннім особам в інтернеті.

Користуйтеся тільки офіційними ресурсами в отриманні державних послуг.

Про можливі шахрайські дії можна повідомити кіберполіцію через форму на сайті: https://ticket.cyberpolice.gov.ua/.

Більше інформації про шахрайство – на сайті #ШахрайГудбай: https://promo.bank.gov.ua/stopfraud/.

Завдяки штучному інтелекту сьогодні можна створювати реалістичні фото й відео за лічені хвилини — настільки правдоподібні, що відрізнити правду від вигадки стає дедалі складніше. Сьогодні достатньо кількох натискань, щоб згенерувати зображення події, якої ніколи не було:

- фото чи відео відомої людини, яка нібито щось сказала або зробила;
- вигадані катастрофи;
- сенсаційні новини.

Такі матеріали швидко поширюються в соціальних мережах і можуть вводити в оману тисячі людей. Саме тому важливо **перевіряти інформацію і не довіряти картинці з першого погляду**.

На що слід звертати увагу?

1. **Деталі зображення**. Збільшіть фото. ШІ часто допускає помилки: неприродні тіні, викривлені лінії, дивні текстури або елементи (сходинки, стіни, стеля, меблі, натовп).
2. **Руки та обличчя**. Можуть бути зайві пальці або їх взагалі не буде, дивні долоні або злиття пальців. Риси обличчя часто непропорційні, зуби та очі виглядають неприродно.
3. **Фон.** Розмитий або штучний задній план, повторювані об'єкти чи люди — поширена ознака генерації фото / відео через ШІ.
4. **Нереалістичний зовнішній вигляд**. Штучний блиск або мультиплікаційний вигляд — особливо помітні разом із розмитим фоном.
5. **Аксесуари**. Сережки, намиста, ремінці сумок або ґудзики можуть бути деформованими, висіти неправильно.
6. **Спотворений текст**. Вивіски, постери чи дорожні знаки часто перетворюються на незрозумілий шифр.
7. **Перевірка зображення**. Скористайтеся зворотним пошуком зображення — це спосіб перевірити картинку через спеціальні сервіси, щоб дізнатися, де і коли вона вже з'являлася в інтернеті. Найпростіший спосіб виконати зворотний пошук зображення (через Google):

- зайдіть у Google та натисніть на значок камери;
- завантажте зображення або вставте посилання на зображення;
- подивіться, де ще воно з'являлося.

Існують інструменти для перевірки контенту (зокрема, чи він згенерований ШІ), однак вони не дають 100% гарантії. Тому, користуючись такими сервісами, важливо також самостійно звертати увагу на деталі.

Важливо! Користуйтеся перевіреними інструментами, але не завантажуйте туди особисті або конфіденційні зображення (документи, банківські дані тощо).

Довіряйте критичному мисленню та перевіряйте інформацію через офіційні джерела. Якщо щось виглядає занадто ідеально або, навпаки, шокує, то це привід зупинитися і перевірити.

А якщо хочете знати більше про те, як не стати жертвою шахраїв, то заходьте на сайт #ШахрайГудбай: https://promo.bank.gov.ua/stopfraud/.

#ШахрайГудбай

Отримали повідомлення нібито від держустанови? Не поспішайте діяти – саме на це й розраховують шахраї. Зловмисники пропонують державні послуги від імені державних установ. Зокрема, можуть:

- надсилати повідомлення про виклик до суду;
- пропонувати допомогу з оформленням документів, наприклад, оформити посвідчення водія;
- обіцяти “грошові виплати”;
- надсилати повідомлення чи телефонувати від імені Пенсійного фонду України, Національного банку України чи інших державних установ.

Їхня мета – змусити вас поспішити і не перевіряти інформацію.

Як не потрапити в пастку шахраїв?

1. Будьте обережні з повідомленнями від імені державних установ

Якщо Ви отримали повідомлення з посиланням нібито від держустанови, не поспішайте переходити – воно може вести на шахрайські ресурси.

Використовуйте лише канали зв’язку, зазначені на офіційному сайті установи, а не ті, що надсилають у повідомленнях.

2. Перевіряйте сайти, на яких вводите свої дані.

