ПАМЯТКА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ПРИ РАБОТЕ С СИСТЕМОЙ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСУЛЖИВАНИЯ
АО "TENGRI BANK"

2016

Уважаемые клиенты Tengri Bank!

В последние годы отмечается значительный рост попыток мошенничества в киберпространстве, нацеленных на клиентов финансовых организаций, а сами мошеннические схемы становятся все более изощренными.

Необходимо четко осознавать, что при дистанционном взаимодействии между Клиентом и Банком, защищенность всецело зависит от усилий обеих сторон и должна обеспечиваться обоюдно. Самые совершенные средства защиты могут оказаться бессильными, если пренебрегать элементарными мерами безопасности.

При этом, как правило, злоумышленники направляют свои усилия не на атаку защищенных систем банка, а пытаются воздействовать на клиента в расчете на то, что уровень защиты на стороне клиента окажется существенно ниже или защитные меры со стороны клиента, будут и вовсе отсутствовать.

Tengri Bank подготовил для вас эту памятку для того чтобы помочь нашим клиентам:

- лучше понимать актуальные угрозы и риски, которые несут клиенты при использовании систем дистанционного банковского обслуживания;
- уметь идентифицировать типичные приемы неправомерного получения злоумышленниками конфиденциальной информации;
- распознавать ситуации и случаи повышенного риска;
- обеспечить требуемый уровень безопасности и комфорта при использовании системы ДБО.

МЫ НАСТОЯТЕЛЬНО РЕКОМЕНДУЕМ ВАМ ВНИМАТЕЛЬНО ОЗНАКОМИТЬСЯ С ДАННОЙ ПАМЯТКОЙ, И НЕУКЛОННО СЛЕДОВАТЬ НАШИМ РЕКОМЕНДАЦИЯМ ПРИ РАБОТЕ С СИСТЕМОЙ ДБО.

1. ТИПИЧНЫЕ ПРИЕМЫ ЗЛОУМЫШЛЕННИКОВ В МОШЕННИЧЕСКИХ СХЕМАХ С СИСТЕМАМИ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ (ДБО) И ИХ ХАРАКТЕРНЫЕ ПРИЗНАКИ

Действия злоумышленников нацелены на завладение конфиденциальной информацией клиента – например, паролями, кодовыми фразами, персональными ключами и т.п. В случае успеха злоумышленники рассчитывают на дальнейшее использование полученной информации, в том числе, для попыток направления Банку распоряжений от имени клиента.

Для этого мошенники пытаются использовать различные способы и каналы воздействия на клиента и их комбинации.

Сообщения электронной почты

Злоумышленники часто используют в своих схемах поддельные сообщения электронной почты (email). Наиболее простой способ – это массовые рассылки под видом рекламы (так называемый спам). Опасность заключается в том, что перейдя по ссылке, размещенной в таком сообщении, пользователь рискует оказаться на веб-сайте, нацеленном на распространение компьютерных вирусов и других видов злонамеренного программного обеспечения. В случае успешного заражения компьютера пользователя вирусы могут незаметно для пользователя собирать, перехватывать и сообщать злоумышленникам конфиденциальную информацию, например – пароли.

Более изощренным и опасным видом злонамеренного использования электронной почты является имитация сообщений Банка. Пытаясь сделать поддельное сообщение максимально похожим на настоящее, злоумышленники могут прибегать к использованию корпоративных логотипов, подделке электронного адреса отправителя и тому подобным уловкам.

В этом случае, как правило, злоумышленники ставят своей целью под разными предлогами заманить клиента на поддельный сайт-ловушку, имитирующий настоящий сайт Банка, и побудить клиента совершить действия, которые приведут к раскрытию конфиденциальной информации, например, ввести свой пароль для входа в систему ДБО, номер своего мобильного телефона и т.п.

Наиболее характерные признаки того, что сообщение электронной почты является поддельным:

- Содержание сообщения побуждает Вас предпринять срочные действия, что может также подчеркиваться возможностью наступления негативных событий в противном случае. Предлоги могут быть разнообразными – возможная блокировка счета, обнаружение несанкционированной операции по Вашему счету, необходимость установить «срочное обновление», подтвердить в системе свои данные в связи с «восстановлением системы после сбоя» и тому подобное;
- В сообщении указана веб-ссылка, якобы ведущая на сайт системы Банка, которой просят воспользоваться для входа в систему ДБО. Если клиент попытается перейти по такой ссылке, то может оказаться на фальшивом сайте, имитирующем

настоящий сайт Банка, или может открыться всплывающее окно, в котором клиента будут запрашивать ввести или
«подтвердить» свою конфиденциальную информацию для входа в систему;

- В теме и/или теле сообщения возможны опечатки, искажение написания слов, сливающиеся или, наоборот, разорванные на части слова. Такие уловки могут предприниматься злоумышленниками чтобы обойти автоматизированные системы распознавания и противодействия спам-почте.

