Пам’ятка з безпечного користування системою

1. Налаштування робочої станції

- Підключення до системи необхідно здійснювати тільки з надійних робочих станцій, на яких встановлено антивірусне програмне забезпечення.
- При вході в систему необхідно впевнитися, що в адресному полі веб-браузера знаходиться адреса саме системи «Райффайзен Онлайн».
- При підключенні до системи «Райффайзен Онлайн» необхідно перевірити, чи ввімкнено шифрування. Про ввімкнене шифрування свідчить наявність значка «Замок» у вікні браузера.
- Підтвердженням того, що між веб-браузером Користувача та веб-сервером Банку встановлено безпечне з’єднання, є наявність цифрового (електронного) сертифікату Банку. Важливо перевірити надійність надавача, дійсність сертифікату та термін його дії.

  Цифровой сертифікат Банку є надійний, якщо:
  - ✓ **Виданий online.aval.ua**
  - ✓ **Термін дії з 29.08.2017 до 28.11.2020**

- Робоча станція, яка використовується для роботи в системі «Райффайзен Онлайн», повинна мати:
  1. встановлену операційну систему, що регулярно оновлюється;
  2. інстальовану останню доступну версію веб-браузера;
  3. програмне забезпечення захисту, що складається з ліцензійної антивірусної системи, антишпигунського програмного забезпечення (antispyware) та програмного персонального мережевого екрана (файервол, брендмауер)*.
- На комп’ютерах зі встановленою операційною системою Windows рекомендується активувати функцію автоматичного оновлення операційної системи.
- Антивірусні бази даних та бази сигнатури антишпигунського програмного забезпечення необхідно постійно оновлювати.
- Рекомендуємо регулярно (не рідше, ніж раз на тиждень) здійснювати повне сканування робочої станції для виявлення вірусів та зловмисного програмного забезпечення.
- Не рекомендуємо встановлювати на робочу станцію програмне забезпечення із ненадійних джерел (публічні бібліотеки програмного забезпечення, програми в електронних повідомленнях тощо).

2. Політика використання паролів

- При введенні логіну та паролю переконайтесь, що за Вами ніхто не спостерігає.
- Перед тим, як змінити пароль, перевірте сертифікат безпеки банківського сервера.
- Не використовуйте функцію збереження паролів, яку може запропонувати веб-браузер.

- Логін повинен бути не менше 5-ти та не більше 30-ти символів та складатися із літер латинського алфавіту та/або цифр та/або спецсимволів, що доступні для вводу однією із клавіш стандартної клавіатури користувача персонального комп'ютера.

  Пароль повинен відповідати наступним вимогам:

  - мінімум 8 символів;
  - максимум 20 символів;
  - мінімум 1 маленька літера;
  - мінімум 1 велика літера;
  - мінімум 1 цифра;
  - мінімум 1 спеціальний знак, такий як %, @,?,*?,тощо;
  - 4-ри останні Паролі для входу не повинні співпадати;
  - термін дії Паролю для входу – 90 днів.

3. Базові правила безпеки при використанні системи «Райффайзен Онлайн»

- Після відкриття сесії перевіряйте дату останнього входу до системи та відстежуйте історію операцій в системі «Райффайзен Онлайн» за допомогою меню «Мої дії».
- Якщо Ви підключені до системи, не залишайте робочу станцію без нагляду.
- Сесія має бути закрита через посилання Вихід та закриття вікна веб-браузера.
- Якщо вхід у систему здійснюється в публічних місцях, перед закриттям вікна браузера рекомендується очистити буфер браузера та видалити тимчасові файли та cookies.
- Не переглядайте інші сайти в тому ж веб-браузері, коли працюєте у в системі «Райффайзен Онлайн».
- Стежте за тривалістю веб-сесії, яка задля безпеки обмежена десятьма хвилинами.
- Для навігації в системі використовуйте виключно посилання і кнопки системи «Райффайзен Онлайн» та не використовуйте кнопки навігації браузера (наприклад «Вперед» / «Назад»).
- Звертайте увагу на повідомлення веб-браузера про небезпеку.

4. Потенційні загрози.

- Для входу в систему «Райффайзен Онлайн» не використовуйте підключення за банерним посиланням або посиланнями, отриманими електронною поштою.
- Не відповідайте на запити (найчастіше розсилаються електронною поштою), які містять вимогу надати або перевірити логін, пароль, секретний код (PIN) тощо.

  Увага!!! Банк за жодних обставин не здійснює розсилку електронних листів із вимогою надіслати пароль, логін або перейти за вказаною електронною адресою.

- Банк не розповсюджує електронною поштою комп'ютерні програми.

- 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.
- У разі виявлення будь-якого зловмисного програмного забезпечення (віруси, троянські програми тощо) на робочій станції, необхідно здійснити вхід в систему «Райффайзен Онлайн» із гарантовано незараженої робочої станції та замінити пароль доступу до системи.

5. Виявлення проблем та шляхи їх вирішення

- При виявленні спроби несанкціонованого доступу до системи «Райффайзен Онлайн» необхідно терміново змінити пароль доступу до системи та звернутися до Інформаційного центру банку за телефоном 0 800 500 500 для отримання рекомендацій щодо подальших дій. Рекомендується також провести сканування робочої станції на виявлення вірусів та іншого зловмисного програмного забезпечення.
- У разі втрати картки ідентифікації клієнта необхідно зателефонувати до Інформаційного центру банку за телефоном 0 800 500 500 та надати розпорядження на блокування каналу «Інтернет-банкінг». Для поновлення картки необхідно звернутись у будь-яке відділення Райффайзен Банку Аваль.

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