Шахраї створюють фейкові сайти, які мають вигляд офіційних ресурсів державних установ. Для цього вони копіюють дизайн, логотипи та структуру сторінок.

Адреса таких сайтів може відрізнятися лише кількома символами або навіть однією літерою. Тому важливо:

• уважно перевіряти адресу сайту, краще шукати сайт самостійно через пошук;
• користуватися сайтами державних установ лише з доменом **gov.ua**;
• не переходити за посиланнями з підозрілих повідомлень.

3. Перевіряйте інформацію через офіційні джерела.

Офіційні установи не ініціюють спілкування з пропозиціями “вирішити питання” чи оформити грошову допомогу в телеграмі / вайбері / директі в інстаграм.

Якщо Вам телефонують від імені державної установи – не довіряйте одразу. Краще самостійно зателефонуйте на офіційний номер, який зазначений на офіційному сайті установи.

4. Не поспішайте виконувати вказівки з повідомлень чи під час дзвінка.

Шахраї тиснуть на емоції: “терміново”, “останній шанс”, “сьогодні потрібно оплатити” Зробіть паузу – перевірте та проаналізуйте інформацію.

5. Тримайте в секреті CVV-код, паролі, коди з SMS та не передавайте свої паспортні дані “для оформлення” послуг незнайомцям у месенджерах.

6. Не оплачуйте державні послуги на картки. Оплата державних послуг має здійснюватися тільки на офіційні рахунки.

Про можливі шахрайські дії можна повідомити кіберполіцію через форму на сайті: https://ticket.cyberpolice.gov.ua/.

Більше інформації про шахрайство – на сайті #ШахрайГудбай: https://promo.bank.gov.ua/stopfraud/.

Довіряйте лише офіційним джерелам і завжди перевіряйте інформацію.

#ШахрайГудбай

Гарний сайт, графіки прибутку та "фінансовий менеджер" не завжди означають, що перед вами справжня інвестиційна платформа.

Інвестиційні шахрайства дедалі частіше маскуються під сучасні онлайн-платформи, які можуть виглядати дуже переконливо. Ось шість ознак, які створюють ілюзію надійності, але насправді не гарантують, що платформа є легальною.

1. Професійний дизайн сайту та особистий кабінет.

Сучасний інтерфейс, графіки зростання прибутку та баланс рахунку в особистому кабінеті можуть виглядати переконливо, але не мати жодного зв'язку з реальними фінансовими ринками чи інвестиціями. Часто це лише візуальна імітація, створена для того, щоб викликати довіру та переконати користувача внести кошти.

2. Логотипи відомих компаній на сайті.

На сторінках шахрайських платформ часто можна побачити логотипи міжнародних компаній. Це створює враження підтримки з боку авторитетних брендів. Насправді такі логотипи просто скопійовані шахраями з інтернету і в жодному разі не є доказом реальної співпраці.

3. Служба підтримки або "персональний менеджер".

Шахрайські платформи нерідко використовують професійно підготовлених операторів або так званих фінансових менеджерів. Вони активно спілкуються з клієнтами, використовують складну фінансову термінологію, дають поради щодо "вигідних інвестицій" та можуть навіть переконувати вкладати більше грошей.

4. Позитивні відгуки в інтернеті.

Велика кількість позитивних коментарів або "історій успіху" не завжди є доказом чесності платформи. Відгуки можуть бути фейковими, купленими або розміщеними на сайтах і форумах, які контролюють самі шахраї.

5. Посилання на ліцензії чи сертифікати без можливості перевірки.

Шахраї можуть демонструвати на сайті документи з печатками, скани ліцензій або сертифікатів у форматі PDF. Але такі документи легко підробити. Перевіряти ліцензії фінансових компаній слід через офіційні джерела, зокрема на сайтах Національного банку України або Національної комісії з цінних паперів та фондового ринку.

6. Можна вивести невелику суму прибутку на початку.

Це поширена психологічна тактика шахраїв. Вона створює відчуття, що система працює чесно, після чого користувача переконують внести значно більшу суму. Саме на цьому етапі люди найчастіше втрачають свої кошти.

Як уберегтися від шахраїв?