В подлинных сообщениях электронной почты от АО «Tengri Bank»:

- никогда не указывает ссылку для входа в систему ДБО и не просит Вас войти в систему по ссылке в почтовом сообщении;
- не запрашивает сообщить, обновить или подтвердить Вашу конфиденциальную информацию, включая пароли для входа в систему ДБО, кодовые фразы, номер мобильного телефона или его модель и т.п.

SMS-сообщения

Подобно сообщениям электронной почты, злоумышленники могут пытаться побудить клиента к действиям, направленным на раскрытие конфиденциальной информации клиента, отправляя клиенту поддельные SMS-сообщения. Такие SMS-сообщения могут достаточно близко имитировать аутентичные сообщения Банка, но следующие характерные признаки помогут Вам отличить поддельные сообщения в случае их получения:

- Содержание сообщения побуждает Вас предпринять срочные действия
- В SMS-сообщении содержится просьба установить какое-либо дополнительное программное обеспечение, «обновление безопасности» и т.п. на Ваш смартфон и приводится веб-ссылка для выполнения такого действия. Переход по такой ссылке может привести к заражению Вашего смартфона специально сконструированным вирусом, который затем может подавлять отображение подлинных SMS-сообщений от Банка, а направляемую Банком в SMS сообщениях конфиденциальную информацию (например, пароли для осуществления операций) будет незаметно пересылать злоумышленникам;
- веб-ссылка для входа систему ДБО и просьба выполнить вход в систему;
- SMS-сообщение поступило Вам с неизвестного номера, а не с официального номера Банка.

Если в полученном SMS-сообщение что-то Вас насторожило или вызвало подозрения, если Вы получили SMS-сообщение с уведомлением о совершении операции или просьбой подтвердить операцию, которую Вы не проводили – незамедлительно свяжитесь Банком по официальным контактным номерам, указанным в Вашей клиентской документации.

Поддельные веб-сайты

Еще одним приемом, часто используемым злоумышленниками, является так называемый фишинг (phishing) – создание поддельных веб-сайтов максимально похожих по дизайну на подлинные вебсайты банковских организаций. Затем

мошенники, отправляя клиенту поддельные сообщения электронной почты, SMS-сообщения, пытаются заманить клиентов на поддельный веб-сайт и выполнить «вход» в систему тем самым раскрыв злоумышленникам свои пароли и другую конфиденциальную информацию. Также опасность представляют собой компьютерные вирусы, которые, в случае заражения компьютера клиента, могут отслеживать попытки входа в системы дистанционного банковского обслуживания и перенаправлять их на подложные сайты.
Как вариант, вместо перехода на поддельный сайт, злонамеренное программное обеспечение может открывать дополнительные или всплывающие окна в программе веб-обозревателя, в которых может запрашиваться, якобы от имени Банка, ввод конфиденциальной информации клиента.

По каким признакам можно распознать сайт-подделку:

- Адрес сайта отличается от официального сайта системы ДБО; При этом отличие в адресе может быть минимальным, например, всего в один или несколько символов, так как создавая поддельный сайт-ловушку злоумышленники пытаются максимально близко скопировать подлинный сайт;
- Веб-ссылка на сайт была получена Вами в сообщении электронной почты или SMS сообщении;
- При входе на сайт Ваш веб-обозреватель сообщает Вам, что подлинность сайта не может быть подтверждена, не установлено защищенное https-соединение или возникли проблемы с SSL-сертификатом веб-сайта;
- При входе на сайт помимо Ваших Логина и Пароля для доступа в Личный кабинет у Вас запрашивают какую-либо дополнительную информацию и/или личные данные, например, «подтвердить» свой номер мобильного телефона, указать производителя и модель Вашего телефона или выполнить установку «обновления» или дополнительного программного обеспечения.

