Правила безпеки

Заходи безпеки при використанні банківських продуктів

Банк Кредит Дніпро завжди забезпечує безпеку Ваших коштів та платежів, але і Ви повинні дбати про безпеку своїх грошей. Рекомендуємо ознайомитися з правилами безпеки, дотримуючись яких Ви зможете не стати жертвами шахраїв.

Ми зібрали рекомендації, які допоможуть зберегти Ваші кошти у безпеці.

МЕТОДИ ПРОТИДІЇ ШАХРАЯМ

Правила спілкування з шахраями та любителями виграшів у лотерею

Як не стати жертвою соціальної інженерії?

Правило № 1. Ніколи не надавайте інформацію про свої картки третім особам, навіть якщо вони звертаються до вас нібито від імені банку.

Банк Кредит Дніпро не телефонує й не надсилає повідомлень, щоб попросити клієнтів зазначити номер банківської картки, строк її дії, ПІН-код або CVV2-код картки, пароль у FreeBank, а також паролі, що надходять у SMS.

Окрім банкоматів, терміналів самообслуговування та POS-терміналів, запитати ПІН-код вашої картки може тільки система Інтернет-банкінгу FreeBank. Банк ніколи не просить продиктувати ПІН-код або переслати його в повідомленні куди-небудь!

Якщо Ви зателефонували до банку, співробітник може уточнити дівоче прізвище вашої матері або інше кодове слово, проте співробітники банку не телефонують клієнтам для уточнення цієї інформації.

Для отримання переказу на картку за продаж товару необхідно зазначити лише номер картки. Вимоги покупця назвати інші дані (CVV2-код, строк дії картки, баланс чи тип картки) для переказу грошей на вашу картку повинні викликати у Вас підозри.

Правило № 2. Будьте пильні, якщо вам приходять SMS невідомого адресата з проханням надіслати отриманий код або дивний набір команд на інший номер.

Швидше за все, це шахрайство. Не розголошуйте зміст отриманого Вами SMS-повідомлення іншим особам. Також не виконуйте на телефоні операцій, суті яких Ви не знаєте. Шахраї можуть обманом змусити вас налаштувати переадресацію викликів та SMS із Вашого номера на чужий. Таким чином, адресовані Вам SMS або дзвінки від банку будуть надходити шахраям, які зможуть використовувати їх для доступу до Ваших рахунків.

Комбінація для переадресації всіх викликів мобільних операторів «Київстар», Vodafone, lifecell: **21*+380XXXXXXXXX#

Переадресація SMS у мобільного оператора Vodafone: надішліть SMS із кодом +380XXXXXXXXX на номер 3031.

Переадресація SMS у решти мобільних операторів налаштовується в особистому кабінеті.

Правило № 3. Сумнівні розіграші.

Якщо Вам надійшло SMS, інформаційне повідомлення, лист тощо про виграш, для отримання якого потрібно терміново сплатити податок, мито або ввести свої персональні дані, – Вас намагаються обдурити шахраї.

Щоб уберегти себе від дій шахраїв, зайдіть на офіційний сайт компанії або зверніться в службу підтримки – великі компанії завжди розміщують інформацію про свої акції.

Ніколи не переказуйте грошей до отримання призу й не поспішайте – розрахунок шахраїв будується на неусвідомлених і швидких діях клієнтів.

Правило № 4. Будьте уважні, якщо отримали SMS фінансового характеру від знайомого (його аккаунт у соц. мережі могли зламати)

Якщо Вам на e-mail, у Skype, Viber, Telegram або в повідомленні в соц. мережах надійшло прохання фінансового характеру або підозріле посилання від Вашого знайомого, який раніше такого не надсилав, зв'яжіться з ним у голосовому режимі та уточніть, чи сам він надіслав це повідомлення. Обліковий запис могли зламати зловмисники. Встановіть на всі свої акаунти (пошта, соц. мережі) надійні та різні паролі. Якщо обліковий запис можна додатково захистити двофакторною аутентифікацією (коли вхід в акаунт підтверджується за допомогою мобільного телефону), використовуйте таку можливість.

ПРАВИЛА БЕЗПЕКИ ПРИ ЗДІЙСНЕННІ ОПЕРАЦІЙ В ІНТЕРНЕТІ

Заходи безпеки оплати карткою в мережі інтернет:

- Використовуйте окрему картку для розрахунків в мережі інтернет з окремим рахунком (поповнюйте її на суму запланованих витрат).