Щоб зменшити ризик втрати грошей, варто дотримуватися кількох базових правил фінансової безпеки:

- перевіряти інформацію про компанію з офіційних джерел;
- критично ставитися до обіцянок швидкого або гарантованого доходу;
- не здійснювати перекази коштів на вимогу невідомих осіб;
- не встановлювати програми віддаленого доступу на свій пристрій за порадою "менеджерів" або "інвестиційних консультантів";
- у разі сумнівів утриматися від будь-яких фінансових операцій;

- перед тим, як інвестувати кошти, ознайомтеся зі списком сумнівних інвестиційних проєктів на сайті Національної комісії з цінних паперів та фондового ринку: https://cutt.ly/rtS7r2Fe;
- у разі виявлення ознак інвестиційного шахрайства повідомте про це правоохоронні органи. Зокрема, можна подати електронне звернення до кіберполіції: https://ticket.cyberpolice.gov.ua.

Більше інформації про шахрайство під маскою інвестицій — на сайті #ШахрайГудбай: https://promo.bank.gov.ua/stopfraud/

Шахраї пропонують “послуги” з виготовлення посвідчення водія, відновлення після позбавлення права керування, відкриття додаткових категорій або навіть “доставку за кордон”.

Щоб увійти в довіру, вони використовують слова: “офіційно”, “без ризиків”, “без зайвих нервів”.

Також зловмисники можуть використовувати світлини військових – як підтвердження того, що ті отримували посвідчення саме через них.

У соцмережах вони вдаються до таких маніпуляцій:

- використовують реальні фото з військовослужбовцями, які справді раніше зверталися до сервісних центрів МВС;
- обіцяють знижки та спеціальні умови для військових;
- запевняють, що посвідчення можна отримати онлайн і без іспитів;
- використовують фото публічних або відомих людей.

У рекламних відео демонструють фейкові листування та відгуки “клієнтів”, а також переконують, що посвідчення буде “легальним” і навіть відображатиметься в застосунку “Дія”.

Такі відео масово поширюються в тіктоці.

Головна мета – виманити гроші та персональні дані.

Пам’ятайте: посвідчення водія, “придбане” в інтернеті, є фальшивим. Воно не відображається в державних реєстрах і застосунку “Дія”.

Замість отримання офіційного документа можна втратити гроші, отримати лише пластикову картку без юридичної сили і ризик проблем із законом. Користуйтеся тільки офіційними ресурсами в отриманні державних послуг.

Консультацію щодо послуг сервісних центрів МВС можна отримати за телефоном: (044) 290-19-88.

Про можливі шахрайські дії можна повідомити кіберполіцію через форму на сайті: https://ticket.cyberpolice.gov.ua/.

Більше інформації про шахрайство – на сайті #ШахрайГудбай: https://promo.bank.gov.ua/stopfraud/.

Купуєте товар у магазині, продавець просить оплатити зараз, а чек обіцяє надіслати пізніше через технічні проблеми? Обережно, якщо чек не видають, то це тривожний сигнал. Це може бути шахрайство.

Чек — це не формальність. Це доказ покупки і захист ваших прав. Без нього ви фактично залишаєтеся без гарантій, тож повернути товар або довести факт оплати буде значно складніше.

Запам'ятайте: оплата без чека = ризик втратити гроші. Надійний продавець завжди видає чек одразу.

Що робити?

• Не погоджуйтеся на оплату без чека.

• Попросіть чек одразу після оплати та перевірте його.

Як перевірити справжність чека?

Згідно із законодавством України фіскальний чек містить обов'язкові реквізити:

1) назву та адресу господарської одиниці;
2) ідентифікаційний номер платника податків;
3) фіскальний номер касового апарата;
4) заводський номер касового апарата;
5) дату та час покупки;
6) інформацію про товари / послуги: назву, кількість, ціну за одиницю, загальну суму;
7) **спосіб оплати:** готівкою, карткою;
8) **податки та коди:** ПДВ, акциз, код УКТ ЗЕД (за наявності);
9) **додаткові реквізити (за наявності):** ідентифікатори еквайра та платіжного пристрою, заокруглення, суму до сплати;
10) **фіскальний номер касового або електронного чека:** дату та час проведення операції.

