Настоящие правила и рекомендации по безопасности работы с Системой «Internet Banking» (далее – Система) разработаны на основе опыта зарубежных банков и компаний. Данные правила приводят описание практических примеров-схем действий злоумышленников, направленных на получение несанкционированного доступа к счетам компаний.

Примите к сведению, что нижеописанные случаи мошенничества не имели места в работе АО «First Heartland Bank». Целью данных правил является предостережение клиентов от всевозможных случаев мошенничества, над которыми банк не имеет прямого контроля, при которых крайне важна осведомленность клиентов и сохранение их бдительности.

Обращаем Ваше внимание, что система удаленного банковского обслуживания на опыте зарубежных компаний зарекомендовала себя как наиболее надежный и безопасный способ работы с банком по сравнению с обменом информацией на бумажных носителях.

ПРАВИЛО №1. Ни при каких обстоятельствах НЕ РАЗГЛАШАТЬ ПАРОЛИ ДОСТУПА к Системе «Internet Banking».

Пароли являются конфиденциальной информацией и должны быть известны только лицу, для которого банком создан логин для доступа в Систему. Пароль для доступа в Систему должен быть не менее 8 символов, содержать буквы, цифры и специальные символы.

Запрещается использование автозаполнения и сохранение паролей и пользовательских данных в веб-браузере (необходимо отказаться при предложении программы Internet Explorer сохранить данные на используемом компьютере).

ПРАВИЛО №2. Ни при каких обстоятельствах НЕ ПЕРЕДАВАТЬ СЕРТИФИКАТ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ другому лицу, предпринимать все меры для предотвращения его несанкционированного копирования!

Сертификат электронной цифровой подписи (ЭЦП) должен быть доступен только владельцу сертификата и/или лицу, уполномоченному на пользование сертификатом в соответствии с законодательством Республики Казахстан.

Для предотвращения копирования Сертификата ЭЦП необходимо соблюдать следующие правила:

использовать Сертификат ЭЦП только в момент подписания платежных документов в Системе;

не хранить Сертификат ЭЦП в общедоступных местах;

не передавать Сертификат ЭЦП посторонним лицам;

строго запрещается использование Сертификатов ЭЦП на общедоступных персональных компьютерах (например, в интернет-кафе).

Возможные схемы действия злоумышленников с целью получить логин и пароль к Системе «Internet Banking», Сертификат ЭЦП:

Вариант 1.

Злоумышленник, представившись сотрудником Банка или уполномоченного органа, звонит сотруднику компании, имеющему доступ для работы с Системой «Internet Banking», сославшись на техническую проблему в системе или под любым другим предлогом, просит назвать логин и пароль для доступа к Системе «Internet Banking».

На что обратить внимание:

А) Сотрудник Банк никогда не будет требовать от Вас предоставить Ваш пароль к Системе. Для решения технических или иных проблем в Системе сотруднику Банка не нужно знать Ваш личный пароль.

Б) Знаете ли Вы этого сотрудника Банка, узнаете ли его голос?

В) Если на Вашем телефоне есть определитель номера – запишите с какого телефона звонит сотрудник Банка.

Какие должны быть Ваши действия:

А) Ни при каких обстоятельствах не называть свой пароль к Системе; Б) По возможности запомнить или записать ФИО звонившего сотрудника, номер телефона, с которого он звонил;

В) Немедленно позвонить в Банк по телефонам: в г. Алматы (727) 2581505 и сообщить о таком случае.

Вариант 2.

На Ваш электронный адрес (e-mail) приходит сообщение от сотрудника банка, администратора Системы или сотрудника уполномоченного органа. Под каким-либо предлогом отправитель просит в ответ на данное сообщение отправить логин и пароль к Системе. При этом электронный адрес отправителя может выглядеть как настоящий, принадлежащий банку, например administrator@fhb.kz (может быть сфальсифицирован).

На что обратить внимание:

А) Сотрудник Банк никогда не будет требовать от Вас предоставить Ваш пароль к Системе. Для решения технических или иных проблем в Системе сотруднику Банка не нужно знать Ваш личный пароль.

Б) Знаете ли Вы сотрудника Банка, подпись которого стоит в сообщении; указаны ли обратные контакты сотрудника Банка.

В) Если нажать кнопку «Ответить» на данное письмо, какой отобразится адрес получателя в поле «Кому» (при ответе на сообщение, возможно, будет отображен реальный адрес отправителя).

Какие должны быть Ваши действия:

А) Ни при каких обстоятельствах не называть свой пароль к Системе; Б) По возможности запомнить или записать ФИО звонившего сотрудника, номер телефона, с которого он звонил;

В) Немедленно позвонить в Банк по телефонам: в г. Алматы (727) 2581505 и сообщить о таком случае.

ПРАВИЛО №3. Производить вход и использование Системы «Internet Banking» только посредством веб-сайта https://online.fhb.kz/ или https://online1.fhb.kz/

При использовании Системы обращайте внимание на адрес веб-сайта, указанный в адресной строке Вашего браузера. В случае, если Вы заметили, что адрес веб-сайта в адресной строке браузера изменился, не вводите Ваш логин и пароль, немедленно закройте данный сайт и обратитесь в Банк.

