ПАМ'ЯТКА

щодо здійснення безпечних операцій з використанням ЕПЗ, заходів щодо мінімізації ризиків, пов'язаних із виконанням платіжних операцій та рекомендації щодо виявлення фішингових ознак (шахрайства) при їх виконанні

Для мінімізації ризиків втрат збережень з рахунків по Вашій платіжній картці (далі – картка) від неправомірних дій та намірів шахраїв і забезпечення секретності реквізитів власних карток, необхідно дотримуватися наступного:

Дозволяється повідомляти для переказу грошей:

- ✓ 16-значний номер Вашої картки;

Дозволяється повідомляти оператору контакт-центру при здійсненні вихідного дзвінка клієнтом Банку:

- ✓ П.І.Б. (за необхідності);
- ✓ Кодове слово для ідентифікації клієнта Банком / дівоче прізвище матері (оператор Контакт-центру може спитати його для проведення ідентифікації).

Не варто розголошувати третім особам реквізити та інші секретні дані Вашої картки:

- ✓ Термін дії картки;
- ✓ CVV2 / CVC2 (3-х значний код на звороті картки);
- ✓ PIN-код;
- ✓ 3D Secure (одноразовий короткостроковий пароль для підтвердження транзакції);
- ✓ не перетелефоновувати на ті номери, які тим чи іншим способом надійшли Вам через SMS-повідомлення чи в інших месенджерах нібито від імені Банку із використанням подібного альфа-імені у стрічці з назвою контакту.

АТ «БАНК «ПОРТАЛ» може надсилати **SMS-повідомлення** виключно від власного зареєстрованого **альфа-імені «BANK PORTAL»** на фінансовий номер телефону клієнта, вказаний при укладанні з Банком договору банківського рахунку.

Для дистанційного обслуговування клієнтів Банку використовується Інтернет-банкінг **PORTAL.LINK** виключно з тієї URL-адреси, що міститься у цьому гіперпосиланні та через мобільний застосунок **PORTAL.LINK**, який можна завантажити з App Store та Play Market для зручного та безпечного використання власними фінансами.

Для безпечного здійснення онлайн-платежів, використовуючи систему дистанційного обслуговування різних Банків на території України та їх представництв на території інших країн, можна переглянути список їх на сторінці офіційного Інтернет-представництва Національного Банку України – список Банків та їх відокремлених підрозділів.

При підозрі щодо намірів та зловмисних дій шахраїв відносно конфіденційних (секретних) даних з Вашою карткою та протиправних дій зі сторони кіберзловмисників, необхідно відразу звернутися **до КОНТАКТ-ЦЕНТРУ** Банку для **блокування** Вашої картки оператором контакт-центру за вищевказаними контактами або звернувшись безпосередньо до працівників Банку для встановлення лімітів на здійснення будь-яких транзакцій по картці.

Окрім цього, можна долучитися до всебічної підтримки та самостійно повідомити про факти кіберзлочинів, кібершахрайства та інші кіберзагрози:

- ✓ до **Кіберполіції** *(про кіберзлочини, кібершахрайство тощо)*: callcenter@cyberpolice.gov.ua

- ✓ до **Урядової команди реагування на комп'ютерні надзвичайні події** *(про кібератаки, кіберінциденти, у тому числі фішингові розсилання на органи влади, бізнес та громадян)*:
  e-mail: incidents@cert.gov.ua, форма повідомлення на сайті: https://cert.gov.ua/contact-us або через сторінку у Facebook: https://www.facebook.com/UACERT
- ✓ до **Оперативного центру реагування на кіберінциденти** *(про кібератаки, кіберінциденти, у тому числі фішингові розсилання)*:
  e-mail: soc@scpc.gov.ua
  тел.: (044) 281-87-37
- ✓ до **Оперативно-технічної служби Державного центру кіберзахисту** *(про кібератаки, кіберінциденти, у тому числі фішингові розсилання на державні органи влади)*:
  тел.: (044) 281-88-01
- ✓ до **Департаменту кіберполіції Національної поліції України** *(про ресурси в Інтернеті, які розповсюджують дезінформацію)*:
  https://t.me/stopdrugsbot
- ✓ до **Ситуаційного центру забезпечення кібербезпеки СБУ** *(про загрозу нацбезпеці України в інтернеті, зокрема спроби та факти кіберрозвідки інших держав, кібертероризму та кібершпигунства)*:
  e-mail: incident@dis.gov.ua – про виявлені кіберінциденти на об'єктах критичної інфраструктури та в органах державної влади;
- ✓ e-mail: cvd@dis.gov.ua – про виявлені вразливості в інформаційно-телекомунікаційних системах на об'єктах критичної інфраструктури та в органах державної влади.
- ✓ до **Міністерства оборони України** *(про загрози для військової кібербезпеки України)*:
  тел.: 0 800 500 442.

Для більшої обізнаності можна ознайомитися із корисними посиланнями:

- ✓ Поради з фінансової та онлайн-безпеки від НБУ
- ✓ Сайт для перевірки чат-ботів (працює в тестовому режимі)
- ✓ Чат-бот Держспецзв'язку, в якому можна знайти відповіді на всі запитання щодо кібербезпеки, кіберзахисту, кіберзагроз тощо.