Також на фіскальному чеку має бути QR-код, який можна сканувати для перевірки.

Важливо! В Україні дозволено видавати фіскальні чеки не лише в паперовій, а й в електронній формі з дотриманням низки вимог. Зокрема, електронний чек може бути у вигляді текстового повідомлення, QR-коду або PDF-файла. Покупець може отримати електронний чек на свою електронну пошту, телефон або в спеціальний мобільний застосунок одразу після оплати товару.

Дотримуйтеся правил платіжної безпеки під час онлайн-покупок.

- Якщо оплачуєте товар на сайті, то обов'язково перевірте, чи він надійний. Не вводьте платіжні дані на підозрілих вебресурсах.
- Якщо купуєте на якомусь сайті вперше, то обирайте післяплату. Якщо сумніваєтеся в надійності продавця — краще відмовитися від покупки.

Купуйте обачно і безпечно.

Якщо ви стали жертвою шахрайства, то повідомте кіберполіцію через форму на сайті: https://ticket.cyberpolice.gov.ua/.

Більше інформації про шахрайство під час онлайн-покупок — на сайті #ШахрайГудбай: https://promo.bank.gov.ua/stopfraud/#section-23.

#ШахрайГудбай

Отримали повідомлення в інстаграмі з попередженням про блокування акаунту нібито за порушення? Не поспішайте діяти — це можуть бути шахраї.

Як працює шахрайська схема?

Зловмисники надсилають повідомлення від імені служби підтримки та лякають блокуванням сторінки. Щоб уникнути блокування, пропонують:

- перейти за посиланням;
- ввести логін і пароль від сторінки в інстаграмі.

Насправді посилання веде на фішингову сторінку. Після введення логіна та пароля дані одразу потрапляють до шахраїв. Вони змінюють налаштування облікового запису, а власник втрачає до нього доступ. Далі шахраї можуть вимагати гроші за повернення доступу до акаунту або розсилати шахрайські повідомлення від імені власника сторінки.

Як себе захистити?

Варто пам'ятати: справжня служба підтримки інстаграму **не надсилає приватні повідомлення або на електронну пошту**. Уся офіційна інформація приходить **тільки як сповіщення в додаток**.

- Не переходьте за посиланнями з таких повідомлень.
- Не вводьте логін і пароль на сторонніх сайтах.
- Увімкніть двофакторну автентифікацію.

Якщо ви вже перейшли за посиланням або ввели дані, то негайно змініть пароль!

У разі шахрайства повідомте про інцидент кіберполіцію через форму на сайті: https://ticket.cyberpolice.gov.ua/.

Більше інформації про шахрайство — на сайті #ШахрайГудбай: https://promo.bank.gov.ua/stopfraud/.

#ШахрайГудбай

Більшість інвестиційних шахрайств починаються з психологічної маніпуляції.

Зловмисники знають, як переконати людей інвестувати гроші. Для цього вони застосовують методи соціальної інженерії — психологічні прийоми, які допомагають схиляти людей добровільно передати свої гроші, розкрити конфіденційні дані або виконати інші дії.

Соціальна інженерія — це маніпуляції довірою, емоціями та рішеннями людини. Саме такі методи дають змогу шахраям вмовляти людей інвестувати гроші в сумнівні або повністю фейкові проєкти.

За даними Національного банку України, соціальна інженерія залишається одним із найпоширеніших методів шахрайства з платіжними картками. Інвестиційні схеми — не виняток.

Щоб переконати людей вкладати гроші, зловмисники можуть:

• демонструвати фейкові "успішні історії" інвесторів;
• використовувати підроблені або куплені відгуки;
• створювати відчуття терміновості: "інвестувати потрібно сьогодні";
• поступово збільшувати суми вкладень;
• знецінювати сумніви людини;
• телефонувати багато разів і тиснути психологічно.

У зображеннях до цієї публікації ми зібрали найпоширеніші методи психологічного впливу, які використовують інвестиційні шахраї.

Збережіть цю інформацію, щоб не потрапити в пастку шахраїв.

Більше інформації про шахрайство під маскою інвестицій — на сайті #ШахрайГудбай: https://promo.bank.gov.ua/stopfraud/

Один коментар – і шахраї вже можуть писати у директ.

