Рекомендации Клиенту по безопасному использованию системы дистанционного банковского обслуживания в АО «БКС Банк»

АО «БКС Банк» постоянно совершенствует системы защиты Вашего счета при использовании дистанционных каналов банковского обслуживания (ДБО). Принимаемые нами меры обеспечения высокого уровня безопасности Вашей финансовой информации основаны на новейших методах и технологиях. Однако их эффективность будет минимальна без Вашего участия и соблюдения рекомендаций Банка в отношении систем ДБО.

Мы стремимся, чтобы Ваш опыт банковского обслуживания через Интернет был положительным и не доставлял неудобств. Система ДБО Банка – удобный, современный и безопасный инструмент удаленного доступа к Вашим счетам и банковским продуктам при условии выполнения некоторых простых мер безопасности, приводимых ниже.

Советы по повышению безопасности при работе с системой ДБО

1. Вход в систему ДБО Банка осуществляйте только с официального сайта www.bcs-bank.com. АО «БКС Банк» никогда не помещает ссылки на страницу входа в систему ДБО в исходящей корреспонденции Клиентам. Не входите в систему ДБО из источников в Интернет, т.к. мошенники часто фабрикуют фишинговые сайты (сайты-двойники) для хищения Вашей аутентификационной (логин, пароль) и, как следствие, финансовой информации. При обнаружении сайта-двойника немедленно сообщите об этом в службу информационной безопасности Банка и перешлите ссылку, с которой осуществлялся вход на него, для проведения расследования нашими специалистами.

2. Избегайте входа в систему ДБО Банка в местах, где услуги Интернета являются общедоступными, например Интернет-кафе, а также с неизвестных Вам компьютеров. В случае, если Вам все же пришлось осуществить вход в систему ДБО с компьютера общего пользования, мы рекомендуем сменить пароль с личного компьютера сразу после того, как Вы завершили работу. Это важно, поскольку существует риск перехвата мошенниками Ваших банковских реквизитов (номера банковской карты), а также иной информации (логин, пароль) без Вашего ведома при помощи вредоносного программного обеспечения и вирусов.

3. Перед осуществлением входа в систему ДБО Банка убедитесь, что Вы находитесь на подлинном сайте и поле «адрес» в адресной строке Вашего Интернет браузера соответствует официальному адресу веб-сайта Банка. Некоторые веб-сайты внешне могут быть похожими на настоящий, но в действительности являются фальшивыми (сайты-двойники). Самый безопасный доступ к достоверному веб-сайту Банка – набрать его адрес вручную.

4. Перед осуществлением передачи Вашей конфиденциальной информации через веб-сайт убедитесь в наличии символа замка в правом нижнем углу веб-страницы (или справа от адресной строки в версиях Internet Explorer 7 и выше). Данный символ указывает на то, что сайт работает в защищенном режиме, и все передаваемые данные будут защищены.

5. Никому и никогда не сообщайте свой пароль к системе ДБО, ПИН-код карты и CVV/CVC (секретный трехзначный код для осуществления операций с использованием

Вашей банковской карты в Интернет). Запомните, АО «БКС Банк» никогда и ни при каких обстоятельствах не запрашивает указанную информацию у Клиентов.

6. Осуществляйте вход и работу в системе ДБО Банка только с защищенного лицензионным антивирусным программным обеспечением компьютера и своевременно производите обновление антивирусных баз. Антивирусное программное обеспечение и персональный firewall требуют постоянного обновления для своевременной и надежной защиты Вашей информации от вредоносных программ, и атак из сети Интернет. Использование персонального firewall особенно важно на компьютерах с высокоскоростным доступом в Интернет. Помните, что даже если Вы не посещаете сайты сомнительного содержания, это не гарантирует вирусной чистоты компьютера, т.к. регулярно выявляются случаи вирусного заражения общеизвестных сайтов (включая новостные и финансовые). Используйте антивирусное ПО проверенных и хорошо зарекомендовавших себя производителей (Лаборатория Касперского, Symantec, ESET Software, Trend Micro, McAfee, Microsoft, Panda Software).

7. Используйте функцию подтверждения операций в ДБО кодом подтверждения, отправляемым на Ваш мобильный телефон. Даже если логин и пароль в систему ДБО скомпрометированы и стали известны злоумышленникам, получить доступ к SMS-сообщениям Вашего телефона они не смогут, как и отключить функцию их отправки.

8. Решив закончить работу с системой ДБО Банка, делайте это в соответствии с установленными процедурами. Не закрывайте Интернет-браузер просто так. Выполняйте последовательное завершение сеанса работы посредством нажатия на клавишу «Выход».