В случае если Банк действительно изменил веб-адрес Системы «Internet Banking» Вы обязательно получите официальное письмо от Банка об изменении адреса, также такая информация будет размещена на главном сайте Банка http://fhb.kz/

Возможные схемы мошенничества с использованием поддельного веб-сайта

Вариант 3.

Вы получаете уведомление по телефону или e-mail об изменении адреса веб-сайта банка, посредством которого осуществляется вход в Систему «Internet Banking». При этом электронный адрес отправителя сообщения может выглядеть как настоящий, принадлежащий банку, например administrator@fhb.kz (может быть сфальсифицирован).

На что обратить внимание:

А) Знаете ли Вы этого сотрудника Банка, узнаете ли его голос? (если получен звонок).

Б) Если на Вашем телефоне есть определитель номера – с какого телефона звонит сотрудник Банка (если получен звонок).

В) Указаны ли обратные контакты сотрудника Банка (если уведомление по e-mail).

Г) Если нажать кнопку «Ответить» на данное письмо, какой отобразится адрес получателя в поле «Кому» (при ответе на сообщение, возможно, будет отображен реальный адрес отправителя).

Какие должны быть Ваши действия:

А) Если не получено официальное уведомление/подтверждение от Банка об изменении адреса веб-сайта Системы, ни в коем случае не заходить на указанный посторонними лицами сайт и тем более не вводить на неизвестном сайте логин и пароль к Системе «Internet Banking».

Б) При получении уведомления от Банка об изменении адреса веб-сайта Системы «Internet Banking» Вам необходимо самостоятельно связаться с Банком и подтвердить полученную информацию.

В) При возникновении подобных случаев или сомнениях в подлинности сайта, немедленно позвонить в Банк по телефонам: в г. Алматы (727) 2581505 и сообщить о таком случае.

Вариант 4.

При входе на сайт Системы «Internet Banking» https://online.fhb.kz/ или https://online1.fhb.kz/ адрес веб-сайта автоматически изменяется на другой. При этом на Вашем компьютере может появиться предупреждение о несоответствии сертификата веб-сайта.

На что обратить внимание:

А) При использовании Системы обращайте внимание на адрес веб-сайта, указанный в адресной строке Вашего браузера. В) При использовании Системы обращайте внимание на любые расхождения в оформлении или порядке входа в Систему (по сравнению с тем, как Системы выглядела или функционировала ранее).

Какие должны быть Ваши действия:

А) Не вводите Ваш логин и пароль к Системе, в случае если у Вас появились малейшие сомнения в его подлинности. Б) Немедленно закройте данный сайт.

В) Немедленно позвоните в Банк по телефонам: в г. Алматы (727) 2581505 и сообщите о таком случае.

ПРАВИЛО №4. В случае рассекречивания Вашего пароля к Системе «Internet Banking», утери/утраты Сертификата ЭЦП или его несанкционированного копирования, подозрений на несанкционированное использование Системы и/или Сертификата ЭЦП, а также в других случаях, которые могут привести к несанкционированному доступу к счетам Вашей компании, необходимо незамедлительно уведомить об этом Банк по телефонам: в г. Алматы (727) 2581505.

ПРАВИЛО №5. Не сохранять на компьютере и не устанавливать файлы или программы, полученные по электронной почте от неизвестных лиц.

Файлы, полученные от злоумышленников, могут содержать вирусы или программы, действие которых направлено на получение Ваших логинов и паролей доступа, получение сертификатов ЭЦП.

Возможные схемы действия злоумышленников с целью получить логин и пароль к системе «Internet Banking», сертификат электронной цифровой подписи

Вариант 5.

Вы получаете на e-mail сообщение с вложенным файлом от неизвестного лица , которое может представиться сотрудником Банка. Ссылаясь на обновление Системы «Internet Banking», помощь в решении технических проблем или под другим предлогом отправитель просит Вас сохранить или установить вложенный файл или программу. При этом электронный адрес отправителя сообщения может выглядеть как настоящий, принадлежащий банку, например administrator@fhb.kz (может быть сфальсифицирован).

На что обратить внимание:

А) Знаете ли Вы сотрудника Банка, подпись которого стоит в сообщении; указаны ли обратные контакты сотрудника Банка.

В) Если нажать кнопку «Ответить» на данное письмо, какой отобразится адрес получателя в поле «Кому» (при ответе на сообщение, возможно, будет отображен реальный адрес отправителя).

Какие должны быть Ваши действия:

А) Не сохранять и не устанавливать файлы и программы, полученные от неизвестных лиц, в том числе подозрительных сотрудников Банка.

В) Позвонить в Банк по телефонам: в г. Алматы (727), сообщить о таком случае и подтвердить, что данное сообщение было действительно отправлено сотрудником Банка.

Вышеописанные возможные схемы мошенничества и схемы действия злоумышленников не являются исчерпывающими. Банк будет прилагать все усилия для своевременного распространения информации о новых ухищрениях злоумышленников. Тем не менее, Вам необходимо обращать внимание на все подозрительные случаи, сохранять бдительность и при возникновении таких случаев немедленно обращаться в Банк по телефонам: в г. Алматы (727) 2581505.