0_Публікація про старт кампанії та знайомство з героями кампанії

30 травня стартувала Всеукраїнська інформаційна кампанія з платіжної безпеки #КібербезпекаФінансів, організаторами якої є Національний банк та Держспецзв'язку. Її мета – поліпшити обізнаність громадян про платіжну безпеку та сформувати навички із захисту фінансових даних у віртуальному просторі.

Головними героями кампанії стали #КіберКіт та #КіберПес, які будуть розповідати населенню про правила платіжної безпеки.

Під час кампанії ви дізнаєтесь:

- як захистити свої облікові записи, комп'ютери, смартфони та інші пристрої від зламу;
- як створювати складні та унікальні паролі;
- як налаштовувати багатофакторну автентифікацію;
- як перевіряти сайти, на яких ви вводите свої платіжні дані, мобільні застосунки та інші програми перед завантаженням;
- як правильно використовувати публічні й домашні Wi-Fi-мережі;
- як дбати про програмне забезпечення на власних пристроях
- про інші правила безпечної поведінки у віртуальному просторі.

Кампанія триватиме до 30 вересня 2024 року у всіх регіонах України.

Більше інформації про платіжну безпеку та правила кібергігієни читайте на сайті НБУ та Держспецзв'язку #КібербезпекаФінансів: https://promo.bank.gov.ua/payment-security/

Інформаційна кампанія проходитиме за підтримки Проєкту USAID "Інвестиції для стійкості бізнесу".

#КібербезпекаФінансів
#КіберПес
#КіберКіт

Плакат 1

Як захистити від зламу сторінки в соціальних мережах і месенджерах та електронну пошту?

#КіберПес радить встановлювати багатофакторну автентифікацію або двоетапну перевірку. Ця функція безпеки допомагає додатково захистити ваш акаунт від шахраїв.

Як це працює?

Під час налаштування такої функції для входу до вашого акаунту, крім логіна та пароля, потрібно зазначити електронний ключ або код підтвердження, що повинен надійти на смартфон, електронну скриньку або у відповідний додаток.

Це слід робити в тих випадках, коли вхід до вашого акаунту здійснюватиметься з невідомого браузера або мобільного пристрою.

Як багатофакторна автентифікація захищає від шахраїв?

Навіть якщо шахрай дізнався ваш пароль, він все ще не зможе отримати доступ до вашого облікового запису без додаткового підтвердження.

Шукайте таку функцію в налаштуваннях або переходьте за посиланнями та налаштовуйте багатофакторну автентифікацію до своїх акаунтів:

- **Facebook:** https://cutt.ly/Tw760pHg;
- **Instagram:** https://cutt.ly/nw760WRw;
- **Telegram:** https://cutt.ly/tw760DzB;
- **Signal:** https://cutt.ly/Kw760My3;
- **Google:** https://cutt.ly/Tw762gAh;
- **WhatsApp:** https://cutt.ly/Vw50ZCdq;
- **Viber:** https://cutt.ly/Vw762SHN**.**

Більше про багатофакторну автентифікацію та способи її налаштування читайте на сайті НБУ та Держспецзв'язку #КібербезпекаФінансів: https://promo.bank.gov.ua/payment-security/

#КіберПес

Плакат 2

Чому не можна використовувати паролі, які містять особисту інформацію та вподобання?

Такі паролі шахраї можуть легко відгадати та отримати доступ до ваших акаунтів, наприклад, до сторінок у соцмережах, месенджерах, електронної пошти, інтернет-банкінгу тощо.

Як шахраї можуть скористатися вашим акаунтом?

- Викрасти гроші з рахунків.
- Просити в борг у соцмережах у друзів від вашого імені.
- Поширювати з вашого акаунту шахрайські посилання та файли.
- Погрожувати видаленням важливої інформації чи її використання та вимагати викуп.