- Підключіть послугу SMS – банкінг та інтернет-банкінгу та слідкуйте за витратами. Не розголошуйте коди з SMS повідомлень третім особам.

- Встановіть денні ліміти в інтернет-банкінгу по сумі та операціях по карті, заблокуйте можливість проведення онлайн-операцій.

- Обмежте можливість проведення операцій в інтернеті (у додатку FreeBank). Надавайте та забороняйте дозвіл на інтернет-операції за допомогою Інтернет-банкінгу. Активуйте можливість тільки на момент оплати.

БЕЗПЕКА ПІД ЧАС КУПІВЕЛЬ В ІНТЕРНЕТІ

Купівлі та продажі в інтернеті

Правило № 1. Якщо Ви продаєте товар на інтернет-майданчику, для отримання переказу на картку за продаж товару необхідно зазначити лише номер картки.

Вимоги покупця назвати інші дані (CVV2-код, строк дії картки, баланс чи тип картки) для переказу грошей на Вашу картку повинні викликати у Вас підозри.

Правило № 2. Не залишайте номер свого фінансового телефону в Інтернеті.

Тим, хто веде бізнес, ми рекомендуємо завести окремий контрактний телефон для переговорів з контрагентами.

Не використовуйте фінансовий номер під час контактів з широким загалом. Це може призвести до крадіжки Вашої SIM-картки шахраями через перевипуск у відділеннях мобільного оператора.

Правило № 3. Якщо Ви здійснюєте купівлі через Інтернет в маловідомих вам людей, рекомендуємо використовувати післяплату.

Якщо Ви платите на перевірених майданчиках інтернет-гігантів, використовуйте під час розрахунків Інтернет-картку.

Під час здійснення покупки деталі угоди обговорюйте тільки в чатах магазинів та ігноруйте пропозиції незнайомців перейти в месенджери для зручності.

Безпечне використання веб-ресурсів

Як розпізнати фішинговий веб-сайт?

Достатньо дотримуватися наступних простих порад:

Обов’язково перевіряйте адресний рядок, за яким рекомендується перейти, на наявність незначних помилок у написанні.

Користуйтеся тільки безпечним з’єднанням https. Відсутність букви s в адресі сайта має насторожити. Перевірте офіційну адресу сайту за допомогою Довідника банків НБУ за посиланням.

Не переходьте за невідомими посиланнями та не вводьте реквізити картки на невідомих сайтах (перевіряйте посилання).

Не скануйте QR-коди на підозрілих сайтах.

З підозрою поставтеся до будь-яких листів із вкладеннями та посиланнями. Навіть якщо вони прийшли зі знайомої адреси, це не дає гарантії безпеки: поштову скриньку могли зламати.

Якщо все ж необхідно відвідати ресурс, краще ввести його адресу вручну або скористатися попередньо збереженими закладками.

Не використовуйте для доступу до онлайн-банкінгу та інших фінансових сервісів відкриті Wi-Fi-мережі: часто їх створюють зловмисники.

На всіх акаунтах, де це можливо, підключіть двохфакторну аутентикацію. Цей захід може врятувати становище, якщо основний пароль став відомий хакерам.

Перевіряйте сайт, як давно він створений, не довіряйте просто позитивним відгуки, бо їх можуть писати самі шахраї. **Перевірте сайт**

Перевірити продавця/покупця на сервісі Кіберполіції STOP FRAUD або дізнатися дані про сайт, послугами якого збираєтесь скористатися, чи присутній він в списку шахрайських Black List ЄМА.

Повідомити про факти шахрайства з боку третіх осіб

Якщо Вам телефонували та намагалися отримати особисту інформацію: CVV2-код, паролі, ПІН-код тощо.

Якщо Ви скористалися фішинговим сайтом (або такий, який тільки здається підозрілим).

Повідомте нам про це за телефоном 0 800 507 700, ми врахуємо Ваш приклад під час розробки нових методів запобігання шахрайству.

Якщо Ви повідомили шахраю пароль до інтернет-банкінгу, продиктували код з SMS-повідомлення, надали реквізити платіжної картки:

- Негайно зателефонуйте до Банку за телефном гарячої лінії 0 800 507 700 і заблокуйте інтернет-банкінг/платіжну картку та повідомте про шахрайство. Також заблокувати Вашу картку можна самостійно, скориставшись Інтернет-банкінгом FreeBank.