Шахраї відстежують коментарі під публікаціями в соцмережах та підписки на тематичні сторінки, щоб знайти довірливих людей і виманити гроші нібито за “офіційні послуги”. Достатньо одного запитання, коментаря чи пошуку поради в соцмережах — і вас уже “взяли в роботу”.

Як це працює? Зловмисники:

• моніторять сторінки сервісних центрів МВС;
• читають коментарі користувачів;
• відстежують нових підписників.

Після цього – пишуть у приватні повідомлення з “вигідною пропозицією”:

- отримати посвідчення водія без складання іспитів;
- “вирішити питання” щодо відновлення водійського посвідчення після позбавлення права керування;
- оформити документи “швидко й офіційно”.

Насправді це шахрайство.

Чому це спрацьовує?

Шахраї переконують, що мають “зв’язки” у сервісному центрі МВС або навіть “працюють там”. Обіцяють зробити все швидко і “без проблем”, усього лише за певну суму, а головне – запевняють, що документ буде “офіційний” – відображатиметься в реєстрах, в застосунку “Дія” та Кабінеті водія.

Щоб здаватися переконливими, шахраї:

• використовують логотипи та надсилають фото “працівників сервісних центрів МВС”;

• імітують офіційну комунікацію.

Як не потрапити на гачок? Запам’ятайте прості правила:

Адміністратори сервісних центрів МВС не пишуть у месенджерах.

Оплата послуг здійснюється тільки на офіційний рахунок, а не на приватні картки.

Перевіряйте сайти, на яких уводите свої дані та отримуєте інформацію про послуги.

Офіційні сайти мають домен gov.ua. Адреса сайту Головного сервісного центру МВС – https://hsc.gov.ua.

“Приваблива пропозиція” = ризик. Ви можете залишитися без грошей і без документів. **Важливо:** за виготовлення та використання підроблених документів передбачена кримінальна відповідальність. Користуйтеся тільки офіційними ресурсами в отриманні державних послуг.

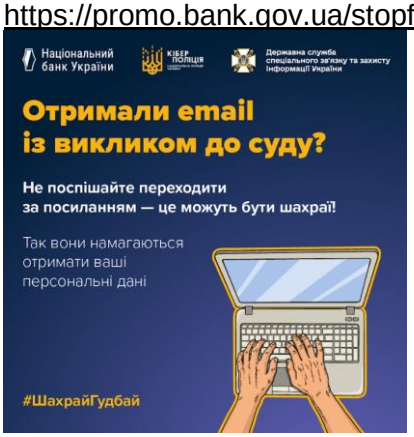
Якщо бачите підозрілу сторінку або чат:

• не платіть та не передавайте свої дані;

• повідомте кіберполіцію через форму на сайті: https://ticket.cyberpolice.gov.ua/.

Консультацію щодо послуг сервісних центрів МВС можна отримати за телефоном (044) 290-19-88.

Більше інформації про шахрайство – на сайті #ШахрайГудбай: https://promo.bank.gov.ua/stopfraud/.



Шахраї розсилають електронні листи нібито від імені судових органів із повідомленням про виклик на судове засідання у кримінальному провадженні. Такі листи виглядають офіційно та можуть викликати тривогу — саме на це й розраховують зловмисники.

Що пропонують у таких листах?

• Перейти за посиланням, яке веде на фішинговий сайт.

• Завантажити файл або встановити спеціальне програмне забезпечення.

Мета шахраїв:

- отримати доступ до персональних даних та викрасти гроші з рахунків;
- встановити шкідливе програмне забезпечення.

У разі отримання такого листа:

- НЕ можна переходити за посиланнями;
- НЕ можна завантажувати файли або встановлювати будь-які програми;
- НЕ можна відповідати на лист або контактувати з відправником.

Що робити?

- Ігноруйте такі повідомлення.
- Видаліть лист одразу після отримання.
- Перевіряйте інформацію лише через офіційні джерела.

Пам’ятайте: справжній виклик до суду надходить у формі судової повістки через офіційні канали комунікацій: рекомендованим листом, через електронний кабінет підсистеми «Електронний суд» Єдиної судової інформаційно-телекомунікаційної системи для

зареєстрованих користувачів або в SMS-повідомленні від адресанта з коротким ім'ям **SUDPOVISTKA**.

