Памятка по безопасному использованию системы

1. Настройка рабочей станции

- Подключение к системе необходимо осуществлять только из надежных рабочих станций, на которых установлено антивирусное программное обеспечение.
- При входе в систему нужно удостовериться, что в адресном поле веб-браузера указан адрес именно системы «Райффайзен Онлайн».
- При подключении к системе «Райффайзен Онлайн» необходимо проверить, включено ли шифрование. Если шифрование включено, в окне браузера появится значок «Замок».
- Подтверждением того, что между веб-браузером Пользователя и веб-сервером Банка установлено безопасное соединение, является наличие цифрового (электронного) сертификата Банка. Важно проверить надежность выданного сертификата, его действительность и срок действия.

  Цифровой сертификат Банка является надежным, если:

  - ✓ **Выдан online.aval.ua**
  - ✓ **Срок действия с 29.08.2017 по 28.11.2020**

- На рабочей станции, используемой для доступа к системе «Райффайзен Онлайн», должны быть:
  1. установленная и регулярно обновляемая операционная система;
  2. инсталлированная последняя доступная версия веб-браузера;
  3. защита программного обеспечения, состоящая из лицензированной антивирусной системы, антишпионского программного обеспечения (antispyware) и программного персонального сетевого экрана (файервол, брендмауер)*.
- На компьютерах с установленной операционной системой Windows рекомендуется активировать функцию автоматического обновления операционной системы.
- Антивирусные базы данных и базы сигнатуры антишпионского программного обеспечения необходимо постоянно обновлять.
- Советуем регулярно (не реже, чем раз в неделю) осуществлять полное сканирование рабочей станции для выявления вирусов и вредоносного программного обеспечения.
- Не советуем устанавливать на рабочую станцию программное обеспечение из ненадежных источников (публичные библиотеки программного обеспечения, программы в электронных сообщениях и т.д.).

2. Политика пользования паролями

- При вводе логина и пароля убедитесь, что за Вами никто не наблюдает.
- Перед тем, как поменять пароль, проверьте сертификат безопасности банковского сервера.
- Не пользуйтесь функцией сохранения паролей, которую может предложить веб-браузер.
- Логин должен быть не менее 5-ти и не более 30-ти символов и состоять из букв латинского алфавита и / или цифр и / или спецсимволов, доступные для ввода одной из клавиш стандартной клавиатуры пользователя персонального компьютера.
  Пароль должен отвечать следующим требованиям:
  - минимум 8 символов;
  - не более 20;
  - минимум 1 маленькая буква;
  - минимум 1 большая буква;
  - минимум 1 цифра;
  - минимум 1 специальный знак, такой как% @,?, * ?, и тому подобное;
  - 4-х последних Пароли для входа не должны совпадать;
  - срок действия пароля для входа - 90 дней.

3. Базовые правила безопасности при пользовании системой «Райффайзен Онлайн»

- После открытия сессии проверяйте дату последнего входа в систему и отслеживайте историю операций в системе «Райффайзен Онлайн» с помощью меню «Мои действия».
- Если Вы подключены к системе, не оставляйте рабочую станцию без присмотра.
- Сессию надо завершать через ссылку «Выход» и закрытие окна веб-браузера.
- Если вход в систему осуществляется в публичных местах, перед закрытием окна браузера рекомендуется очистить буфер браузера и удалить временные файлы и cookies.
- Не просматривайте другие сайты в том же веб-браузере, когда работаете в системе «Райффайзен Онлайн».
- Следите за продолжительностью веб-сессии, которая для безопасности ограничена десятью минутами.
- Для навигации в системе пользуйтесь исключительно ссылками и кнопками системы «Райффайзен Онлайн» и не пользуйтесь кнопками навигации браузера (к примеру, «Вперед» / «Назад»).
- Обращайте внимание на сообщения веб-браузера об опасности.

4. Потенциальные угрозы.

- Для входа в систему «Райффайзен Онлайн» не используйте подключение по баннерным ссылкам либо ссылкам, полученным по электронной почте.
- Не отвечайте на запросы (чаще всего рассылаются через электронную почту), содержащие требование предоставить или проверить логин, пароль, секретный код (PIN) и др.

Внимание!!! Банк ни при каких обстоятельствах не рассылает электронные письма с требованием прислать пароль, логин или перейти по указанному электронному адресу.

- Банк не распространяет через электронную почту компьютерные программы.
- Рекомендуется удалять подозрительные электронные письма, не открывая их, особенно письма от неизвестных отправителей с прикрепленными файлами с расширениями *.exe, *.pif, *.vbs и другие файлы.
- В случае выявления любого вредоносного программного обеспечения (вирусы, троянские программы и прочее) на рабочей станции, необходимо осуществить вход в систему «Райффайзен Онлайн» из гарантированно незараженной рабочей станции и поменять пароль доступа к системе.

5. Обнаружение проблем и пути их решения

- При обнаружении попытки несанкционированного доступа к системе «Райффайзен Онлайн» необходимо как можно быстрее поменять пароль доступа к системе и обратиться в Информационный центр банка по телефону 0 800 500 500 для получения рекомендаций относительно дальнейших действий. Рекомендуем также провести сканирование рабочей станции для выявления вирусов и другого вредоносного программного обеспечения.
- В случае утери карты идентификации клиента необходимо позвонить в Информационный центр банка по телефону 0 800 500 500 и дать распоряжение на блокирование канала «Интернет-банкинг». Для восстановления карты обратитесь в любое отделение Райффайзен Банка Аваль.

* На рынке существует ряд программных комплексов, объединяющих функции антивируса, сетевого экрана, антишпионского и других программных средств, предназначенных для защиты рабочих станций