Рекомендації щодо безпечної роботи в системі дистанційного обслуговування «Інтернет-Банкінг»

Дані Рекомендації розроблені Банком для здійснення Клієнтом безпечної роботи в системі дистанційного обслуговування «Інтернет-банкінг» та дозволяють значно знизити ризики шахрайських операцій із рахунками, доступ до яких здійснюється каналами «Інтернет-Банкінгу».

1) Рекомендації щодо безпеки поводження з даними автентифікації (особистим ключем та паролем доступу до нього):
   - Особистий ключ та пароль доступу до нього є найкритичнішими даними з точки зору безпечної роботи в системі «Інтернет-банкінг». Особистий ключ генерується за ініціативою користувача — його власника під особистим контролем. Банк ні за яких обставин не має доступу до особистих ключів користувачів. Для забезпечення надійного зберігання та використання особистих ключів **наполегливо рекомендується** використання апаратних пристроїв формування підпису (токенів - «**iBank-2 Key**») та пристроїв багатофакторної аутентифікації і підтвердження документів корпоративних і приватних клієнтів (**OTP-токенів або SMS-підтвердження**), що постачаються Банком.
   - У разі, якщо користувач обирає метод зберігання ключів в файловому контейнері, особисті ключі повинні зберігатися виключно на рухомому носії інформації (диск, USB-накопичувач). Не допускається навіть тимчасове зберігання ключів ЕЦП на жорсткому диску робочих станцій (комп'ютерів).
   - Носій ключової інформації, який містить чинний ключ (рухомий носій інформації, токен), повинен постійно бути під особистим контролем користувача, що забезпечує унеможливлення доступу до нього інших осіб. Ні за яких обставин не допускається передача носія ключової інформації (токену) та/або розголошення паролю до нього іншим особам, у тому числі співробітникам банку.
   - Носій ключової інформації, який містить чинний ключ (рухомий носій інформації, токен), повинен використовуватися тільки під час роботи у системі «Інтернет-банкінг». Носій ключової інформації (токен) не повинен залишатись приєднаним до персонального комп'ютера, якщо робота в системі призупинена чи не проводиться, персональний комп'ютер використовуються для виконання інших функцій, а також у неробочий час.
   - Пароль доступу (ПІН-код) до особистих ключів не повинен зберігатися у відкритому вигляді (наприклад, бути записаним на папері) та використовуватися для інших систем та сервісів. Персональна відповідальність за збереження паролю доступу (ПІН-коду) та унеможливлення використання носія ключової інформації іншою особою покладається виключно на користувача.
   - Необхідно періодично змінювати пароль доступу до ключа (не рідше одного разу на місяць). Пароль повинен складатися з цифр, літер верхнього та нижнього регістрів, а також спеціальних символів. При виборі паролю не повинні використовуватись комбінації, що легко вгадуються, наприклад, імена, дати народження, телефонні номери тощо.
   - У разі звільнення користувачів або переведення їх на посади, які не передбачають роботу у системі «Інтернет-банкінг», необхідно негайно звернутися у банк із метою блокування їхніх ключів.
   - У разі компрометації або підозри у компрометації ключа (втрати, пошкодження носія ключової інформації, розголошення пароля або інших подій та/або дій, що призвели або можуть призвести до несанкціонованого використання ключа), необхідно терміново звернутися у банк для блокування скомпрометованого ключа з відповідним листом або по телефону, обов'язково назвавши при цьому блокувальне слово.

2) Необхідно щоденно аналізувати всі повідомлення про прийняті та неприйняті банком електронні розрахункові документи та негайно повідомляти банк про випадки несанкціонованого зарахування (перерахування) коштів!
3) На робочу станцію, з якої здійснюється доступ до системи «Інтернет-банкінг», необхідно встановити ліцензійне антивірусне програмне забезпечення, підтримувати оновлення версій, регулярно та своєчасно оновлювати антивірусні бази даних. Рекомендується до системи Інтернет-банкінгу iBank-2, компанії «Біфіт», використовувати антивірусне програмне забезпечення.
4) На робочу станцію, з якої здійснюється доступ до системи «Інтернет-Банкінг», необхідно встановити:
   - ліцензійне антишпигунське програмне забезпечення (antispyware);
   - програмний персональний мережевий екран (файервол, брендмауер)*.

