Рекомендації клієнтам АТ «Альфа-Банк» щодо забезпечення фінансової та кібербезпеки під час користування банківськими послугами

З метою забезпечення високого рівня безпеки інформації та унеможливлення доступу сторонніх осіб до конфіденційної інформації Клієнтів під час користування банківськими послугами пропонуємо використовувати рекомендації наведені нижче.

Рекомендації щодо безпечного використання систем дистанційного обслуговування Банку:

- Використовуйте надійні паролі для запобігання несанкціонованого доступу до пристроїв з яких Ви здійснюєте доступ до систем дистанційного обслуговування Банку. Важливо створювати унікальну складну комбінацію для входу до облікового запису.
- Для запобігання несанкціонованого доступу до конфіденційної інформації не повідомляйте свої авторизаційні дані у системах дистанційного обслуговування (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.
- Банк ніколи та за жодних обставин не здійснює розсилку електронних листів із вимогою надіслати ключ, логін чи пароль, перейти за вказаною електронною адресою, а також не розповсюджує електронною поштою комп'ютерні програми. Відповідальність за збереження ключів та паролів покладається на користувача.
- У разі отримання подібних листів, програм чи будь-яких повідомлень електронною поштою, необхідно терміново проінформувати про це Банк зателефонувавши за номером +38 044 494-01-01 (по Україні) та +38 0462 61 61 11 – для дзвінків з-за кордону. Рекомендується видаляти підозрілі електронні листи без їх відкриття, особливо листи від невідомих відправників із прикріпленими файлами, що мають розширення *.exe, *.pif, *.vbs та інші файли
- Звертайте увагу на можливі повідомлення веб-браузера про будь- яку небезпеку. У разі виникнення будь-якої підозри рекомендується завершити роботу із системою дистанційного обслуговування та закрити її.
- 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.
- На комп'ютерах, з яких здійснюється робота в системі, використовуйте тільки ліцензійні операційні системи і антивірусні програми з регулярно оновлюваними антивірусними базами. Також регулярно оновлюйте операційну систему (в першу чергу це стосується оновлень безпеки). У повсякденній роботі не використовуйте обліковий запис із правами локального адміністратора (використовуйте призначений для користувача обліковий запис).

Повідомлення про несанкціонований доступ або зміну інформації Клієнта в системах дистанційного обслуговування

- Нікому не передавати управління своїм Обліковим записом в системі дистанційного обслуговування.
- Нікому не передавати в будь-якій формі свої логін та пароль Облікового запису в системі дистанційного обслуговування.
- Клієнт має забезпечити захист свого мобільного телефону та SIM-картки, на номер якої система дистанційного обслуговування надсилає коди підтвердження операцій.
- Клієнт має забезпечити антивірусну безпеку своїх інформаційних систем (на персональних комп'ютерах, смартфонах, планшетах і т.п.), за допомогою яких виконується доступ до системи дистанційного обслуговування.
- Негайно змінити пароль в системі дистанційного обслуговування у випадку якщо пароль, або його частина стала відома іншій особі.

Рекомендації щодо користування електронними платіжними засобами та уникнення випадків підвищеного ризику збитків для користувача електронного платіжного засобу

- Запам'ятайте або занотуйте телефон цілодобової клієнтської підтримки Банку +38 044 494-01-01 (по Україні) та +38 0462 61 61 11 – для дзвінків з-за кордону. За цими телефонами Ви можете зв'язатися з Банком та отримати консультацію по Вашій банківській платіжній картці (надалі - Картка).
- 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.
- Ніколи не записуйте ПІН або CVV2 коди на картці або інших паперових носіях .
- Ніколи не передавайте Картку або та не повідомляйте її реквізити (ПІН-код, повний номер картки, термін дії та CVV2/CVC2-код) іншим особам, в тому числі родичам, друзям, дітям по телефону, СМС, під час листування тощо. Пам'ятайте про те, що співробітники Банку ніколи не запитують цю інформацію.
- Ніколи не передавайте реквізити Картки через відкриті канали інформаційного обміну: електронну пошту, SMS, соціальні мережі, чати тощо.
- 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.
- 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.
- Завжди встановлюйте ліміти на покупки як на фізичній, так і на віртуальній картці, зокрема в мережі Інтернет.
- 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.
- 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.

