Золоті правила

Безпека роботи з системою StarAccess

УКРСИББАНК
BNP PARIBAS GROUP

STAR ACCESS

Золоті правила безпеки при роботі з системою StarAccess

Інтернет розвивається, зі зростанням популярності з'являються і певні загрози при роботі в ньому. Це вимагає більш відповідального відношення, як з боку банку, так і клієнта.

StarAccess – наша система електронного банкінгу, яка безумовно є зручним сервісом. Як Ваш банк, ми використовуємо тільки найкращі сучасні технології та практики для того, щоб вона також була і найбезпечнішою.

Ми не зупиняємося ні на день в розробках і впроваджені найсучасніших методів безпеки, починаючи з самого першого дня запуску StarAccess.

З повагою, Ваш УкрСиббанк

Про які загрози ми говоримо…

З розвитком інтернет-технологій активізувалися і шахраї, єдиною метою яких є крадіжка Ваших грошей або грошей Вашої компанії.

Шахраї використовують різноманітні методи для того, щоб заволодіти Вашою персональною інформацією з метою її подальшого неправомірного використання.

Приклади таких методів:

- **Встановлення на комп'ютер шкідливих програм** – вірусних і троянських програм, здатних вкрасти пароль і секретний ключ електронно-цифрового підпису.

- **Розсилка листів від імені банку** з проханнями перейти на вказану інтернет-адресу, вказати шлях і пароль до свого ключа електронно-цифрового підпису, або вислати персональні дані для їх перевірки чи поновлення в базах даних банку, тощо.

Як захистити себе - наші золоті правила

StarAccess - надійна і безпечна система. Для того, щоб максимально захистити Ваші кошти, StarAccess використовує багато методів, таких як:

- **Шифрування даних** - для забезпечення конфіденційності інформації.
- **Електронний цифровий підпис під електронними документами** - підписуючи документ, Ви будете певні, що Ваш документ переданий до банку саме в тому вигляді, в якому Ви його створили.
- **IP-фільтрація** - для забезпечення доступу до StarAccess тільки з комп'ютерів, які використовуєте Ви.
- **Оперативне сповіщення** за допомогою безкоштовних SMS-повідомлень або електронних листів про події, такі, як вхід до системи або проведення платежів - для того, щоб Ви завжди були в курсі всіх подій і мали можливість реагувати на них.
- **Одноразові паролі (OTP)** - для додаткового контролю при вході до StarAccess, а також для підтвердження платежів.

Як захистити себе - наші золоті правила

Ми вважаємо, що StarAccess - це не тільки система, але і форма взаємовідносин, в якій завжди є дві сторони: ми - Ваш банк, і Ви - наш клієнт.

Зі свого боку ми робимо все можливе, щоб Ваші кошти завжди були в безпеці, а Ви відчували задоволення від співпраці з нами.

Ми хочемо, щоб наші стосунки завжди приносили Вам тільки радість, тому просимо також і Вас дотримуватися певних «золотих» правил роботи зі StarAccess.

Як захистити себе - наші золоті правила

- **Персональна відповідальність** - ніколи не передавайте іншим особам персональну інформацію, таку як ключі та паролі, або OTP-токени. Закінчуючи роботу, завжди виходьте зі StarAccess для того, щоб ніхто інший не міг скористатися StarAccess для доступу до Ваших даних.

- **Електронні листи** - ніколи не відкривайте листи від відправників, які Вам не знайомі, тим більше, якщо до листа включені будь-які файли. Не відповідайте на такі листи і не відправляйте свою персональну інформацію. Пам'ятайте, таким способом шахраї часто намагаються отримати Ваші персональні дані, такі як паролі, логіни, номери пластикових карток і рахунків та ін.

- **Операційна система** - використовуйте тільки ліцензійне програмне забезпечення, проводьте регулярні оновлення, як правило, вони завжди доступні на сайті розробника. По можливості, налаштуйте автоматичне оновлення. Це важливо, тому що в оновленнях містяться нові елементи для забезпечення безпеки Вашого комп'ютера.

- **Антивірусне програмне забезпечення** - завжди використовуйте та оновлюйте на Вашому комп'ютері антивірусне програмне забезпечення. Ми, зі свого боку, рекомендуємо використовувати тільки офіційні продукти, наприклад, Касперський, McAfee, Dr.Web та ін. Бажано проводити сканування комп'ютера такими програмами раз на день, але обов'язково не рідше ніж раз на тиждень.

