БАНК КЛІРИНГОВИЙ ДІМ

Рекомендації щодо безпечного використання системи дистанційного обслуговування банку «Мобільний банкінг «MyBank365»

- ✓ Під час роботи в системі дистанційного обслуговування АБ «КЛІРИНГОВИЙ ДІМ» (далі – Банку) «Мобільний банкінг «MyBank365» (далі - МБ) не залишайте мобільний телефон без нагляду.
- ✓ Здійснюйте регулярне та своєчасне оновлення операційної системи свого мобільного телефону та МБ. Саме оновлення дозволить виправити уразливості в програмному забезпеченні та зменшити ризики інфікування шкідливими програмами.
- ✓ Використовуйте надійні паролі для запобігання несанкціонованого доступу до пристрою. Важливо створювати унікальну складну комбінацію для входу до облікового запису.
- ✓ Для запобігання несанкціонованого доступу до конфіденційної інформації не повідомляйте свої авторизаційні дані у МБ (логін, пароль тощо) третім особам (включаючи членів родини, друзів і т.д.).
- ✓ При використанні паролів не рекомендується зберігати паролі, взагалі, в будь-якому місці (на папері, на комп'ютері, на флеш-носіях, дискетах тощо). Пароль рекомендується запам'ятати!
- ✓ Після завершення роботи у МБ необхідно закрити сесію, натиснувши піктограму «Вихід».
- ✓ Рекомендується звертати увагу на можливі повідомлення веб-браузера про будь-яку небезпеку. У разі виникнення будь-якої підозри рекомендується завершити роботу із МБ та закрити МБ.
- ✓ Не відповідайте на запити (найчастіше запити розсилаються через SMS-повідомлення засобами мобільного зв'язку, електронною поштою тощо), які містять вимогу надати або перевірити логін, пароль тощо.
- ✓ Уникайте підключення до публічних Інтернет-мереж, які є менш захищеними та часто поширюють різні загрози.

Рекомендації щодо уникнення випадків підвищеного ризику збитків для користувача електронного платіжного засобу

- ✓ Запам'ятайте або занотуйте телефон цілодобової клієнтської підтримки Банку 0-800-50-18-08 або +38 044 593-10-20. За цими телефонами Ви можете зв'язатися з Банком та отримати консультацію по Вашій банківській платіжній картці (далі – Картка).
- ✓ Під час отримання Картки в Банку перевірте особисті дані, термін дії, цілісність ПІН-конверта (якщо він є) з персональним ідентифікаційним номером (далі – ПІН).

Поставте власний підпис на зворотному боці Картки (на спеціально відведеній смузі, що призначена для підпису держателя). Це зменшить вірогідність використання Картки без вашої згоди або в разі її втрати.

- ✓ Запам'ятайте слово-пароль, яке Ви вказали при оформленні Картки! Слово-пароль буде необхідне для голосової авторизації при Вашому зверненні до цілодобової клієнтської підтримки Банку.
- ✓ Зберігати ПІН-конверт потрібно окремо від Картки, в місці, яке відоме тільки Вам, і до якого не мають доступу інші особи, або запам'ятайте ПІН-код, а ПІН-конверт – знищіть (але не викидайте його цілим).
- ✓ Не записуйте ПІН-код навіть у змінній формі на Картці або на інших, паперових носіях у відкритому вигляді.
- ✓ Нікому не повідомляйте ПІН-код, навіть співробітникам Банку.
- ✓ Пам'ятайте: банк-емітент ніколи не здійснює запити та/або телефонні дзвінки своїм клієнтам – держателям Карт щодо перевірки реквізитів виданої платіжної картки або уточнення персональних даних (серія, номер паспорта, ідентифікаційний номер, персональний пароль, номер мобільного телефону тощо).
- ✓ Завжди тримайте в полі зору Вашу Картку при обслуговуванні у торгово-сервісній мережі.
- ✓ Не передавайте Вашу Картку або її реквізити іншим особам, в тому числі родичам, друзям, дітям.
- ✓ У разі виявлення втрати Картки або підозри на її незаконне використання – заблокуйте її за телефоном 0-800-50-18-08 або +38 044 593-10-20, та зверніться за перевипуском втраченої Картки.
- ✓ Знання повного номеру Картки або останніх її чотирьох цифр прискорить операцію блокування.
- ✓ Розблокування Картки, яку було втрачено, або яка побувала у руках сторонніх осіб, підвищує ризик втрати коштів з Вашого поточного рахунку та виникнення шахрайських операцій.
- ✓ Пам'ятайте, розрахунок Карткою в мережі інтернет, підвищує ризик шахрайських операцій по Вашій Картці в наслідок і втрати коштів з Вашого рахунку.
- ✓ З метою недопущення несанкціонованого використання Ваших коштів (шахрайських операцій), рекомендуємо відмовитися від введення даних Картки (номер, строк дії, CVV2-код) на сайтах, що пропонують Вам участь у різноманітних акціях з виплатою бонусної винагороди, а також на інших підозрілих сайтах. Дані сайти спеціально створені для незаконного збору реквізитів Карток з метою подальшого шахрайського використання.
- ✓ Обов'язково активуйте послугу SMS-інформування, яка надасть можливість отримувати інформацію про операції, які виконуються по Карті та рахунку, а також отримувати повідомлення для підтвердження операцій в мережі інтернет за технологією 3D-Secure.
- ✓ Встановлюйте ліміти на розрахунок Картками в мережі інтернет.