- Ніколи не просіть незнайомих осіб допомоги вам при використанні банківської картки, особливо при роботі з банкоматом, не називайте їм ПІН-код.
- 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.
- 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.
- 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.
- Якщо Вам телефонують з банку та повідомляють про несанкціоноване списання з рахунку – не продовжуйте розмову та 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.
- Співробітники Банку або представники компаній платіжних систем Visa та MasterCard ніколи не здійснюють надсилання листів електронною поштою/запитів/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). Необхідно ігнорувати та не відповідати на запити та/або листи, які потребують введення певних параметрів Вашої Картки або персональних даних. В таких випадках слід негайно зв’язатись з Банком за телефоном +38 044 494-01-01 (по Україні) та +38 0462 61 61 11 – для дзвінків з-за кордону
- 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.

Рекомендації щодо виявлення фішингових веб-сайтів

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

До конфіденційної інформації належать::

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

Фішинговий сайт – це шахрайський веб-ресурс, що здійснює крадіжку реквізитів платіжних карт під виглядом надання послуг (це може бути, наприклад, поповнення мобільного рахунку або переказ коштів з картки на картку), або клон веб-ресурсу організації, якій користувач довіряє.

Основні схеми фішингових операцій:

- використання розсилок електронних листів (спаму) з певними пропозиціями купівлі товарів та послуг, листами-повідомленнями про блокування облікового запису пошти, доступу до системи клієнта банку та ін.
- розповсюдження через електронні листи чи веб-сайти програмного забезпечення із зловмисним кодом (тобто програмного вірусу) для заволодіння даними автентифікації користувача;
- переадресування користувачів на зловмисні (підробні) сайти, які ззовні, або за доменним ім'ям, схожі до офіційних сайтів певних організацій.
- голосовий фішинг,
- фішингові СМС – повідомлення,
- фішинг в соціальних мережах тощо.

Отримавши за допомогою схеми 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.

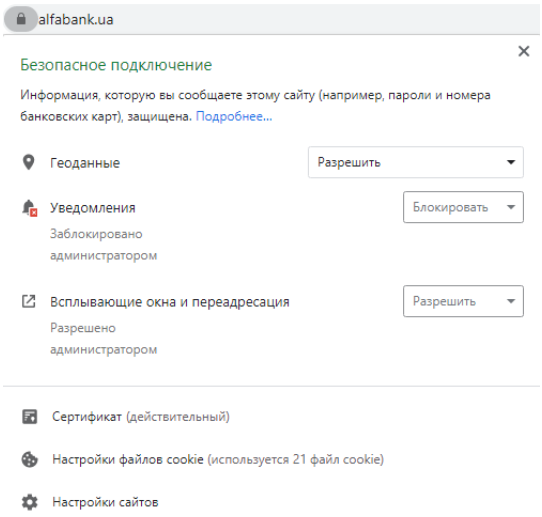
Можливі ознаки фішингових /небезпечних сайтів:

- неправильне доменне ім'я – як правило, шахраї реєструють схожі домени. Наприклад, замість «alfabank.ua» можна побачити «alfa.bank.ua» або «alfabank.ua». Також сайт може розташовуватися на піддомені, наприклад, «alfabank.site.ua» тощо.
- відсутність SSL сертифікату – пошукові системи використовують шифрування SSL для передачі даних користувачів. При використанні цієї технології адреса сайту починається на «https: //». Якщо веб-сайт 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.
- 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»,
- наявність нульових комісій та інших «неймовірних» пропозицій,
- тематичні недоліки, наприклад відмінності в назві домену в адресному рядку і в тексті або на банері,
- в адресному рядку відображаються однакові адреси для всіх сторінок сайту,
- легітимні сайти маскують введення карткових реквізитів (наприклад, зірочками) або використовують віртуальну клавіатуру, фішингові ресурси - не маскують.