#КіберПес радить не використовувати паролі, які містять особисту інформацію та вподобання, а саме:

- дату народження;
- прізвище, ім'я, адресу;
- номер телефону;
- дівоче прізвище;
- ім'я вашого домашнього улюбленця;
- ваші хоббі та вподобання, наприклад, улюблену марку авто, назву улюбленої книги тощо. Адже цією інформацію ми могли раніше ділитися в соцмережах, а отже, її можна легко дізнатися.

Якщо у вас є такі паролі, негайно замініть їх на надійніші.

Також забудьте про типові комбінації паролів, наприклад: Qwerty12, Password123456, Admin1234 тощо.

Не полегшуйте життя шахраям, використовуйте надійні паролі!

Більше про надійні паролі та захист акаунтів читайте на сайті НБУ та Держспецзв'язку #КібербезпекаФінансів: https://promo.bank.gov.ua/payment-security/

#КіберПес

Плакат 3

Шахраї можуть використовувати будь-які ситуації у своїх інтересах. Проблеми з енергопостачанням в Україні не є винятком. Через масовані ворожі атаки на енергосистему країни виникає дефіцит потужності, що призводить до обмеження постачання електроенергії. Українцям важливо стежити за графіками відключень, щоб організувати свій побут у таких умовах. Однак, потрібно бути уважними й обережними під час моніторингу ситуації щодо відключень електроенергії, адже зловмисники можуть використовувати цю ситуацію, створюючи фейкові онлайн-ресурси, наприклад, створювати телеграм-боти від імені енергетичної компанії для поширення дезінформації, викрадення конфіденційних даних та шахрайства.

Важливо! Отримуйте інформацію про відключення світла тільки з офіційних джерел!

Щоб дізнатися про графіки планових відключень у своєму регіоні та списки постачальників електроенергії, скористайтеся офіційним сайтом Міністерства енергетики України за посиланням: https://mev.gov.ua/storinka/ye-svitlo, на якому також доступні контакти постачальників електроенергії в розрізі областей: https://mev.gov.ua/storinka/kontakty-postachalnykiv.

Більше інформації, а також посилання на сайти операторів розподільчих мереж можна знайти на сайті Кіберполіції: https://cutt.ly/NetNt5h7.

Будьте обачними! Не переходьте за посиланнями з незнайомих джерел та не довіряйте стороннім ресурсам.

Більше про те, як захистити себе та свої дані від шахраїв читайте на сайті НБУ та Держспецзв'язку #КібербезпекаФінансів: https://promo.bank.gov.ua/payment-security/

#КіберПес

Плакат 4

Як придумати надійний пароль, який запам'ятати просто, вгадати неможливо?

Використовуйте для створення паролів фрази. Це можуть бути цитати, рядки з віршів, пісень, ваші потаємні мрії, плани, важливі для вас думки тощо.

Нижче приклади створення комбінацій паролів з використанням фраз.

Варіант 1. Використовувати перші літери кожного слова знайомої фрази як основу комбінації для пароля. Наприклад, якщо з фрази "КіберПес любить гризти мамині капці та одяг!" обрати перші літери слів і додати спеціальні символи та цифри вийде така комбінація: Kplgmkto!#24.

Варіант 2. Використовувати всю фразу як пароль.

Наприклад, якщо за основу для пароля взяти афоризм Лесі Українки “Без надії сподіваюсь”, може вийти така комбінація: BezNadiiSpodivaius, до якої необхідно також додати спеціальні символи та цифри.

Варіант 3. Поєднувати перші склади чи частини кількох слів фрази.

Наприклад, якщо з афоризму Григорія Сковороди “Бери вершину і матимеш середину” взяти перші склади слів та додати спеціальні символи та цифри, вийде такий пароль: BeVerMaSer24!#.

Як додавати цифри та спеціальні символи до паролів, щоб їх також легко було запам’ятати?