- ✓ Зверніть увагу! Банк ніколи не здійснює розсилання листів електронною поштою з проханням повідомити інформацію про Картку (номер, ПІН-код, строк дії та інше). Банк ніколи не вимагатиме введення на будь-яких сайтах таких параметрів Вашої Картки, як її номер, строк дії, CVV2 -коду та ПІН-код. Необхідно ігнорувати та не відповідати на листи, які потребують введення певних параметрів Вашої Картки. В таких випадках слід НЕГАЙНО зв'язатись з Банком за телефоном 0-800-50-18-08 або +38 044 593-10-20.
- ✓ Не записуйте та нікому не повідомляйте CVV2/-код. Введення CVV2 є підписом клієнта й прирівнюється до введення ПІН-коду при проведенні операцій в мережі Інтернет та/або операцій з ручним вводом даних Картки.
- ✓ Ніколи не передавайте реквізити Картки через відкриті канали інформаційного обміну: електронну пошту, SMS, соціальні мережі, чати тощо.
- ✓ Щонайменше 1 раз на місяць отримуйте в Банку контрольну виписку по поточному рахунку та підключіться до послуги «SMS -інформування».
- ✓ Рекомендуємо здійснювати операції з використанням Карт через банкомати, які встановлені в безпечних місцях (наприклад, в установах, банках, великих торговельних комплексах, готелях, аеропортах тощо). Не користуйтесь підозрілими банкоматами (на яких є предмети, залишки клею або інші сторонні пристрої, що викликають підозру).
- ✓ Будьте уважні до умов зберігання та використання Карти. Не піддавайте платіжну картку механічним, температурним та електромагнітним діям, а також уникайте потрапляння на неї вологи. Платіжну картку не можна зберігати разом з мобільним телефоном, побутовою та офісною технікою, а також поблизу металевих предметів та інших магнітних носіїв/пристроїв.
- ✓ Після отримання готівки в банкоматі необхідно її перерахувати та переконатись у тому, що платіжна картка була повернена банкоматом, дочекатись видачі чека в разі його запиту і тільки після цього відходити від банкомата.
- ✓ Роздруковані банкоматом чеки потрібно зберігати для звірки зазначених у них сум з випискою про рух коштів на картковому рахунку.
- ✓ Не слід проводити ніяких дій за підказками третіх осіб, а також не приймайте від них допомоги під час здійснення операцій через банкомат з використанням платіжної картки.
- ✓ Якщо під час проведення операції через банкомат платіжна картка не повертається, то необхідно зателефонувати до Банку за телефоном, який зазначено на банкоматі, та описати ситуацію, що склалася, а також звернутися з цього приводу до банку-емітента, який видав платіжну картку.
- ✓ Не здійснюйте операцій через банкомат/термінал самообслуговування, якщо Вам не зрозуміле його меню або інформація на екрані. Також не слід використовувати банкомати та термінали, якщо на них містяться невідомі пристрої та ті, що розташовані в підозрілих неосвітлених місцях.

- ✓ Розрахунки з використанням платіжної картки мають виконуватися тільки у вашій присутності. Це забезпечить зниження ризику неправомірного отримання ваших персональних даних, зазначених на платіжній картці.
- ✓ Перед набором ПІН слід переконатися, що треті особи, які перебувають у безпосередній близькості, не зможуть його побачити.
- ✓ Перед тим, як підписати квитанцію, в обов'язковому порядку перевірте суму, зазначену на ній.
- ✓ Якщо під час спроби здійснити оплату товарів або послуг з використанням Картки не вдалося здійснити успішно операцію, то необхідно зберігати один примірник виданої терміналом квитанції для перевірки відсутності зазначеної операції у виписці про рух коштів за картковим рахунком.
- ✓ Необхідно використовувати сторінки в мережі Інтернет (сайти/портали) тільки відомих і перевірених Інтернет-магазинів.
- ✓ Рекомендуємо не сканувати QR-коди на сторінках/сайтах, що викликають підозру.
- ✓ Якщо оплата товару (послуги) здійснюється через чужий комп'ютер, то рекомендуємо після завершення всіх розрахунків переконатися, що персональні дані та інша інформація не збереглася (знову відкривши сторінку продавця, на якій здійснювалась оплата товару).