Если Вы получили сообщение, содержащее веб-ссылку и просьбу войти в систему ДБО, или у Вас возникли подозрения, что Вы оказались на поддельном сайте, то незамедлительно покиньте сайт и сообщите об этом в Банк, связавшись по официальным контактным номерам, указанным в Вашей клиентской документации.

Инфицирование компьютера зловредным программным обеспечением:

Зачастую злоумышленники пытаются инфицировать компьютер пользователя злонамеренным программным обеспечением, таким как компьютерные вирусы, программы-шпионы, перехватчики клавиатурных нажатий и т.п.,

Злоумышленники пытаются разместить злонамеренное программное обеспечение на различных веб-сайтах – начиная от сайтов с сомнительным содержанием и до сайтов социальных сетей и новостных сайтов с недостаточным уровнем защиты.

Заражение компьютера пользователя может происходить незаметно при посещении пользователем таких сайтов, а отправной точкой часто служат сообщения электронной почты с веб-ссылками, отправляемые пользователю адресно или в рамках массовой спам-рассылки.

Относитесь крайне настороженно к сообщениям электронной почты, полученных от неизвестных Вам отправителей, особенно если такие сообщения содержат присоединенные файлы или веб-ссылки. Очень часто веб-ссылки в таких сообщениях могут привести Вас на сайт, с которого будут осуществляться попытки заражения Вашего компьютера.

Использование современного антивирусного программного обеспечения, своевременное его обновление и регулярные полные проверки Вашего компьютера на наличие вирусов являются адекватными мерами по снижению риска инфицирования и/или оперативного обнаружения злонамеренного программного обеспечения.

Разумная осторожность при посещении веб-сайтов также поможет Вам снизить этот риск.

Телефонная связь

Злоумышленники могут пытаться использовать телефонную связь в комбинации с методами «социальной инженерии» для целей получения доступа к Вашей конфиденциальной информации.

Запомните, что реальные сотрудники Банка никогда не будут просить Вас сообщить по телефону Ваши пароли для входа и другую конфиденциальную информацию. Контактные данные (номера телефонов и адреса электронной почты) могут быть изменены клиентом только путем личной подачи заявления в Банк.

Только если Вы самостоятельно позвонили в Банк, то в зависимости от типа обращения, работники банка идентифицировав Вас, могут попросить назвать Вашу личную кодовую фразу для целей подтверждения Вашей личности.

Держите Вашу кодовую фразу в секрете и не сообщайте ее никому постороннему.

Если Вы получили входящий звонок от имени Банка, и он вызывает у Вас подозрения, то не спешите отвечать на вопросы звонящего. Уточните цель звонка, имя, фамилию, должность и отдел звонящего и по какому телефону Вы можете связаться. Затем перезвоните в Банк по контактным номерам, указанным в Вашей клиентской документации с тем, чтобы проверить подлинность полученного звонка.

Также Банк сообщает, что не использует в своей работе автоматические системы информирования для совершения звонков своим клиентам. Если Вы получили входящий звонок от имени Банка и система автоматического информирования запрашивает Вас ввести в тоновом режиме Ваш пароль или другую конфиденциальную информацию – это явный признак попытки мошеннических действий. В таком случае свяжитесь незамедлительно с Банком.

2. ПЕРСОНАЛЬНЫЕ МЕРЫ БЕЗОПАСНОСТИ И РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

1. Установите и используйте современное антивирусное программное обеспечение, персональный сетевой экран (брандмауэр, firewall). Обеспечьте регулярное обновление антивирусных баз.
   Наилучшая практика 1) активируйте автоматическое обновление Вашего антивируса и 2) периодически проводите полную проверку Вашего компьютера.

   2. Современные смартфоны и планшеты представляют собой вычислительные устройства, сравнимые по сложности и возможностям с давно привычными персональными компьютерами. Установите современное антивирусное программное обеспечение на Ваш смартфон или другое устройство, используемое Вами для взаимодействия с ДБО.

3. Своевременно устанавливайте обновления безопасности операционной системы и ключевых приложений (например, веб-обозревателя), выпускаемые производителями.
   Наилучшая практика – активируйте автоматическое обновление.

4. Избегайте постоянной работы на Вашем компьютере под учетной записью с административными полномочиями (напр., Администратор). Выполнение ежедневной работы, в том числе использование Интернет-ресурсов, под учетной записью с широкими полномочиями делает Ваш компьютер гораздо более уязвимым для заражения вирусами, программами-шпионами и другим злонамеренным программным обеспечением.