Змінювати деякі літери фрази, яку ви використовуєте для створення пароля, на спеціальні символи та цифри за тільки вам відомою схемою. Наприклад, літеру “о” замінювати на знак “%” тощо.

Це лише кілька прикладів, як створити та легко запам’ятати надійний пароль!

Ви також можете використовувати власні способи створення паролів, головне, щоб їх не змогли відгадати шахраї.

Більше про правила створення та зберігання паролів та платіжну безпеку читайте на сайті НБУ та Держспецзв’язку #КібербезпекаФінансів: https://promo.bank.gov.ua/payment-security/

#КіберПес

Плакат 5

#КіберПес застерігає! Шахраї можуть перехоплювати дані банківських карток, паролі, повідомлення та інші конфіденційні дані під час використання загальнодоступних мереж Wi- Fi!

Це мережі, до яких можуть підключатися різні користувачі без необхідності вводити пароль або ідентифікувати себе. Такі мережі зазвичай доступні в громадських місцях, наприклад, у кафе, готелях, аеропортах, торгових центрах, бібліотеках тощо.

Як шахраям це вдається?

Загальнодоступні мережі Wi-Fi не захищені належним чином, тому зловмисники, перебуваючи в одній мережі з іншими користувачами, можуть перехоплювати дані банківських карток, паролі, повідомлення та інші конфіденційні дані.

Метою зловмисників зазвичай є здійснення кібератак, зламу акаунтів, викрадення коштів на рахунках тощо.

Щоб убезпечити свої дані, дотримуйтеся таких порад:

- **користуйтеся мобільним інтернетом від вашого оператора** (Hotspot), краще не підключатися до загальнодоступної мережі Wi-Fi;
- **не здійснюйте банківські операції** під час підключення до загальнодоступної мережі Wi-Fi;

- **не використовуйте мережі Wi-Fi, що просять авторизуватися за номером телефону,** адресою електронної пошти або через соціальні мережі, адже в такий спосіб ви надаєте більше особистої інформації і цим можуть скористатися зловмисники;
- **вимкніть опцію автоматичного підключення** до загальнодоступних мереж Wi-Fi;
- **використовуйте VPN-сервіси** під час підключення до загальнодоступних мереж Wi-Fi.

Який VPN-сервіс обрати та більше порад про платіжну безпеку читайте на сайті НБУ та Держспецзв'язку #КібербезпекаФінансів: https://promo.bank.gov.ua/payment-security/

#КіберПес

Плакат 6

Більше половини шахрайських сайтів походять з рф, не дайте ворогу себе ошукати, перевіряйте сайти, на яких вводите свої дані!

Удвічі уважніше перевіряйте сайти, на яких просять зазначити інформацію про платіжні картки, логіни та паролі від інтернет-банкінгу, соціальних мереж тощо.

Шахраї можуть створювати сайти, схожі на сайти державних, банківських установ, міжнародних організацій, благодійний фондів, онлайн-магазинів тощо.

Щоб уникнути шахрайства:

- **перевірте адресу** потрібного ресурсу, адже будь-які відмінності можуть свідчити про те, що ви опинилися на фішинговому сайті;

Звертайте увагу на протокол сайту:

- ✔ http – це ненадійний протокол, це означає, що сайтом користуватися не можна;
- ✔ https – потрібно продовжити перевірку сайту;

- якщо потрібно перейти на сайт організації, адресу якого ви отримали в посиланні, краще введіть у пошуковій системі назву необхідного сайту і лише тоді переходьте на вебресурс;
- **перевіряйте інформацію з офіційних джерел.**

Більше про платіжну безпеку в інтернеті та ознаки шахрайських сайтів читайте на сайті НБУ та Держспецзв'язку #КібербезпекаФінансів: https://promo.bank.gov.ua/payment-security/

#КіберКіт

Плакат 7

Використовуйте різні паролі. Однакові паролі – це те саме, що мати один ключ до будинку, автомобіля, сейфа. Якщо зловмисники отримають доступ до цього пароля, вони зможуть отримати доступ до всіх облікових записів, де він використовується.