Рекомендації клієнтам щодо виявлення фішингових вебсайтів

Фішинг: що це і як захиститись від нього.

Фішинг – вид шахрайства, метою якого є отримання доступу до конфіденційної інформації користувачів для послідуючого використання такої інформації у зловмисних цілях.

До такої конфіденційної інформації відносяться:

- ✓ логін та пароль для входу в систему дистанційного банківського обслуговування;
- ✓ номер, термін дії, CVV2/CVC2, ПІН платіжної картки;
- ✓ одноразові цифрові паролі;
- ✓ адреса електронної пошти;
- ✓ фінансовий номер телефону;
- ✓ слово-пароль (кодове слово), відповіді на секретні питання тощо

Фішинг, як правило, працює у двох напрямках – використання несанкціонованих розсилок електронних листів (СПАМу) або переадресування користувачів на зловмисні (підробні) вебсайти які ззовні або по імені дуже схожі на офіційні вебсайти певних організацій.

Зловмисники можуть також застосовувати голосовий фішинг, фішингові SMS – повідомлення, фішинг в соціальних мережах тощо. Як приклад, отримавши по схемі фішинга інформацію про номер платіжної картки, термін дії, імені та прізвище держателя платіжної карти, CVV/CVC2-коду, одноразового цифрового паролю – зловмисники можуть використати конфіденційну інформацію для здійснення несанкціонованих списань грошових коштів з даної платіжної карти. Держатель платіжної картки дізнається

про несанкціоновані операції вже по факту їх здійснення, отримуючи інформацію про рух коштів за допомогою SMS-інформування чи перегляду руху коштів в системі дистанційного обслуговування Банку «Мобільний банкінг «MyBank365».

Як розпізнати фішинговий сайт.

Перевірити сайт можна навіть просто візуально, не використовуючи жодних додаткових сервісів:

- ✓ Якщо домен сторінки починається з http://, а не з https:// і не має стилізованого символа замка, який повідомляє про встановлення безпечного https-з'єднання, ресурс, як мінімум, небезпечний, як максимум – може бути фішинговим.
- ✓ Реєстрація сайту, який надає послуги переказу коштів з картки на картку, а також поповнення мобільного телефону або онлайн-кредитування не в домені національного рівня «.UA», може бути ознакою фішингового ресурсу.
- ✓ Наявність нульових комісій та інших «НЕЙМОВІРНИХ» пропозицій має насторожити.
- ✓ Тематичні недоліки, наприклад відмінності в назві домену в адресному рядку і в тексті або на банері, теж можуть свідчити про те, що це шахрайський сайт.
- ✓ Якщо в адресному рядку відображаються однакові адреси для всіх сторінок сайту, свідчить що це шахрайський сайт.
- ✓ Легітимні сайти маскують введення карткових реквізитів (наприклад, зірочками) або використовують віртуальну клавіатуру, фішингові ресурси – не маскують.

Для боротьби з фішингом Українська міжбанківська асоціація членів платіжних систем ЕМА, яка за підтримки Державного департаменту США реалізує в Україні Національну програму сприяння безпеці електронних платежів і карткових розрахунків Safe Card, створила та регулярно оновлює список виявлених фішингових сайтів.

Ознайомитися з переліком сайтів, які становлять небезпеку, може кожен інтернет-користувач на офіційному ресурсі ЕМА в розділі «Чорний список сайтів»: https://www.ema.com.ua/citizens/blacklist/
Перелік перевірених надійних платіжних сервісів:
https://www.ema.com.ua/citizens/whitelist/
Посилання на офіційні сторінки учасників Української міжбанківської асоціації членів платіжних систем ЕМА (банки, платіжні системи):
https://www.ema.com.ua/about/members/

З метою забезпечення високого рівня безпеки інформації та унеможливлення доступу до конфіденційної інформації сторонніх осіб при роботі з вебсайтом Банк пропонуємо використовувати рекомендації наведені нижче:

- ✓ Користуватись лише офіційним вебсайтом Банку за посиланням: https://www.clhs.com.ua;
- ✓ Ніколи не здійснювати введення конфіденційної інформації у разі якщо Вас було переадресовано на невідомий вебсайт з незрозумілим доменним іменем.

БАНК КЛІРИНГОВИЙ ДІМ

УВАГА! АБ «КЛІРИНГОВИЙ ДІМ» ні при яких обставинах не здійснює телефонні дзвінки своїм діючим та потенційним клієнтам для отримання будь-якої конфіденційної інформації.

Посилання на сторінку офіційного Інтернет-представництва Національного банку України, на якій розміщено довідник банків, що містить інформацію про банки та відокремлені підрозділи банків.

Національний банк України на своєму офіційному Інтернет-представництві розмістив довідник банків, що містить інформацію про банки та відокремлені підрозділи банків України, який розміщено за даним **посиланням**.