Використані скорочення:

«Eurobank 24/7» (Система) - система електронного банкінгу «Eurobank 24/7».

Банк – ПАТ КБ «ЄВРОБАНК».

Клієнт - юридична або фізична особа - клієнт банку, який експлуатує систему «Eurobank 24/7».

1. Загальні рекомендації при роботі з системою при виявленні або підозрі на виявлення загроз.

У разі підозр виникнення наступних ситуацій при роботі з системою:

- Розбіжності санкціонованих клієнтом операцій з даними по рахунку, наданими банком (підозра на несанкціоноване управління рахунком);
- Підозрі на компрометацію пароля та/або секретного ключа;
- Виявлення листів від Банку з проханнями відвідати вкладені в лист гіперпосилання або проханнями ввести пароль та/або надати іншу конфіденційну інформацію.

Клієнту рекомендується виконати наступні дії:

1. Негайно розірвати з'єднання комп’ютера з мережею Інтернет, локальною, бездротовою і будь-якою іншою мережею (фізично відключити мережевий кабель або кабель модему від системного блоку/ноутбука, bluetooth-адаптер, Wi-Fi і т.п.).
2. Негайно зв'язатися з співробітниками Контакт-Центру Банку (+380-44-584-2222 або безкоштовний номер для дзвінків зі стаціонарних телефонів по Україні 0-800-600-800) і звернутися в обслуговуюче відділення Банку, виклавши суть виниклих підозр.
3. Надати співробітникам банку якнайповнішу інформацію, суть проблеми і за яких обставин вона виникла, які дії проводилися з комп’ютером.
4. У разі підтвердження підозр на несанкціоноване управління рахунком (списання) підготувати і терміново доставити лист в Банк з описом проблеми, що склалася і заяву в правоохоронні органи.
5. Не підключаючи комп'ютер до мережі Інтернет, локальної або бездротової мережі, перевірити комп’ютер на предмет наявності / відсутності вірусів та іншого шкідливого програмного забезпечення. Один із способів - використання безкоштовної утиліти DrWeb CureIT, для цього необхідно попередньо завантажити з Інтернету (http://www.freedrweb.com/) свіжу версію утиліти за допомогою іншого комп’ютера (якщо інший комп’ютер відсутній - у Інтернет-кафе, комп'ютерному клубі, будь-яким іншим доступним шляхом) і скопіювати утиліту на комп’ютер з Системою за допомогою зовнішнього носія (наприклад, USB-накопичувач або компакт-диск). Перед копіюванням утиліти зовнішній носій слід перевірити за допомогою вищевказаної утиліти.
6. Якщо перевірка не виявить вірусів і шкідливого програмного забезпечення - підключити комп’ютер до мережі Інтернет та негайно оновити антивірусну базу встановленого антивірусного програмного забезпечення.
7. Не починати роботу з Системою до тих пір, поки не переконаєтеся у відсутності загрози, а в разі несанкціонованого керування рахунком вимкнути комп'ютер і нікого не підпускати до нього до прибуття співробітників правоохоронних органів.
8. Не використовуйте носій з секретними ключами до тих пір, поки не переконаєтеся у відсутності загрози.
9. Коли переконаєтеся у відсутності загроз і почнете використовувати Систему, відразу згенеруйте нові секретні ключі, обов'язково змінивши пароль.

10. Продовжувати використання Системи лише після того, як переконаєтеся, що комп’ютер не містить вірусів та/або шкідливого програмного забезпечення, залишки на Ваших рахунках не змінилися і ключова інформація не скомпрометована, або Вами проведена перегенерація ключа (ключів).
11. При подальшому використанні Системи контролювати регулярність оновлень антивірусного програмного забезпечення і залишки грошових коштів на Ваших рахунках.

Увага! Кожен клієнт зобов'язаний обмежити доступ третіх осіб до ключової інформації і паролів. Ключова інформація повинна зберігатися на зовнішніх носіях (наприклад, флеш-картах, дискетах тощо) в недоступних іншим особам місцях (наприклад: сейф, тумби що закриваються і т.п.).