Щоб убезпечити свої особисті дані та кошти на рахунках, потрібно:

- **створювати унікальний пароль** для кожного інтернет-банкінгу, електронної пошти, соціальних мереж тощо;
- **створювати паролі, які істотно відрізняються від попередніх,** що використовувалися на цьому ж сервісі чи пристрої;

● **регулярно змінювати паролі** (кожні 3–6 місяців або тоді, коли система попросить вас це зробити). Для дуже важливих облікових записів їх рекомендується змінювати частіше;

● **уникати типових комбінацій паролів, наприклад:** Qwerty12, Password123456, Admin1234 тощо;

● **не використовувати** особисті дані та послідовне / зворотне написання символів або цифр для створення паролів;

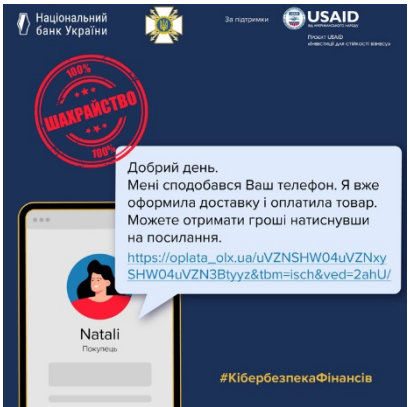
● **створювати складні паролі,** що можуть містити не менше 12 символів, великі та малі літери, цифри та спеціальні знаки / символи.

Більше про надійні паролі та захист акаунтів читайте на сайті НБУ та Держспецзв'язку #КібербезпекаФінансів: https://promo.bank.gov.ua/payment-security/

#КіберПес

Плакат 8

Додаткові плакати до основного



83% випадків шахрайства з платіжними картками в минулому році відбувалося через мережу Інтернет.

Шахраї з метою отримання інформації про паролі, платіжні картки, рахунки та інші персональні дані створюють шахрайські сайти та поширюють посилання на них в інтернеті.

Як вберегтися від подібного шахрайства?

Не переходьте за посиланнями від незнайомців! Перевіряйте інформацію через офіційні джерела, не поспішайте клікати на посилання, які ви побачили десь у соцмережах, у груповому чаті, в телеграм-каналі тощо. Особливо, якщо йдеться про будь-які грошові виплати, акції, розіграші, легкі види підробітку, важливі новини чи повідомлення від державних установ, банків, міжнародних організацій. Краще знайдіть у пошуку офіційний сайт відповідної установи і ознайомтеся з відповідною новиною там.

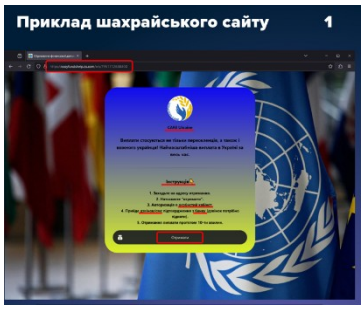
Не поспішайте клікати на посилання, які ви отримуєте від друзів. Є випадки, коли шахраї зламують сторінки в соцмережах, месенджерах, електронної пошти та від імені власника акаунту поширюють шахрайські посилання серед підписників та друзів. Адже люди довіряють більше інформації, яку отримують від знайомих. Приклад шахрайського повідомлення від імені друзів: “Подивися, чи це ти на відео?”

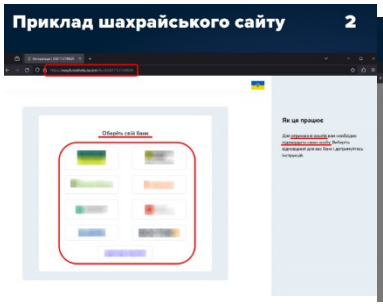
Щоб уникнути шахрайства, запитайте в знайомого для чого він надіслав посилання або краще зателефонуйте йому та запитайте, чи справді посилання від нього.

