ПАМ’ЯТКА КЛІЄНТА
з питань безпеки використання системи дистанційного банківського обслуговування

1. При здійсненні операцій засобами дистанційного банківського обслуговування:

- Зберігайте у режимі суворої секретності Ваші аутентифікаційні дані: логіни, паролі, PIN-коди, TouchID, які Ви використовуєте у роботі із сервісами системи дистанційного банківського обслуговування (далі - Система). Ніколи не зберігайте їх на SIM-картках, flash-накопичувачах і жорстких дисках Вашого мобільного телефону, планшету, ноутбуку або комп’ютера.
- Нікому (зокрема, і працівникам Банку) за жодних обставин не повідомляйте паролі та логіни у телефонному режимі або електронною поштою. Якщо Ви отримали електронний лист (зокрема, з будь-якої адреси Банку) з проханням повідомити або підтвердити Ваш логін або пароль – не відповідайте на запит. Зателефонуйте до служби підтримки клієнтів Банку та залиште повідомлення про спробу несанкціонованого отримання Ваших аутентифікаційних даних. Не надсилайте з власної ініціативи без прохання працівника служби підтримки отриманий лист на адреси Банку.
- Пам’ятайте, що Банк ніколи не запитує та не повідомляє (!) паролі у телефонному режимі або електронною поштою.
- Відключіть функцію запам’ятовування паролів у браузерах (Internet Explorer, Google Chrome, FireFox, Opera тощо) на мобільному телефоні, планшеті, ноутбуку і комп’ютері, за допомогою яких Ви працюєте з Системою.
- Для входу у Систему завжди використовуйте власні логін і пароль.
- Не залишайте без нагляду Ваш мобільний телефон, планшет, ноутбук або комп’ютер під час роботи з Системою.
- У разі втрати мобільного телефону, на який Ви отримуєте SMS-повідомлення з одноразовими паролями, негайно заблокуйте SIM-карту (номер телефону).
- На час довготривалої (декілька місяців і більше) перерви у роботі із Системою, зверніться до служби підтримки клієнтів Банку та заблокуйте свій логін.
- Не здійснюйте роботу із Системою з комп’ютерів інтернет-кафе, бізнес-центрів, готелів, ігрових залів або інших осіб, оскільки Ви не можете бути впевненими, що вони відповідають вимогам безпеки та захисту Ваших даних. Такі комп’ютери можуть бути заражені програмами для пошуку і крадіжки паролів, номерів платіжних карт тощо.

2. Фішинг: що це і як захиститись від нього

Фішинг (від англ. Fishing – «рибалка») – один з найбільш поширених видів шахрайства з використанням методів соціальної інженерії. Його мета – різними приводами виманити у власників платіжних карток конфіденційну інформацію, зокрема, й реквізити платіжних карт, що дає можливість отримати доступ до рахунку і вкрасти гроші. Аби зловити на гачок довірливого користувача, злочинці імітують діяльність наявних банків-емітентів і компаній, активно використовуючи неголосові засоби комунікації: SMS-повідомлення, e-mail-повідомлення, форму оплати на сайті, який є фішинговим вебресурсом.

Щоб зберегти свої персональні дані (конфіденційну інформацію) та грошові кошти в безпеці, перед тим, як вводити свої дані на вебсайті, потрібно звернути увагу на:

- Неправильне доменне ім'я – як правило, шахраї реєструють схожі домени. Наприклад, замість «ukrgasbank.com» можна побачити «ukrgazbank.com» або «ukrgasbnk.com».

- Відсутність SSL сертифікату – пошукові системи використовують шифрування SSL для передачі даних користувачів. При використанні цієї технології адреса сайту починається на «https: //». Якщо вебсайт починається на «http: //», це привід засумніватися в оригінальності сторінки. Шахраям не важко отримати дійсний SSL сертифікат для підробленого сайту – його можна отримати безкоштовно за допомогою спеціальних сервісів.
- Граматичні, орфографічні і дизайнерські помилки – розпізнати шахраїв можна за наявністю граматичних і орфографічних помилок в тексті вебсайтів. Насторожити повинні неправильні назви організації, численні помилки. Наприклад, збилась верстка, неправильне використання кольорів в дизайні, наявність сторонніх елементів дизайну.
- Різниця структур сторінок з оригінальним сайтом і підозрілі платіжні форми – потрібно звертати увагу на наявність посилань на сторінці. Якщо при натисканні на них ви переходите на сторінку з помилкою або на сторінки, які не схожі на оригінальний вебсайт – це свідчить, що ви потрапили на фішинговий сайт. Просто закрийте вкладку і не вводьте персональні дані в платіжні форми.
- Старий дизайн – ознакою фішингової форми може стати той факт, що вона розміщена на тлі застарілого дизайну вебсайту. Якщо вебсайт викликав у вас підозру, ігноруйте його та платіжну форму.
- Розділ вебсайту «Контакти» – слід перевіряти розділ «Контакти», аби переконатись, що фізична адреса вказана правильна, а не вигадана. Наприклад, авіакомпанія не може перебувати в промисловій зоні, а банківська установа – в покинутому офісі на околиці міста.

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/

Перелік Банків України та їх власних сайтів на офіційному сайті Національного банку України: https://bank.gov.ua/ua/supervision/institutions

3. Під час використання електронних платіжних засобів:

- Ніколи не повідомляйте конфіденційні дані вашої картки стороннім особам (ПІН-код, повний номер картки, термін дії та CVV2/CVC2-код). Пам'ятайте про те, що співробітники банку НІКОЛИ не запитують цю інформацію.
- Якщо вам телефонують з банку та повідомляють про несанкціоноване списання з рахунку – кладіть слухавку, незалежно від того, з якого номеру цей дзвінок надійшов. Для перевірки інформації передзвоніть у свій банк САМОСТІЙНО на номер, що зазначено на зворотному боці вашої картки.
- Завжди встановлюйте ліміт на покупки, як на фізичній, так і на віртуальній картці.
- Для online-покупок використовуйте ОКРЕМУ фізичну або віртуальну картку, аби не «розкривати» дані основної картки, наприклад, зарплатної. Не зберігайте на картах для online-покупок свої кошти тривалий час – краще витратити кілька хвилин для переказу потрібної суми, ніж втратити свої гроші.
- Негайно змінюйте ПІН-код до вашої карти, якщо є підозри, що він став відомий іншим особам. Блокуйте картку в разі виявлення спроб здійснити несанкціоновані платежі.
- Звертайте особливу увагу на сайти, де Ви плануєте здійснювати оплату товарів/послуг. Поле з назвою сайту повинно мати захисний протокол, який у разі наведення в це поле курсора має такий вигляд: «https://{назва сайту}»

4. Повідомлення в банк

ЯКНАЙШВИДШЕ звертайтесь до банку в разі виявлення:

- втрати електронного платіжного засобу;
- несанкціонованого доступу або зміни інформації клієнта в системах дистанційного обслуговування;
- фішингових вебсайтів або інформації про них.

Телефон цілодобової підтримки:

0 800 309 000 (безкоштовно з усіх телефонів)

358 - короткий номер з мобільного телефона (вартість дзвінків згідно з тарифами Вашого оператора)

503 (з мобільного і тільки для VIP-клієнтів, вартість дзвінків згідно з тарифами Вашого оператора)

+ 38 (044) 494 - 46 - 50 (вартість дзвінків згідно з тарифами Вашого оператора)
+ 38 (044) 590 - 49 - 99 (вартість дзвінків згідно з тарифами Вашого оператора)