Завжди будьте уважні та перевіряйте інформацію перед тим, як діяти, — це найкращий спосіб захистити себе.

Якщо Ви стали жертвою шахрайства, то повідомте кіберполіцію через форму на сайті: https://ticket.cyberpolice.gov.ua/.

Більше інформації про шахрайство — на сайті #ШахрайГудбай: https://promo.bank.gov.ua/stopfraud/.

#ШахрайГудбай

Телефонне шахрайство залишається одним із найпоширеніших способів виманювання персональних даних та викрадення грошей. Шахраї можуть представитися будь-ким: працівниками банку, мобільного оператора, державної установи тощо. Під час телефонних розмов вони вміло маніпулюють довірою змушуючи людей самостійно розкривати конфіденційні дані.

Зокрема, поширеною є схема, коли шахраї телефонують від імені відомих магазинів і розігрують один із типових сценаріїв:

1) **“Вигідна акція”.** Кажуть, що залишився останній товар або діє велика знижка тільки для вас.

2) **“Ви виграли техніку”.** Повідомляють про виграш смартфона чи іншої техніки. Але потрібно оплатити доставку або податок.

3) **“На вас оформили кредит”.** Лякають, що на вас оформляють розстрочку або кредит. Потім допомагають скасувати оформлення і, наприклад, просять назвати коди з SMS.

На що слід звернути увагу?

- Поспіх і тиск: “тільки сьогодні”, “терміново”.
- Неочікувані виграші або надто вигідні пропозиції.
- Розмова зводиться до питань про дані платіжної картки. Просять назвати CVV-код, PIN-код від платіжної картки або SMS-код

Як себе захистити

1. Не повідомляйте конфіденційних даних та не переходьте за підозрілими посиланнями.
2. Завершіть розмову. Інформацію про акції перевірте на офіційному сайті магазину.

Стали жертвою шахраїв? Повідомте кіберполіцію через форму на сайті: https://ticket.cyberpolice.gov.ua/.

Більше інформації про шахрайство — на сайті #ШахрайГудбай: https://promo.bank.gov.ua/stopfraud/.

#ШахрайГудбай

Одним із поширених шахрайств щодо водіїв є пропозиції купити сертифікат відповідності на транспортний засіб за заниженою ціною.

Це важливий документ, який є обов'язковим під час першої державної реєстрації авто (у тому числі ввезеного з-за кордону), а також у разі його переобладнання. Саме тому такі "вигідні пропозиції" виглядають дуже привабливо – обіцяють усе зробити швидко, онлайн і без зайвого клопоту.

Як працює схема?

Шахраї створюють ілюзію "вигідної угоди". Наприклад:

• розміщують оголошення про продаж авто за привабливою ціною;

• додають нібито "готовий пакет документів" для реєстрації в сервісному центрі МВС;

• переконують, що все вже оформлено і не потребує додаткових дій.

Також вони можуть:

• пропонувати "допомогу" з оформленням документів для авто, ввезених із-за кордону;

• обіцяти швидке виготовлення сертифіката відповідності онлайн;

• запевняти, що процес максимально простий і "офіційний".

Насправді виданий зловмисниками "документ" недійсний, шахраї отримують гроші за послугу, а потім зникають.

Завжди звертайтеся до офіційних органів, які займаються сертифікацією транспортних засобів.

Як розпізнати шахраїв? Зверніть увагу на ці ознаки:

• **"Все онлайн і без візитів".** Обіцяють оформити документи повністю дистанційно – без відвідування офіційних установ і перевірок.

• **"Вигідна ціна".** Сертифікат пропонують значно дешевше, ніж в офіційних установах, створюючи ілюзію вигідної угоди.

• **Відсутність перевірок.** Запевняють, що жодних процедур проходити не потрібно – достатньо просто подати документи онлайн.

• **Оплата на картку.** Просять переказати кошти на особисту банківську картку.

