Уважаемые клиенты Банка!

ДО АО Банк ВТБ (Казахстан) напоминает Вам о необходимости соблюдения обязательных требований для безопасной работы в системах дистанционного банковского обслуживания Интернет-Банк «VTB Online-Banking» (далее – ДБО).

Основные правила безопасной работы с ДБО.

- Безопасно хранить ключи ЭЦП, использовать только при необходимости и извлекать их по окончании сеанса.
- Не допускать использование простых паролей (123456, qwerty и подобных).
- Не назначать пароль, используемый в системе ДБО, в любых других системах и сервисах.
- Не сообщайте логин и/или пароль кому-либо, в том числе ИТ-специалистам компании, обслуживающих систему от Банка и т.д. для проверки работы системы, настроек взаимодействия с Банком и т.п.
- На компьютере с ДБО не должно быть установлено программ, не являющихся необходимыми на данном рабочем месте.
- Пользователь не должен работать с правами Администратора.
- Не записывайте пароли на бумажных носителях с открытым хранением (на столах, в выдвижных шкафах тумбочек и т.д.) или в текстовых файлах на компьютерах, в случае необходимости храните пароли в защищенных сейфах, на защищенных носителях с наличием доступа только Вам.
- Не оставлять включенным сеанс ДБО сверх необходимого времени.
- На компьютере с системами ДБО необходимо ограничить работу в сети Интернет минимальным необходимым количеством сайтов.
- Не использовать на компьютере с ДБО средств удаленного доступа и администрирования.
- Доступ к ресурсам компьютера с системами ДБО из локальной сети должен быть закрыт, папок общего доступа быть не должно.
- На компьютере с системами ДБО желательно не использовать сеть Wi-Fi. В случае необходимости – устанавливать максимально возможный уровень защиты сети.
- Не допускать использования социальных сетей.
- Использовать только корпоративную почту через почтового клиента с использованием СПАМ фильтра с жестким ограничением.
- Доступ к ресурсам сети Интернет должен быть ограничен фиксированным списком доверенных сайтов, не допускать использование месседжеров типа ICQ, Skype и др.
- Отключить службы сервера, удаленного доступа и др. ПО связанные с удаленным администрированием.
- Должны быть установлены все актуальные обновления безопасности Windows
- Антивирусная защита должна включать, кроме обычных функций, модули проверки почты, входящего http трафика, Брандмауер, СПАМ фильтр и обновляться не реже одного раза в час. Желательно использовать Централизованное управление антивирусной защитой. Пользователь ДБО должен быть лишен возможности управления антивирусной защитой и возможности её отключения.
- Поддерживать систему антивирусной защиты в работоспособном и актуальном состоянии.

- Не пользоваться ДБО в случае возникновения проблем с антивирусной защитой.
- Не пользоваться ДБО при повторяющихся сбоях в работе компьютера.
- Не предоставляйте никому Вашу персональную информацию, Банк **никогда не запросит** имя пользователя и пароль, ответы на кодовые и контрольные вопросы **по электронной почте, телефону или sms.**
- Банк никогда не направит Вам с каких либо внешних интернет ресурсов и почтовых систем файлы обновления либо оптимизации работы Интернет банкинга, ключевую информацию и любое другое программное обеспечение, не принимайте и не инсталлируйте любое вышеуказанное и стороннее программное обеспечение. (***Например, рассылка от имени банков писем по электронной почте с требованием (под разными предлогами) перейти по предлагаемой ссылке, скачать и установить ПО оптимизирующее/обновляющее Банк-Клиент и т.д.)***

Успеху злоумышленников способствует пренебрежение пользователями вышеуказанных элементарных правил безопасной работы с системами ДБО.

При работе с системой ДБО следует исходить из соображений, что данный сервис должен функционировать абсолютно бесперебойно, поэтому всякое отклонение от нормальной работы следует воспринимать как сигнал тревоги.

Дополнительные мероприятия:

В случае если требования безопасности не могут быть выполнены в полном объеме на компьютере бухгалтера, необходимо взвесить риски и, возможно, принять решение о выделении отдельного компьютера для работы с ДБО.

Учитывая тот факт, что **работники бухгалтерий** не являются специалистами в области информационной безопасности, они бывают недостаточно информированы о рисках и могут недооценивать необходимость дополнительных мероприятий по защите систем ДБО. Поэтому **разъяснение правил безопасной работы является одним из важнейших составляющих общей системы безопасности**.

Для повышения уровня ответственности и дисциплины, общие правила безопасной работы с ДБО следует оформить соответствующим приказом руководителя предприятия.

На что следует обращать внимание?

- необычно медленная работа компьютера, зависания во время сеансов ДБО или при попытке входа, произвольная перезагрузка.
- перебои с доступом в систему ДБО.
- невозможность авторизации в системе ДБО.
- несоответствие порядковых номеров платежных поручений.
- попытки авторизации в ДБО с других IP-адресов или в нерабочее время.
- неоднократное удаление антивирусным монитором одного и того же вируса.
- выход из строя ПК, на котором установлена система ДБО.
- DDoS-атака на вашу ИТ-инфраструктуру.

Если Вы не можете войти в систему ДБО в течении 5- 10 минут, обязательно свяжитесь с банком и установите источник проблемы (в банке или в вашей сети). Если проблема в вашем оборудовании или ПО и Вы не можете её быстро разрешить или локализовать,

обязательно свяжитесь с банком, **проверьте последние отправленные поручения и сообщите сотрудникам банка об имеющихся проблемах.**

В случае обнаружения факта (или попытки) мошенничества:

1. **Необходимо максимально быстро сообщить о происшествии в Банк с целью остановки платежа и блокирования доступа к системе ДБО**.
2. Компьютер с системой ДБО необходимо выключить. Если в компании имеется межсетевой экран или прокси-сервер, на котором ведутся логи, то необходимо сохранить их в электронном виде и распечатать на бумажном носителе. В случае проведения самостоятельного расследования или привлечения для этих целей консультантов, следует иметь в виду, что работа с оригиналами носителей информации может повредить целостности доказательств, хранящихся на них.
3. Даже если мошенничество не было завершено, и Вы успели остановить его, **инцидент остается уголовным преступлением,** которое попадает под ряд статей, начиная с создания и распространения вредоносного программного обеспечения и заканчивая попыткой хищения в особо крупном размере. Поэтому следует обязательно написать заявление в правоохранительные органы с требованием возбудить уголовное дело.