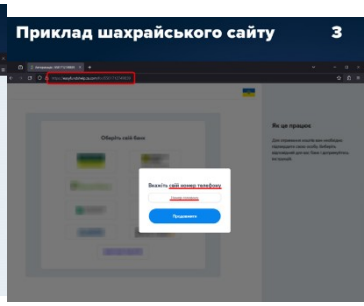
Більше про ознаки шахрайських сайтів та платіжну безпеку читайте на сайті НБУ та Держспецзв’язку #КібербезпекаФінансів: https://promo.bank.gov.ua/payment-security/

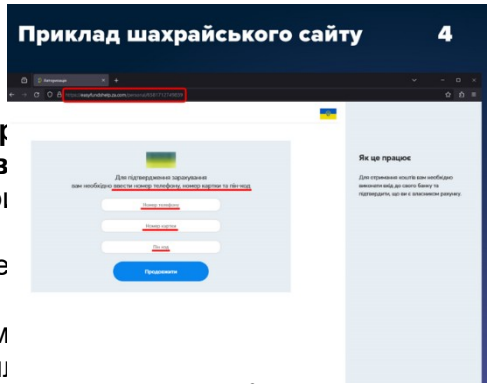
#КіберПес

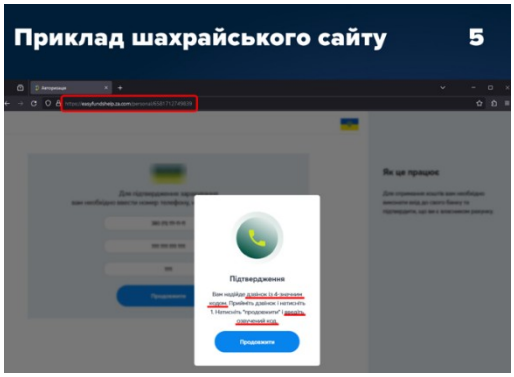
Плакат 9 (текст до плакату буде в одному стилі)











пр
складно відрізнити їх в

Розглянемо пр
пропозицією оформити
ресурсу, який був створе

Через соціальні
поширили повідом
отримання грошової вип

Повідомлення містило активне посилання на фішингову сторінку-приманку, яка була стилізована з використанням айдентики благодійної організації. На цій сторінці шахраї розмістили інструкції щодо проходження ідентифікації, а також активні посилання на шахрайські фішингові ресурси, які маскувалися під сторінки авторизації банків.

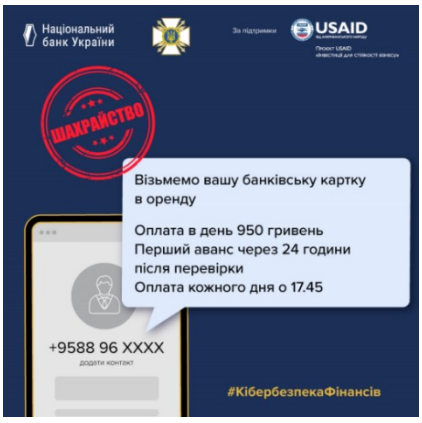
Щоб оформити грошову виплату, шахрайський ресурс пропонував ввести номер мобільного телефону, пароль від особистого кабінету, номер картки, CVV, пін-код та поточний баланс картки для підтвердження входу в особистий кабінет. Отримані дані шахраї використовували для “прив'язки” акаунта користувача до нового пристрою або для онлайн авторизації на порталі відповідного банку, що давало їм змогу вивести кошти з рахунку жертви.

Подібні схеми шахрайства є дуже поширеними.