   Наилучшая практика – для выполнения рядовых задач используйте учетную запись с ограниченными правами доступа. Используйте административный уровень доступа только для тех задач, где он действительно требуется.

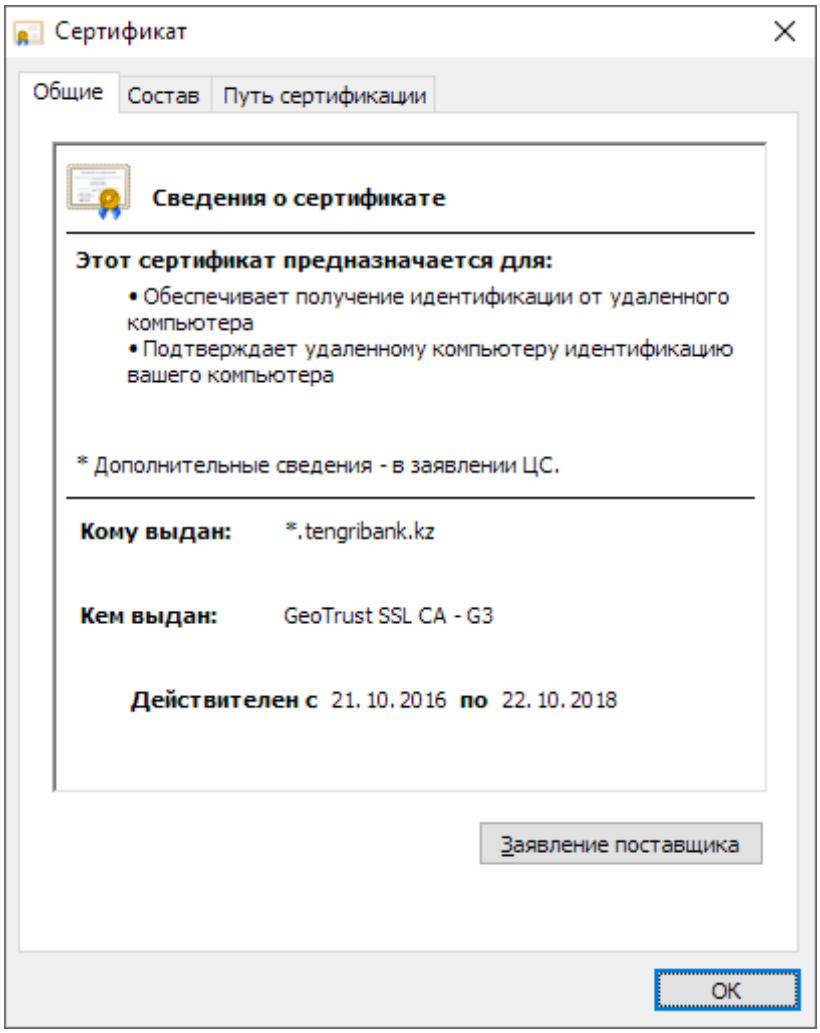
5. Избегайте работы с другими веб-сайтами во время сеанса использования системы ДБО.
   Наилучшая практика: закройте все окна веб-обозревателя перед началом работы с системой ДБО. Затем откройте приложение веб-обозревателя и войдите в систему ДБО.
6. Всегда заходите в систему ДБО только с официального сайта
   Никогда не заходите в систему ДБО по ссылке, полученной в сообщении электронной почты (e-mail) или СМС-сообщении.

   Злоумышленники часто используют сообщения электронной почты, имитирующие сообщения от Банка, с целью заманить пользователя на поддельный веб-сайт. Напротив, Банк никогда не помещает ссылки на страницу входа в систему ДБО в исходящей электронной корреспонденции, адресованной клиентам.

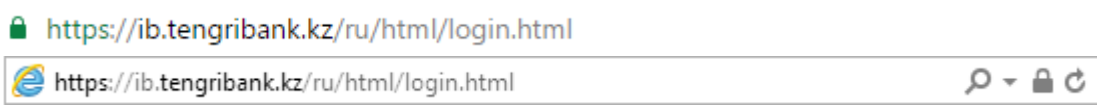
   Наилучшая практика: потратьте несколько лишних секунд и наберите адрес системы ДБО вручную в адресной строке веб-обозревателя

7. Прежде чем вводить Ваши логин и пароль для входа в систему ДБО, обязательно убедитесь, что

   а) установлен сеанс защищенного соединения (https) с веб-сайтом
   б) Вы находитесь на подлинном сайте системы ДБО, а действующий SSL-сертификат выдан Tengri Bank.