- **Мережевий екран (firewall)** на Вашому комп'ютері - це захист від небажаного доступу з Інтернету. За допомогою такого доступу шахраї можуть встановлювати вірусні, троянські та інші шкідливі програми на Ваш комп'ютер.

Як захистити себе - наші золоті правила

- **Інтернет-браузери** - ми рекомендуємо використовувати новітні версії інтернет-браузерів. Вони доступні для завантаження на сайтах розробників і містять поліпшені властивості безпеки, наприклад:

  Google Chrome
  Microsoft Internet Explorer
  Mozilla Firefox

- **Пароль** - намагайтеся використовувати складні для вгадування комбінації. Не використовуйте дати народження, прості комбінації цифр і паролі, які Ви використовуєте для входу на будь-який інший сайт або в іншу програму, тощо.

- **OTP (англ. One Time Password - одноразові паролі**) - використовуйте їх, це необхідний і надійний захист. Підтвердження входу до StarAccess та підтвердження платежів одноразовим паролем робить вкрай важкою крадіжку Ваших коштів шахраями. Більш докладно Ви можете дізнатися про OTP і методи їх генерації, звернувшись до свого менеджера або в Контакт-центр.

- **Підозра компрометації** – якщо Ви підозрюєте, що Ваші персональні дані скомпрометовані, або Ви помітили щось незвичайне в роботі StarAccess, негайно зв'яжіться з Контакт-центром банку за телефонами 0 800 505 800 (безкоштовно зі стаціонарних телефонів в Україні) або 380 44 590 06 90 (для міжнародних дзвінків).

Робота з одноразовими паролями

OTP (англ. One Time Password) – це пароль, який використовується при вході до StarAccess або для підтвердження платежу. OTP неможливо вкрасти за допомогою вірусу або троянської програми, саме тому він є надійним засобом захисту від шахраїв.

Ви можете отримувати OTP на свій мобільний телефон у **вигляді SMS-повідомлення**, або використовуючи **OTP-токен** (виданий у відділенні банку).

OTP-токен (генератор одноразових паролів) – це компактний і зручний пристрій з однією кнопкою та екраном, який використовується для генерації одноразових паролів. Підключення токена до комп'ютера не потрібне.

Після натискання на кнопку на екрані відображається одноразовий пароль, який необхідно використовувати для підтвердження входу в систему StarAccess і для відправки платежів.

Як захистити себе - наші золоті правила

Підводячи підсумки, для Вашої безпеки при роботі з системою StarAccess, ми просимо Вас дотримуватися наведених правил. Коротко, вони будуть виглядати наступним чином:

- **Завжди використовуйте тільки ліцензійне програмне забезпечення** на Вашому комп'ютері, стежте за його регулярними оновленнями.

- **Використовуйте антивірусне програмне забезпечення і мережевий екран** з найжорсткішими налаштуваннями.

- **Не відвідуйте** підозрілі інтернет-сайти і не відкривайте електронні листи, отримані від невідомих Вам відправників.

- **Завжди використовуйте OTP** (токен або SMS), як для входу до StarAccess, так і для підтвердження платежів.

- **Ніколи не передавайте** іншим те, що призначене тільки для Вас - пароль, OTP-токен і т.д. Завжди виходьте зі StarAccess, коли завершуєте роботу з системою.

- **Використовуйте безкоштовні сервіси сповіщення** за допомогою SMS-повідомлень або електронних листів про події з Вашим рахунком.

- Якщо у Вас виникли підозри, що Ваші дані могли бути скомпрометовані, або Ви помітили щось незвичне у роботі StarAccess, **негайно повідомте про це Вашого менеджера або зверніться до Контакт-центру банку.**

Дякуємо за Вашу увагу!

Ми сподіваємося, що ці прості правила допоможуть нам і далі будувати прекрасні відносини.

Якщо у Вас виникнуть додаткові питання, Ви завжди можете зв'язатися з Вашим персональним менеджером, або звернутися до Контакт-центру банку за телефонами:

- ***0 800 505 800*** *(безкоштовно зі стаціонарних телефонів в Україні);*
- ***38 044 590 06 90*** *(для міжнародних дзвінків).*