Перевіряйте будь-яку інформацію про грошові виплати, яку побачили в інтернеті чи в повідомленнях через офіційні джерела. Не переходьте за посиланням, зазначеним у таких повідомленнях. Перейдіть на офіційний сайт відповідної організації, від імені якої пропонується грошова допомога через пошукову систему, ввівши назву необхідного сайту.

Більше про ознаки шахрайських сайтів та платіжну безпеку читайте на сайті НБУ та Держспецзв’язку #КібербезпекаФінансів: https://promo.bank.gov.ua/payment-security/

Плакат 10



Протягом останнього часу в соціальних мережах з’являються оголошення з пропозицією здати банківську картку в оренду. За це обіцяють непогану плату (приблизно 1000 гривень на добу), більше нічого робити не потрібно. Також можуть траплятися оголошення з пропозицією легкої роботи, де “роботодавець” відразу просить номер картки для зарахування “зарплати”, або з пропозицією відкрити банківський рахунок на своє ім’я для отримання та переказу коштів від імені іншої особи. Але чи все так просто як здається? Давайте з’ясуємо.

Найперше важливо розуміти, що за кожною такою пропозицією ховається небезпечна шахрайська схема!

Ви щось знаєте про грошових мулів?

Грошові мули або дропи – це особи, які дають змогу третій особі (шахраю) за фінансову винагороду використовувати свій банківський рахунок для проведення операцій з коштами незаконного походження.

Як вони це роблять?

Дропи перераховують незаконно отримані кошти через різні банківські рахунки, використовуючи свої платіжні картки. Це робиться для того, щоб ускладнити роботу слідства. Такий процес дає змогу злочинним групам працювати в різних країнах, залишаючись у тіні.

Що це за гроші?

Це кошти, які були отримані незаконним шляхом: через торгівлю наркотиками, людьми, тероризм, фішинг та інші тяжкі злочини. Також банківські картки можуть бути використані для проведення фінансових операцій, пов'язаних зі здійсненням незаконної діяльності, наприклад, для роботи онлайн-казино, що не мають ліцензії, ухилення від сплати податків тощо.

Чи усвідомлює дроп, що він став частиною злочинного ланцюжка?

Найімовірніше ні, оскільки ніхто йому про це не скаже. А якщо він і поцікавиться, то шахраї завжди розкажуть якусь красиву та правдоподібну легенду.

У чому полягає головна небезпека?

Грошовий мул – це співучасник злочину, нижча ланка злочинної схеми, яку правоохоронці знаходять найшвидше. Участь у таких схемах може мати серйозні наслідки: штрафи, конфіскацію майна і навіть позбавлення волі.

Як вберегти себе?

- ✔ Будьте обережні з пропозиціями щодо легкого заробітку.
- ✔ Уникайте підозрілих пропозицій і не погоджуйтеся брати участь у сумнівних схемах.

Зрозуміли що стали дропом? Що робити?

- ✔ Погодилися на роботу, але через деякий час зрозуміли що стали дропом? Негайно зверніться до кіберполіції, подавши заяву на їхньому сайті.
- ✔ Встигли попрацювати дропом? Припиніть співпрацю з таким "роботодавцем" і зверніться до кіберполіції, а також до банку, рахунок в якому використовувався для відмивання коштів.

Більше про те, як захистити себе та свої дані від шахраїв читайте на сайті НБУ та Держспецзв'язку #КібербезпекаФінансів: https://promo.bank.gov.ua/payment-security/

#КіберКіт

Плакат 11

Чи знали ви, що через недостатньо захищену домашню мережу Wi-Fi до вас можуть завітати непрохані кібергості?

І тут, звісно, мова не про сусідів, які можуть дивитися серіали або завантажувати музику, використовуючи ваш Інтернет. Тут все набагато складніше.

Незахищена домашня мережа Wi-Fi може створити ризик незаконного доступу зловмисників, які можуть викрасти ваші особисті дані, такі як паролі, особисті ключі для створення електронного підпису, дані про картки та рахунки тощо.