Меры безопасности при работе с компьютером

1. Не работайте на компьютере под учетной записью с правами администратора системы. Помните, что атакующее Ваш компьютер вредоносное ПО при работе с административными правами также может получить максимальные привилегии в системе, и этим значительно облегчить задачу злоумышленников. Возьмите за правило регистрировать и использовать для постоянной работы учетную запись с ограниченными правами, а учетной записью администратора системы пользоваться лишь при необходимости (например, для установки новых программ или перенастройки компьютера).

2. Не отключайте без особой необходимости средства обеспечения безопасности Вашего компьютера. К ним относятся: антивирусное ПО, межсетевой экран (firewall), системы обеспечения безопасного повышения привилегий (например, UAC в Microsoft Windows Vista и старше), системы поиска и установки обновлений ПО.

3. Несмотря на то, что большинство современных антивирусных продуктов имеет режим постоянной проверки (резидентный режим) компьютера на вирусы **не стоит пренебрегать периодической полной проверкой всего содержимого компьютера**. Как правило, при установке антивирусного ПО создаются задачи проверки компьютера по расписанию.

4. Не используйте взломанное либо нештатным образом активированное ПО, полученное из сомнительных источников. Нет никаких гарантий, что взлом защитных механизмов ПО не привел к ослаблению штатной защиты ПО от неблагоприятных

внешних воздействий, и, более того, что взломщики сами не встроили в дистрибутив ПО вредоносные компоненты.

5. По возможности, не используйте предлагаемую браузером функцию сохранения паролей к сайтам (в т.ч. к сайту ДБО), т.к. сохраненная информация может стать легкой добычей злоумышленников при проведении атаки на браузер. В случае необходимости централизованного безопасного хранения паролей, рекомендуется использовать специализированные решения (например, LastPass).

6. При отправке по открытым каналам связи (например, по электронной почте) **конфиденциальной информации** (Ваших персональных, либо контактных данных, финансовых, медицинских и др. аналогичных документов) **принимайте меры по защите этой информации**. Достаточно надежной мерой, например, является упаковка данных в зашифрованный архив с защитой последнего стойким паролем; пароль при этом должен быть сообщен адресату по иному каналу связи, например, по телефону.

7. Не храните на серверах электронной почты (в особенности, бесплатных ресурсов веб-почты) **письма, содержащие конфиденциальную информацию**, в частности, переписку с Банком: хранимая в почте информация может стать сравнительно легкой добычей злоумышленников и быть использованной ими против Вас. Регулярно производите очистку папок веб-почты, не забывая про папки «Черновики», «Отправленные», «Удаленные» и/или «Корзина».

8. Не открывайте вложения в почтовые письма, полученные от незнакомых отправителей. Даже если отправитель Вам знаком, не лишним будет проверить файл антивирусной системой перед его запуском.

9. В случае, если компьютер ведет себя странно (появляются сообщения об ошибках в программах, программы самопроизвольно запускаются либо завершаются, их выполнение занимает больше, чем обычно, времени, появляются вплывающие окна в браузере на тех сайтах, где их не должно быть, вместо указанного в адресной строке браузера адреса открываются другие ресурсы и т.п.) настоятельно рекомендуется немедленно прекратить использование компьютера и провести внеочередную полную антивирусную проверку.

Описание и характерные признаки мошенничества, направленного на получение доступа к Вашим данным в системах ДБО

Фишинг (phishing) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — в основном, логинам и паролям. Это достигается путем проведения массовых рассылок электронных писем, SMS-сообщений от имени популярных брендов, а также личных сообщений внутри различных сервисов, от имени Банков или внутри социальных сетей.

Рассылаемые мошенниками массовые электронные письма, которые играют роль приманки, часто похожи на настоящие электронные сообщения, направляемые Банком своим Клиентам; однако, их целью является заманить Клиента на сайт-двойник, замаскированный под веб-сайт Банка, чтобы получить финансовую информацию и персональные данные (номер банковской карты, ПИН-код карты, CVV/CVC, логин и пароль в систему ДБО, почтовую систему). В дальнейшем полученная информация может быть использована мошенниками для хищения денежных средств с Вашего счета.

Даже если Вы просто перешли по направленной ссылке на сайт-двойник и не согласились передать Вашу персональные данные, Ваш компьютер уже может быть заражен вредоносным ПО, которое будет перехватывать результат работы средств ввода (клавиатуры, мыши) в момент инициации входа в систему ДБО, и передавать мошенникам все необходимые для совершения хищения денежных средств данные.

Ниже по тексту указаны основные варианты мошенничества, осуществляемого в отношении Клиентов Банка с целью получения доступа к их конфиденциальной информации, и способы противодействия.