- У разі якщо пройшли шахрайські операції по картці, зверніться до поліції або кіберполіції. Залишіть заяву на сайті департаменту кіберполіції (www.cyberpolice.gov.ua), заповнивши форму електронної заявки за **посиланням**.

Негайно повідомте Банк Кредит Дніпро:

- про втрату чи крадіжку платіжної картки (для її блокування);
- про втрату телефону, фінансового номеру телефону (SIM-картки), щоб ми змогли запобігти шахрайству;
- при підозрілих операціях по картці, які ви не здійснювали, щоб ми змогли оперативно провести перевірку.

ЗАХОДИ БЕЗПЕКИ ПІД ЧАС КОРИСТУВАННЯ БАНКІВСЬКИМИ КАРТКАМИ

Правило № 1. Ніколи не записуйте ПІН-код на пластиковій картці: у разі крадіжки або втрати картки сторонні особи можуть без перешкод зняти з неї кошти.

Правило № 2. Ніколи не просіть незнайомих людей допомогти Вам скористатися пластиковою карткою.
Самостійно вводіть ПІН-код, не показуючи його оточуючим і не вимовляючи вголос.

Правило № 3. Заблокуйте свою картку або номер фінансового телефону в разі викрадення або втрати.

Правило № 4. Попередьте банк про те, що збираєтеся використовувати картку за кордоном.

Використання картки в банкоматі та торгівельній мережі

Правило № 1. Користуйтеся карткою в надійних банкоматах (у відділеннях, у торгових центрах чи людних місцях або в банкоматах Банка Кредит Дніпро), при цьому:

- перевіряйте на наявність сторонніх предметів банкомату, вікно видачі купюр та картоприймач;
- помістіть картку до карткоприймача, вона повинна самостійно затягуватися в банкомат, не прикладайте зусиль для цього;
- під час введення ПІН-коду прикривайте клавіатуру рукою;
- у разі, якщо банкомат не видав кошти – не панікуйте. Перевірте вікно видачі купюр, там може бути стронній пристрій. Якщо Ви отримали SMS про списання коштів, але невидав їх у вікно видачі, передзвоніть не відходячи від банкомату до Банку;
- звіряйте вигляд пристроїв банкомату з зображенням на екрані самого банкомату.

Правило № 2. У разі оплати в супермаркетах:

- використовуйте безконтактну оплату PayPass, Google Pay, Apple Pay;
- не передавайте картку в руки касирові під час розрахунків.

Правило № 3. Не проводьте операції, суть яких Вам не зрозуміла, через банкомат або термінал самообслуговування.

Правило № 4. Якщо Ви плануєте значні витрати за кордоном, випустіть окрему чиповану картку, що буде поповнюватися на суму планованих витрат.

ЗАХОДИ БЕЗПЕКИ ПІД ЧАС КОРИСТУВАННЯ СМАРТФОНОМ

Захист смартфону.

Правило № 1. Установіть пароль. Сучасні телефони та планшети дозволяють обмежити доступ до пристрою за допомогою пароля, ПІН-коду, графічного ключа тощо.

Правило № 2. Не передавайте смартфон стороннім. Якщо Ваш телефон або планшет потрапить до рук зловмисника, він зможе користуватися Вашим SMS-банкінгом, отримувати одноразові паролі для входу до Вашого FreeBank та підтвердження платежів.

Правило № 3. Не зберігайте конфіденційні дані на смартфоні та планшеті

Номери Ваших карток, логін і пароль для FreeBank, персональні дані (кодове слово, ІПН тощо) не можна записувати в смартфоні, інакше в разі втрати або крадіжки вони дістануться шахраям. Після закінчення роботи з мобільними додатками виходьте з сесії за допомогою кнопки «Вихід» у додаткових налаштуваннях.

Перевірте ваш GOOGLE-диск і поштові скриньки: чи немає там фотографій Ваших документів? Відключить зберігання паролів у Веб-браузері. Шахраї заволодівши ними, можуть оформити кредити.

Правило № 4. Захистіть свої смартфон і планшет від вірусів. Щоб не заразити свій телефон вірусами:

- не зламуйте операційну систему свого смартфону та не проводьте банківських операцій через Інтернет на пристрої зі зламаною операційною системою;
- не відвідуйте незнайомі Вам сайти;
- не переходьте за підозрілими посиланнями;

- встановлюйте програмне забезпечення тільки з перевірених джерел;
- під час встановлення додатків з App Store чи Play Market уважно ознайомтеся з дозволами, що запитують додатки;
- стежте за тим, щоб на Вашому мобільному телефоні було встановлено та своєчасно оновлювалось антивірусне програмне забезпечення.