Що ж робити, щоб захистити домашню мережу Wi-Fi?

#КіберПес радить:

- обирайте роутер зі стійкими протоколами безпеки. Важливо вибирати роутери з протоколами безпеки WPA3 або WPA2, оскільки WEP та WPA вважаються застарілими та менш безпечними;
- встановлюйте надійні логіни та паролі. Замість стандартних логінів та паролів від виробника створіть власні. Зробіть це до того, як підключати роутер до інтернету;
- налаштуйте списки доступу за визначеними атрибутами (наприклад, MAC-адреса);
- приховайте SSID – назву мережі Wi-Fi зі списку доступних мереж, щоб уникнути виявлення вашої мережі сторонніми користувачами;
- створіть окрему мережу Wi-Fi для гостей. Так, ваші гості зможуть підключатися до інтернету, але не знатимуть вашого основного пароля;
- зменшіть зону покриття роутера. Обмежте зону покриття Wi-Fi, щоб сигнал був доступний лише у вашому помешканні;
- вимкніть функцію WPS: Забезпечте додатковий захист, вимкнувши функцію WPS, що дає змогу підключати пристрої без введення пароля;
- постійно оновлюйте програмне забезпечення для роутера, налаштуйте автоматичні оновлення за можливості. Звертайтеся до сервісних центрів, якщо не можете встановити оновлення самостійно;
- не використовуйте застарілі моделі роутера. Зазвичай виробники на своїх сайтах публікують переліки застарілих моделей, які не підтримують оновлення безпеки.

Більше інформації про налаштування домашньої та про особливості використання загальнодоступної мережі Wi-Fi читайте на сайті НБУ та Держспецзв'язку #КібербезпекаФінансів: https://promo.bank.gov.ua/payment-security/.

#КіберПес

Плакат 12

Шахраї пропонують роботу та виманюють гроші!

Згідно з даними кіберполіції шахраї надсилають у месенджерах повідомлення з пропозиціями легкого заробітку. Схема полягає в нібито популяризації товарів на відомому маркетплейсі. Люди повинні купити певний товар і потім продати його на іншому сайті (сайті шахраїв).

Всі, хто погодився на таку «роботу», отримували завдання від злочинців, за виконання яких зловмисники обіцяли платити гроші.

На перших етапах українці дійсно могли отримувати невеликі виплати на свої банківські картки. Таким чином, їх залучали до злочинної схеми. Далі шахраї вимагали зареєструватися на їх сайті і здійснювати купівлю-продаж товарів за інструкціями «менеджерів».

Щоб купити товар, українці мали поповнювати свій баланс в особистому кабінеті, перераховуючи власні кошти на зазначені злочинцями банківські картки.

Для виведення коштів зловмисники вимагали повторних перерахувань коштів на їх банківські картки. Такий алгоритм продовжувався доти, доки жертви не розуміли, що мають справу з шахраями.

Як уникнути шахрайства?

- Не намагайтеся отримати гроші від зловмисників навіть на перших етапах, і якщо ви обізнані про таку «схему». Будь-яке спілкування з ними – це ризик втратити кошти.
- Не переходьте за сумнівними посиланнями!
- Перевіряйте сайти, на яких вводите свої платіжні дані!

Якщо ви випадково розкрили дані своєї платіжної картки, інтернет-банкінгу на підозрілому сайті, негайно телефонуйте до банку за номером, зазначеним на звороті картки. Вимагайте блокування коштів на рахунку, а у випадку несанкціонованого списання коштів – блокування трансакцій та надайте звернення до банку – отримувача коштів щодо їх блокування / повернення.

Якщо ви стали жертвою інтернет-шахрайства, негайно повідомте про це кіберполіцію.

Більше інформації про правила платіжної безпеки в інтернеті читайте на сайтах НБУ та Держспецзв'язку: https://promo.bank.gov.ua/payment-security/internet.html.

#КібербезпекаФінансів