Сертифікат відповідності підтверджує, що транспортний засіб відповідає встановленим вимогам (ДСТУ, технічним регламентам або умовам). Його можуть видавати:

• виробник або його офіційний представник – для нових авто;

• уповноважені органи сертифікації або визначені Міністерством розвитку громад та територій України органи із сертифікації, акредитовані відповідно до законодавства, – для авто, що були у користуванні. Перелік таких органів є за посиланням: https://mindev.gov.ua/diialnist/tekhnichne-rehuliuvannia-na-transporti/vykonannia-zhenevskoi-uhody-1958-roku/perelik-pryznachenykh-orhaniv-iz-sertyfikatsii-kolisnykh-transportnykh-zasobiv – за їхніми контактами можна перевірити чинність сертифіката, його серію, номер і відповідність конкретному авто.

Про можливі шахрайські дії можна повідомити Кіберполіцію через форму на сайті: https://ticket.cyberpolice.gov.ua/

Більше інформації про шахрайство – на сайті #ШахрайГудбай: https://promo.bank.gov.ua/stopfraud/.

#ШахрайГудбай

Шахраї намагаються виманити гроші у громадян, пропонуючи вигідно інвестувати кошти та отримувати пасивний дохід. Для цього зловмисники активно шукають потенційних жертв в інтернеті та використовують різні канали комунікації. Найчастіше це:

• реклама в соціальних мережах;
• телеграм-канали та боти;
• телефонні дзвінки;
• фейкові сторінки псевдоекспертів;
• e-mail або смс-розсилання.

Іноді люди самі знаходять такі платформи. Це часто відбувається, коли користувачі шукають у мережі інформацію про криптовалюти, трейдинг або пасивний дохід. Алгоритми соціальних мереж починають показувати дедалі більше подібної реклами – у результаті людина може потрапити на шахрайський ресурс.

Як уберегтися від шахраїв?

Щоб зменшити ризик втрати грошей, варто дотримуватися кількох базових правил фінансової безпеки:

- перевіряти інформацію про компанію з офіційних джерел;
- критично ставитися до обіцянок швидкого або гарантованого доходу;
- не здійснювати перекази коштів на вимогу невідомих осіб;
- не встановлювати програми віддаленого доступу на свій пристрій за порадою "менеджерів" або "інвестиційних консультантів";
- у разі сумнівів утриматися від будь-яких фінансових операцій;
- перед тим, як інвестувати кошти, ознайомтеся зі списком сумнівних інвестиційних проєктів на сайті Національної комісії з цінних паперів та фондового ринку: https://cutt.ly/rtS7r2Fe;
- у разі виявлення ознак інвестиційного шахрайства повідомляти про це правоохоронні органи. Зокрема, можна подати електронне звернення до кіберполіції: https://ticket.cyberpolice.gov.ua.

Більше інформації про шахрайство під маскою інвестицій — на сайті #ШахрайГудбай: https://promo.bank.gov.ua/stopfraud/.

У соціальних мережах поширюються повідомлення про нібито грошові виплати за тривалі відключення електроенергії. Користувачам пропонують перейти за посиланням і оформити заявку на отримання компенсації. Важливо розуміти – це чергова шахрайська маніпуляція з метою заволодіння коштами довірливих громадян.

Що відбувається, якщо перейти за запропонованим посиланням? Таке посилання як правило веде на фішинговий сайт, створений для викрадення персональних і банківських даних. На підробленому сайті вас попросять ввести конфіденційну інформацію:

- логін і пароль до інтернет-банкінгу;
- номер платіжної картки та термін її дії;
- CVV-код і навіть PIN-код;
- номер телефону та дату народження.

Отримавши ці дані, шахраї зможуть отримати доступ до вашого інтернет-банкінгу зі свого пристрою та викрасти ваші кошти.

Як не потрапити в пастку?

- Не переходьте за підозрілими посиланнями з повідомлень.
- Завжди перевіряйте інформацію через офіційні джерела.
- Нікому не повідомляйте логін і пароль до банкінгу, PIN-код від платіжної картки та CVV-код.

Якщо Ви стали жертвою шахрайства, то повідомте кіберполіцію через форму на сайті: https://ticket.cyberpolice.gov.ua/.

Більше інформації про шахрайство — на сайті #ШахрайГудбай: https://promo.bank.gov.ua/stopfraud/.

#ШахрайГудбай