Рекомендуємо! Звернутися до мобільного оператора (віртуального мобільного оператора), якому Ви надаєте перевагу та користуєтесь його відповідними послугами, для відключення можливості віддаленого перевипуску SIM-картки (eSIM) для Вашого мобільного телефону, смартфону чи планшету.

Дізнатися про це та іншу необхідну інформацію можна зателефонувавши до контакт-центру Банку за номерами **0 800 50-24-50** або **+38 044 277-277-5**, які вказані на зворотній стороні кожної картки, виданої Банком.

Іншим корисним ресурсом для перевірки підозрілих сайтів є база шахрайських сайтів «BlackList EMA» та список надійних сервісів для онлайн платежів і онлайн кредитування у «Білому списку». Для Вашої цікавості та обізнаності там можна пограти в онлайн-гру «ZДОЛАЙ ШАХРАЯ», в якій симулюються різні види платіжного шахрайства: телефонне, банкоматне та кредитне шахрайство, угон SIM-картки, шахрайство на дошках оголошень, фішинг, вішинг, шкідливе програмне забезпечення, програми-вимагачі тощо.

Перед здійсненням будь-яких онлайн-транзакцій слід переконатися в тому, що відвідувана вебсторінка не відноситься до **фішингових** та на безпечне з'єднання з нею.

Перевірка адреси сайту

Перш за все необхідно перевірити URL-адресу сайту, щоб переконатися, що вона точно відповідає оригінальному сайту. Шахрайські вебсторінки зазвичай містять помилки в URL-адресі або використовують заміну літер.

Перевірка сертифікату безпеки

Наступним кроком це перевірка наявності сертифікату безпеки SSL на відвідуваному сайті. SSL/TLS-сертифікат — це технологія шифрування, яка забезпечує захищене з'єднання між вебсторінкою та користувачем. Це дозволяє захистити конфіденційні дані, такі як паролі, номери кредитних карток і інші особисті дані від зловмисних атак і протиправних дій.

При переході на сайт з SSL/TLS-сертифікатом, має бути наявний замок або інша індикація безпеки в адресному рядку браузера. Це означає, що таке з'єднання з вебсторінкою зашифроване та захищене, а користувач може передавати свої особисті дані без особливого ризику їх втрати чи крадіжки.

Ознаки **офіційного** та **безпечного** сайту:

- адреса сайту починається з https://… із наявним замочком ліворуч або іншої індикацію безпеки в адресному рядку браузера, що означає про те, що передача даних буде здійснюватися по захищеному каналу зв’язку та застосовується чинний SSL/TLS-сертифікат;
- сайт має бути зареєстрований на надійному домені, без використання конструкторів для створення сайтів, а в адресній стрічці мають відображатися різні адреси для різних сторінок сайту;
- відсутність помилок у структурі сайту, граматичних і синтаксичних помилок у його вмісті (контенту) чи сумнівного зовнішнього вигляду;
- легітимні сайти при введенні реквізитів платіжних карток у відповідні форми маскують їх зірочками або використовують віртуальну клавіатуру зі зміною її вигляду при введенні CVV2/CVC2 коду;

Шахрайські вебсторінки зазвичай існують короткий період часу та доволі часто після введення реквізитів картки відбувається збій операції або виникає невідома помилка.

Якщо немає SSL/TLS-сертифікату на вебсторінці, то краще не передавати особисті дані на цьому сайті, оскільки це може бути небезпечно.

Перевірка сертифікату домену

Якщо необхідно з’ясувати дату реєстрації домену, можна скористатися інструментами, такими як WHOIS відвідавши вебсторінку, яка надає цю інформацію, наприклад https://www.whois.com. Дата реєстрації вебсторінки може бути корисною інформацією для визначення періоду життєдіяльності вебсторінки та потенційних проблем з безпекою, оскільки тривалий час існування вебсторінки вказує на легітимність даного вебресурсу.

Перевірка електронних листів

Слід ретельно перевіряти електронні листи на відправника, адресу відправника та зміст повідомлення. Необхідно бути обачним та особливо уважними, якщо отримуєте незапрошені електронні листи від банків, фінансових установ або інших організацій.

Посилання можуть вести на підроблену вебсторінку, яка може імітувати оригінальну вебсторінку з проханням ввести особисті дані та/або конфіденційну інформацію. Посилання також можуть містити в собі зловмисне вкладення, яке при натисканні (переходу по гіперпосиланню) завантажує вірус або зловмисне програмне забезпечення на комп’ютер чи мобільний пристрій.

Шахрайство у вигляді фішингу також може спрямовувати користувачів на вебсторінки і використовувати спливаючі вікна для отримання їх особистої інформації. Якщо миттєво з’являється спливаюче вікно з проханням ввести особисту інформацію, такі як ім'я користувача та пароль, то це може свідчити про фішинг.

Антивірусне програмне забезпечення та вбудовані функції антифішингу

Встановлення антивірусного програмного забезпечення (далі - АВПЗ), увімкнення вбудованих функцій виявлення фішингу, регулярне оновлення його сигнатурних баз допоможе виявляти фішингові сайти та інші шкідливі програми, які можуть завдати значних фінансових втрат та втрати особистих даних.

Якщо є будь-які сумніви щодо легітимності вебсторінки, краще утриматися від введення своїх особистих даних і звернутися за консультацією від кваліфікованих фахівців у даній галузі.