Захист фінансового номера.

Правило № 1. Використовуйте стандартний механізм захисту SIM-картки (ПІН). Завжди використовуйте для захисту SIM-картки ПІН-код. Змініть стандартний пароль SIM-картки на власний. Ці заходи не дозволять скористатися Вашою SIM-карткою в разі втрати/крадіжки телефону.

Правило № 2. Завантажте додаток мобільного оператора, з метою контролю стану номеру телефону. Встановити додаткові паролі. Відключіть можливість віддаленого перевипуску SIM-карти.

Правило № 3. У разі втрати смартфону заблокуйте свій номер телефону та картки. Якщо Ви загубили смартфон або планшет, терміново зателефонуйте в банк на номер 0 800 507 700 (безкоштовно з мобільного) і заблокуйте свої картки, інтернет-банкінг та номер телефону. Наголосіть про блокування токену картки, якщо він був у Вас. Потім зв'яжіться з мобільним оператором для блокування SIM-картки.

Правило № 4. Зробіть так, щоб мобільний оператор знав про Вас більше ніж просто номер. Зверніться до місцевого відділення мобільного оператора, щоб до вашого номера додали дані власника, копію паспорта і т. д. Це захистить Вашу SIM-картку в разі спроб перевипуску.

ЗАХОДИ БЕЗПЕКИ ПІД ЧАС КОРИСТУВАННЯ ОНЛАЙН-БАНКІНГОМ

Правило № 1. Створіть безпечний пароль до онлайн-банкінгу

Створіть складний пароль до онлайн-банкінгу, який може містити:

- 8 і більше символів;
- ВЕЛИКІ та малі літери;
- цифри та спеціальні знаки/символи (! @ «# № $ %:; ^ &? * () — _ + =.).

Створюйте унікальний пароль для кожного інтернет-банкінгу, електронної пошти, соціальних мереж тощо.

Правило № 2. Перевіряйте безпечність логування

- Для логування в онлайн-банкінг **ніколи не використовуйте гіперпосилань, які надіслані вам в SMS-повідомленнях**, **месенджерах (Telegram, Viber, WhatsApp, ін.) в електронних листах від незнайомих адресатів**.
- Вхід в онлайн-банкінг здійснюйте виключно **з головної сторінки** Банк Кредит Дніпро.
- Здійснюйте логування виключно через мобільні додатки онлайн-банкінгу, що завантажені на пристрій **з офіційних магазинів Google Play для Android та App Store для iOS**.

Правило № 3. Не здійснюйте вхід до онлайн-банкінгу через загальнодоступні пристрої, відкриті (незахищені) мережі WI-FI

- **Використання відкритих (незахищених) WI-FI** мереж є великою загрозою;
  Не підключайтесь до відкритих WI-FI мереж, якщо хочете скористатися онлайн-банкінгом;
- Уникайте **використання онлайн-банкінгу з пристроїв, які перебувають поза вашим контролем** (чужий комп'ютер, наприклад, інтернет кафе);
- Загальнодоступні пристрої можуть мати **вірус або на них може бути встановлене зловмисне програмне забезпечення.** Їх краще використовувати для читання новин, порталів тощо.

Правило № 4. Нікому не повідомляйте конфіденційну інформацію (паролі, коди, інше)

Будьте пильні з телефонними шахраями!

Телефонне шахрайство — це вид шахрайства, коли шахрай телефонує і переконує Вас повідомити особисту, фінансову чи конфіденційну інформацію або переказати гроші.

Рекомендації як зупинити списання з Вашої картки, раніше прив'язаної до платних послуг

Повідомляємо, що при додаванні банківської картки до платних сервісів App Store/Google Play можуть бути утримані суми за передплату!

Якщо Ви давно не використовуєте або видалили програму App Store/iTunes/Google Play, але не скасували підписку, плати за передплату можуть продовжувати списуватися з картки автоматично на регулярній основі або щоразу за фактом отримання послуги. Банк наполегливо рекомендує всім своїм клієнтам уважно вивчати всі умови підписок, що оформлюються, на різних платних сервісах.

Пам'ятайте, що підписка перестане діяти з наступного платного періоду після її скасування.

Якщо Вам все ж таки не вдалося скасувати підписку, рекомендуємо звернутися до служби підтримки Google Play/App Store/iTunes або підтримки іншого ресурсу, де Ви могли прив'язати картку до платного облікового запису.