* *На ринку існує низка програмних комплексів, які поєднують функції антивірусу, мережевого екрана, антишпигунського та інших програмних засобів, призначених для захисту робочих станцій*

Налаштування мережевого екрану необхідно здійснити таким чином, щоб максимально обмежити вихідний та вхідний мережевий трафік. Зокрема, рекомендується дозволити доступ тільки до ресурсів системи «Інтернет-банкінг» та інших мінімально необхідних ресурсів, наприклад, для оновлення баз вірусних сигнатур антивірусних програмних засобів, оновлення антишпигунських програмних засобів, операційної системи та іншого програмного забезпечення.

Антивірусне та антишпигунське програмне забезпечення необхідно налаштувати для моніторингу всіх подій та періодичного сканування даних, що зберігаються на жорсткому диску персонального комп'ютера, з якого здійснюється доступ до системи «Інтернет-Банкінг».

5) Необхідно регулярно та своєчасно оновлювати системне програмне забезпечення робочої станції, за допомогою якого здійснюється доступ до системи «Інтернет-банкінг», особливо операційної системи, web-браузера. Рекомендується активувати можливість автоматичного оновлення програмного забезпечення.
6) Не рекомендується встановлювати на робочі станції, через які ведеться робота з системою «Інтернет-банкінг», програмне забезпечення з ненадійних джерел (публічні бібліотеки програмного забезпечення, програми в електронних повідомленнях тощо) та здійснювати з такого комп'ютера доступ до ненадійних (незнайомих) інтернет-ресурсів.
7) Під час доступу до системи «Інтернет-банкінг» строго не рекомендується працювати в операційній системі з обліковим записом користувача, який має розширені права в операційній системі, наприклад, «Адміністратор».
8) Під час підключення до веб-сайту системи «Інтернет-банкінг» необхідно переконатися у коректній автентифікації веб-серверу системи «Інтернет-банкінг» за протоколом SSL та уникати підключень до веб-сайту системи за банерним посиланням або посиланням, отриманим електронною поштою. Рекомендується вводити адресу веб-сайту системи самостійно та додати її у закладки браузера. При доступі до веб-сайту необхідно звертати увагу на адресне поле браузера. Оскільки веб-сайт системи «Інтернет-банкінг» має справжній та дійсний сертифікат безпеки від світового Інтернет-центру сертифікації, то при вході на сайт в адресному полі браузера мають відображатися перші символи адреси https://, а не http:// (у вікні браузера може з'явитися повідомлення про те, що розпочинається перегляд сторінок через безпечне з'єднання).
9) Не рекомендується здійснювати доступ до системи «Інтернет-банкінг» через посилання, отримані електронною поштою, а також із неконтрольованих та ненадійних робочих станцій, розташованих в інтернет-кафе, готелях, офісах, інших організаціях.

10) З метою заволодіння даними автентифікації користувачів системи «Інтернет-банкінг» (особистий ключ ЕЦП та пароль доступу до нього) для їх подальшого незаконного використання, зловмисниками можуть здійснюватись атаки на робочі станції користувачів. Основні методи заволодіння ключовою інформацією:

- розсилання користувачам підроблених електронних листів із посиланням на адресу веб-сайту, що маскується під банківський;
- розповсюдження через електронні листи чи веб-сайти програмного забезпечення із зловмисним кодом (тобто програмного вірусу) для заволодіння даними автентифікації користувача;
- несанкціоноване дистанційне управління персональним комп'ютером користувача шляхом віддаленого доступу.

Для запобігання подібних ситуацій необхідно знати, що банк ніколи та за жодних обставин не здійснює розсилку електронних листів із вимогою надіслати ключ, 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 листом або по телефону. 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.

11) При проведенні налаштування робочої станції, з якої здійснюється доступ до системи «Інтернет-банкінг», стороннім спеціалістом, рекомендується забезпечити контроль за його діями.