Безопасность интернет подключения и интернет банкинга

Системы онлайн банкинга - это безопасный и удобный способ дистанционного управления банковским счётом. Но пользователи должны осознавать, что кибер-мошенники могут получить несанкционированный доступ к онлайн-банкингу. Обычно это происходит путем получения доступа к паролю, имени пользователя, и к другой конфиденциальной информации (например, ПИН кодам и т.н. секретным вопросам).

Безопасность интернет банкинга

Несколько полезных советов по безопасности

- Никогда не вводите Ваши личные данные (имя пользователя) на веб странице, переход на которую произошёл по ссылке из электронного письма, даже в том случае, если электронное письмо выглядит как аутентичное письмо, полученное из ФИНКА Банка. Всегда вводите адрес страницы самостоятельно, непосредственно в адресную строку браузера.

- Безопасность веб-станицы интернет банкинга обеспечивается механизмом шифрации данных. Следовательно, когда вы находитесь на защищенной странице, вы должны видеть логотип «закрытый замочек» в адресной строке браузера. При этом аутентичность сертификата можно проверить просто - нажав на изображение «закрытый замочек». При переходе на защищенный сайт протокол ‘http’ должен измениться на ‘https’

- С осторожностью относитесь к «всплывающим» окнам, особенно если они появляются во время вашей работе в системе интернет банкинга.

- Ни при каких обстоятельствах не делитесь Вашими личными данными с третьими лицами по средствам телефонного разговора, или электронного письма. Помните, что ФИНКА Банк никогда не запрашивает конфиденциальные данные через такие каналы общения.

- Часто злоумышленники вводят в заблуждение пользователей, требуя от имени банка проведения «тестовой транзакции». ФИНКА Банк никогда не требует от клиентов проведения т.н. «тестовых», или каких-либо транзакций по телефону, или с помощью электронного письма.

- регулярно проверяете выписки ваших счетов, и в случае обнаружения подозрительной, или несанкционированной операции незамедлительно сообщите об этом ФИНКА Банку.

- Перед тем, как завершить операцию, перепроверьте сумму операции и реквизиты получателя платежа.

- В обязательном порядке установите и регулярно обновляйте антивирусное программное обеспечение на вашем персональном компьютере. Хотя это может показаться сложной технической задачей, попытайтесь настроить безопасность браузера. Дополнительную информацию можно найти по ссылке https://www.us-cert.gov/publications/securing-your-web-browser#why

- Банки используют различные механизмы и дополнительные устройства, для того, чтобы удостовериться в аутентичности пользователя, который совершает удаленную операция с помощью интернет банкинга. ФИНКА Банк внедрил систему проверки аутентичности с помощью одноразовых СМС кодов, которые высылаться на номер мобильного, который был указан клиентом при регистрации услуги. СМС код вводится как дополнительный механизм безопасности при совершении клиентом определенных типов операций. Этот механизм так же известен под названием двухфакторная аутентификация. Никогда не используете при авторизации операции код, который был получен не от ФИНКА Банка.

- Удостоверьтесь в том, что банк владеет вашей обновленной контактной информацией, в особенности номером мобильного телефона. При проведении операций рекомендовано использовать номер телефона, который принадлежит вам.

Точки доступа wi-fi

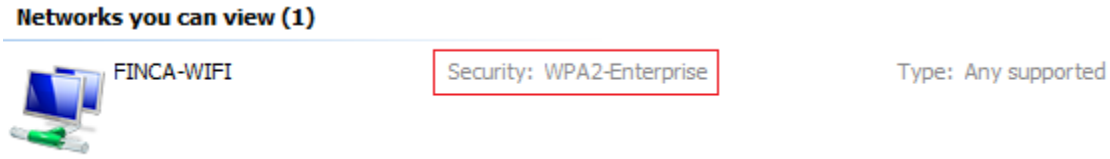
При использовании интернет и мобайл банкинга, надо с особой осторожностью относиться к точкам доступа wi-fi. Помните, что несмотря на то, что wi-fi, несомненно, являются очень удобным способом доступа в интернет, они могут стать источником утечки вашей конфиденциальной информации. Мы рекомендуем не пользоваться точками общего доступа при работе с интернет и мобайл банкингом.

В случае, если это является крайней необходимостью и не удается отказаться от использования, мы рекомендуем соблюдать следующие правила безопасности.

Если есть возможность подключения к нескольким точкам, выберите СРАВНИТЕЛЬНО безопасную точку следующим образом:

- в первую очередь попытайтесь подключиться к соединению, использующим шифрацию WPA2, а уж потом WAP
- не используйте WEP, так как - это самый опасный способ открытой передачи данных через Wi-fi соединение.

После подключения к Wi-fi сети, обычно операционная система устройства требует указать к какой категории отнести сеть. Если предоставляется возможность Wi-fi соединение должно быть отнесено Вами к категории Public Network. При этом по умолчания выставляются настройки операционной системы, защищающие данные в сети Wi-fi.



- Помните, если вы регулярно пользуетесь wi-fi сетями, в особенности сетями общего доступа, для работы с системами онлайн банкинга, мы настоятельно рекомендуем использовать VPN клиент. VPN клиент – это специальное программное обеспечение, которое обеспечивает доступ с системе онлайн банкинга через защищенный канал. VPN клиенты доступны как для персональных компьютеров, так и для мобильных устройств.