2. Рекомендації по дотриманню заходів інформаційної безпеки.

В цілях захисту своїх конфіденційних даних рекомендується дотримуватись таких заходів безпеки:

1. Вимоги до налаштувань системи і програмного забезпечення (ПЗ):

- використовувати виключно легальне (ліцензійне) ПЗ;
- заборонити використання будь-яких служб і засобів віддаленого управління комп’ютером (наприклад, бездротова настройка, служба терміналів, Telnet, диспетчер сеансу довідки для віддаленого робочого столу, віддалений реєстр і т.п.);
- налаштувати і запустити в роботу програмні засоби обмеження доступу;
- термін дії пароля облікового запису не повинен перевищувати 30 днів;
- пароль повинен задовольняти рекомендаціям, викладеним нижче;
- користувач не повинен працювати під технологічними обліковими записами (Адміністратор і т.п.);
- повинні бути запущені служби контролю безпеки (журнали доступу, запуску додатків і т.п.).

2. Вимоги до ПЗ:

- на комп'ютері необхідно використовувати тільки ліцензійне антивірусне ПЗ, необхідно проводити своєчасне оновлення такого ПЗ і оновлення антивірусних баз;
- на комп'ютері не повинно бути встановлено / запускатися ігрове і розважальне ПЗ;
- не допускати установки неліцензійного ПЗ, своєчасно проводити оновлення ПЗ;
- не рекомендується використання інтернет-пейджерів (на приклад ICQ, Miranda тощо) з можливістю передачі / прийняття файлів.

3. Загальні рекомендації:

- рекомендується використання ліцензійного / легального (законно придбаного для використання) міжмережевого екрану (firewall);
- неприпустимо використання комп’ютера для відвідування розважальних сайтів (непристойного змісту, відео, фото, ігри і т.п.) і сайтів, які містять інформацію про способи "злому" інформаційних систем, програм, паролів і т.п.;
- неприпустимо надання доступу до робочої станції третім особам;
- неприпустима передача паролів і носіїв з ключовою інформацією третім особам, зберігання їх в доступному для третіх осіб вигляді і місці;
- неприпустимо зберігання ключової інформації в неробочий час в непристосованих для цього місцях (поза сейфів відповідальних працівників);
- неприпустимо зберігання ключової інформації в пам'яті або на жорсткому диску комп’ютера;

- неприпустимо залишати підключеним до комп’ютера носій з ключовою інформацією, якщо не проводяться операції в Системі віддаленого обслуговування або здійснюється «вихід» в мережу Інтернет;
- використання ключової інформації рекомендується враховувати у відповідних журналах (генерація, використання, зберігання);
- при генерації нового ключа необхідно провести зміну пароля доступу до нього.

3. Рекомендації щодо створення надійних (стійких) паролів.

При виборі пароля користувачеві необхідно керуватися пропонованими правилами:

- не використовувати атрибути користувача - імена та прізвища користувачів, пам'ятні дати та будь-яку іншу легкодоступну інформацію (наприклад, номери телефонів, адреси і т.п.);
- заборонено використання комбінації символів / знаків з клавішею Ctrl;
- паролі повинні складатися шляхом комбінації двох або більше слів;
- довжина пароля повинна складати не менше 8 символів;
- пароль повинен містити не менше 3-х з 4-х наступних символів - заголовні букви, прописні букви, цифри, спецсимволи;
- заборонено використовувати слова з реальних словників (наприклад, англійська, французька, японська і т.п.) і вигаданих (наприклад, ельфійський Р. Р. Толкієна і т.п.);
- пароль необхідно змінювати не рідше ніж кожні 30 календарних днів.

Увага! Пам'ятайте, що ні за яких обставин Ваш пароль не повинен бути відомий третім особам, ніхто не має права вимагати від Вас розкриття пароля, навіть співробітники Банку.