Під час користування інтернет-сайтами АТ «Альфа-Банк» звертайте увагу на наступне:

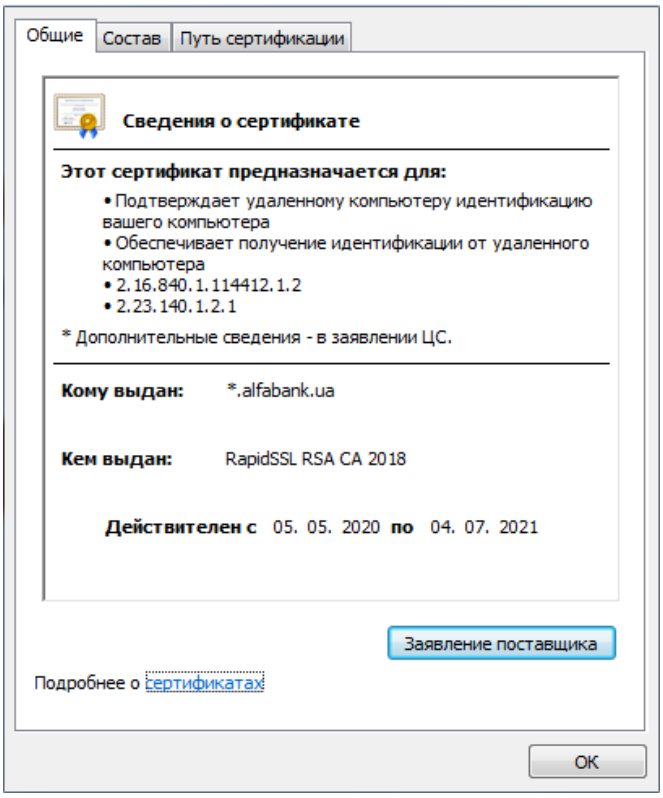
- Завжди здійснюйте візуальну перевірку перевіряти доменне ім'я для впевненості, що це офіційна, а не фішингова сторінка зловмисників. На даний час АТ «Альфа-Банк» має такі офіційні веб-сайти:
  https://alfabank.ua/– офіційний корпоративний веб-сайт Банку в мережі Інтернет
  https://auth.alfabank.com.ua – офіційна система Інтернет-сервісу Банку
  https://ap.alfabank.com.ua - офіційна система надання послуги «Альфа-погашення»
  https://a-club.alfabank.com.ua – офіційна сторінка «A-Club»
  https://ok.alfabank.com.ua – офіційна сторінка Інтернет-банкінгу для бізнесу «Ок! Альфа»
  та інші веб-сайти, розміщені на доменних іменах alfabank.ua та alfabank.com.ua

- Виконуйте перевірку кому та ким виданий SSL сертифікат і стежте за строком його дії (див. рис.нижче).



Зображення замкнутого «замка» означає, що на веб-сайті встановлений SSL-сертифікат і вся інформація передається по захищеному протоколу. SSL-сертифікат не дає шахраям перехопити або підмінити особисті дані користувачів.

Натиснувши на значок «замка» ліворуч від доменного імені (див. рисунок нижче) і можна переглянути властивості сертифікату:



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.

На офіційному ресурсі ЕМА можна ознайомитись із:

- переліком сайтів, які становлять небезпеку - в розділі «Чорний список ЕМА» за посиланням: **https://www.ema.com.ua/citizens/blacklist/**
- переліком перевірених надійних платіжних сервісів – в розділі «Білий список»: за посиланням **https://www.ema.com.ua/citizens/whitelist/**

Також на офіційній сторінці ЕМА можна ознайомитись із учасниками Української міжбанківської асоціації членів платіжних систем ЕМА (банки, платіжні системи) за посиланням: https://www.ema.com.ua/about/members/

Рекомендації щодо дій з негайного інформування Банку

Максимально швидко звертайтесь до Банку у разі:

- виявлення втрати Картки або підозри на її незаконне використання;
- несанкціонованого доступу або зміни Вашої інформації в системах дистанційного обслуговування.

Цілодобова клієнтська підтримка:
3344[1] - для дзвінків з мобільних телефонів

+38 (044) 494 01 01 - згідно з тарифами Вашого оператора

+38 (0462) 616 111 - для дзвінків з-за кордону

Посилання на сторінку офіційного Інтернет-представництва Національного банку України

На сторінці офіційного Інтернет-представництва Національного банку України розміщено довідник банків, що містить інформацію про банки та відокремлені підрозділи банків, з яким можна ознайомитись за посиланням **https://bank.gov.ua/supervision/institutions**.

[1] Вартість дзвінка на короткий номер 3344 становить 2,00 грн. Тариф у гривнях з урахуванням ПДВ. Додатково утримується збір до Пенсійного фонду у розмірі 7,5 % від вартості послуги без урахування ПДВ. Послуга надається абонентам всіх національних GSM операторів . Тільки для повнолітніх