Характерные признаки того, что электронное письмо/SMS-сообщение направленно мошенниками:

- Ссылка, указанная в сообщении, не содержит названия Банка, либо содержит его в искаженном виде, например, http://www.site.com/bcsbank.html.
- Запрашиваемые в них действия требуют Вашего срочного ответа или принятия немедленного действия. Например, Ваш счет будет заблокирован или Вам срочно необходимо сменить контактные данные.
- Требуют предоставить, обновить или подтвердить Ваши персональные данные (кодовое слово, номер банковской карты, ПИН-код карты, CVV/CVC, логин и пароль к системе ДБО).
- Содержат форму для ввода Ваших персональных данных (ФИО, паспортные данные, контактная информация).
- Содержат информацию, что на Ваш счет поступили денежные средства, которых Вы не ожидали.
- Содержат информацию о том, что Вы выиграли ценный приз, для получения которого Вам необходимо осуществить немедленные действия или принять срочное решение.
- Содержат ссылки на веб-сайты, которые имеют похожее наименование оригинальных (они могут содержать фрагмент или полное наименование Банка). Однако эти ссылки приведут Вас на сайт-двойник или открывают всплывающее окно, которое запрашивает или требует подтвердить Ваши персональные данные.
- Содержат (не обязательно) явные опечатки или орфографические ошибки, замену букв цифрами и т.п., что помогает таким сообщения обходить spam-фильтры почтовых систем.

Меры безопасности при получении подозрительной корреспонденции

1. Работая с электронной почтой, убедитесь в том, что антивирусное программное обеспечение Вашего компьютера функционирует и своевременно обновляется.
2. Никогда не переходите по ссылкам в сообщениях, если содержание сообщений либо адрес отправителя кажется Вам подозрительным.
3. Читая сообщение, будьте внимательны. Как правило, сообщения, отправляемые мошенниками, содержат ряд вышеупомянутых признаков, по которому их легко

распознать. Проще всего это сделать, внимательно просмотрев (не открывая) присланную ссылку.

4. Помните, что АО «БКС Банк» никогда и ни при каких обстоятельствах:
    - не отправляет сообщения с просьбой подтвердить, обновить или предоставить Ваши персональные данные (номер банковской карты, ПИН-код карты, CVV/CVC, логин и пароль в систему ДБО);
    - не отправляет сообщений либо писем с просьбой ввода Ваших персональных данных (ФИО, паспортные данные, контактная информация);
    - не просит Вас зайти в систему ДБО посылке в письме, т.к. это противоречит Политике безопасности.

Меры безопасности при общении по телефону

Непосредственное общение по телефону в последнее время активно используются мошенниками для сбора персональной информации и убеждения Клиента в необходимости осуществления немедленных действий, направленных на незаметный для Клиента перевод денежных средств в пользу третьих лиц под различными предлогами (например, под предлогом разблокирования банковской карты, получения или оформления ценного выигрыша и т.п.). Цель мошенника – хищение денежных средств со счета Клиента путем любых доступных приемов психологического воздействия на человека (страх, жалость, обещание ценного выигрыша и т.п.). Основное и наиболее эффективное средство от такого вида мошенничества – немедленно прекратить разговор и перезвонить в Банк самостоятельно (если собеседник представился сотрудником АО «БКС Банк») по номерам, указанным на официальном сайте www.bcs-bank.com или на оборотной стороне банковской карты Банка.

Характерные признаки мошенничества по телефону

1. Собеседник требует от Вас принятия немедленного действия или срочного ответа. В качестве причин, как привило, приводятся следующие: техническое блокирование Вашего доступа в систему ДБО, блокирование банковской карты, наличие неоплаченной задолженности по кредиту, обновление баз данных и т.п.
2. От Вас требуется назвать Ваши персональные данные (номер банковской карты полностью, ПИН-код карты, CVV/CVC, логин и пароль в систему ДБО). Запомните, АО «БКС Банк» никогда и ни при каких обстоятельствах не запрашивает эту информацию у Клиентов.
3. Собеседник путается или ведет себя нетерпеливо при уточнении с Вашей стороны его ФИО, контактного номера, цели звонка, подразделения (отдела, департамента и т.д.), в котором он работает, фамилии руководителя.
4. При разговоре Вас просят произвести вход в систему ДБО Банка, сменить ПИН-код в банкомате или пароль. В этом случае спросите у собеседника контактный номер телефона Банка, по которому Вы сможете перезвонить позже, закончите разговор и обратитесь в АО «БКС Банк» (если Вам представились сотрудником АО «БКС Банк») по номерам, указанным на официальном сайте www.bcs-bank.com или на оборотной стороне банковской карты Банка. Ваше обращение позволит предотвратить инциденты мошенничества в будущем.