   Для отображения данных SSL-сертификата необходимо щелкнуть по изображению защищенного соединения (закрытого замка) в веб-обозревателе. Может выглядеть по-разному (в зависимости от веб обозревателя).



8. После входа в систему всегда обращайте внимание на информацию о последнем входе в систему. Эта информация доступна на главной странице Личного кабинета и отображает дату, время и сетевой адрес, с которого был осуществлен последний вход в систему под Вашей учетной записью.

   Если у Вас на основе этой информации возникло подозрение, что кто-то другой входил в систему под Вашей учетной записью – незамедлительно смените Ваш

пароль и свяжитесь с Банком по контактным номерам, указанным в Вашей клиентской документации.

9. Используйте надежные пароли для входа в систему ДБО и регулярно их меняйте.

   Для этого надежный пароль должен:

- Быть не менее 8 символов длиной. Более длинные пароли являются более надежными. С каждым дополнительным символом устойчивость пароля к подбору значительно возрастает;
- Пароль должен включать в себя прописные и строчные буквы, цифры и специальные символы;
- Не следует выбирать повторяющиеся последовательности символов или нажатий клавиш, расположенных в легко предугадываемом порядке на клавиатуре (например, Qwerty123! – это очень уязвимый пароль, несмотря на его длину и кажущуюся сложность);
- Не используйте в качестве паролей имена, даты дней рождения близких Вам людей и другую персональную информацию, которую при желании злоумышленники все же могут достаточно легко выяснить из открытых источников;
- Пароль необходимо регулярно менять – не реже одного раза в 90 дней;
- Надежный пароль должен быть легок Вам для запоминания и не требовать записи. Как только надежный пароль записан, неважно - на бумагу или в электронном виде, он перестает быть надежным.

10. Не используйте свой пароль к системе ДБО в качестве пароля к любым другим системам. В особенности – к системам, расположенным в сети Интернет (например, Web-почта, социальные сети, Интернет-магазины и т.п.). Требования по уровню защиты и безопасности к таким системам могут быть существенно ниже, а возможный взлом такой системы, о котором Вы, скорее всего, даже не узнаете, может поставить под угрозу раскрытия Ваш пароль.

11. Никогда и никому не сообщайте пароль для доступа к ключевому файлу, записанному на USB e-Token, используемому для работы с ДБО;

12. После проведения операций в системе ДБО, либо при длительном отсутствии на рабочем месте, физически извлеките USB eToken и храните его в безопасном недоступном для посторонних лиц месте, до проведения следующих операций.

13. Обеспечьте конфиденциальность Вашего пароля, кодовой фразы, персональных USB eToken носителей. Ни при каких условиях не сообщайте никому Ваш пароль. Если у Вас появились подозрения, что Ваш пароль стал известен кому-либо еще кроме Вас – незамедлительно поменяйте Ваш пароль используя функцию «Сменить пароль».

14. При осуществлении входа в систему ДБО учитывайте, что в целях обеспечения конфиденциальности Вашего пароля и защиты его от попыток подбора злоумышленниками, после определенного числа идущих подряд неуспешных

попыток входа в систему с неправильным паролем Ваш доступ к системе ДБО может быть временно ограничен или заблокирован.

15. Всегда корректно завершайте сеанс работы с системой ДБО, используя пиктограмму системы «Выход из приложения» в верхнем правом углу экрана системы. После этого закрывайте приложение веб обозревателя.

16. Банк настоятельно не рекомендует осуществлять доступ к системе ДБО используя гостевые рабочие места (например, Интернет-киоски) и/или общедоступные сети беспроводного доступа (Wi-Fi), например, в кафе, ресторанах, аэропортах, гостиницах, офисных центрах и т.д., так как такие условия и способы использования системы ДБО представляют собой случаи повышенного риска перехвата конфиденциальной информации. Если Вам все же пришлось в силу обстоятельств воспользоваться доступом к системе ДБО в таких условиях, поменяйте Ваш пароль как можно скорее, используя среду доступа с более высоким уровнем доверия.