Рекомендации по обеспечению безопасности при работе в Системе ДБО

Соблюдение настоящих рекомендаций, направленных на обеспечение информационной безопасности и предотвращение мошенничества при использовании системы Дистанционного банковского обслуживания Авто Финанс Банк («Интернет-банк» и «Мобильный банк», далее – системы ДБО), позволит обеспечить защиту конфиденциальной информации, а также снизит возможные риски при совершении операций в системе ДБО. Следование настоящим рекомендациям позволит Вам максимально безопасно работать с Системой ДБО, защитить себя от мошенничества и свести финансовые потери к минимуму.

Будьте бдительны, следуйте приведенным ниже рекомендациям.

Общие рекомендации

1. При использовании системы ДБО хранить в секрете информацию, используемую для осуществления аутентификации в системе ДБО: учетные данные (логин, пароль), код доступа, а также получаемые Пользователем SMS-коды на привязанный к ДБО номер мобильного телефона.

2. В целях безопасности, в системе ДБО необходимо осуществлять смену пароля на любой другой, отличный от ранее используемых, с регулярностью изменения не реже 1 раза в квартал. При осуществлении первого входа в систему ДБО изменить временный пароль для первичного входа на постоянный пароль. Банк рекомендует изменять пароль не реже 1 раза в месяц.

3. Не отвечать на подозрительные звонки и звонки с неизвестных номеров или номера, которые не определяются, электронные письма (в т.ч. переходить по ссылкам в электронных письмах от неизвестных отправителей) и сообщения из социальных сетей, которые запрашивают конфиденциальную информацию (логин, пароль, код доступа, SMS-код, персональные данные и т.п.), в том числе от работников Банка. Банк никогда не обращается к клиентам с подобными просьбами и никогда не отправляет СМС и email-рассылки с неизвестных номеров и адресов.

4. Следует помнить, что для входа в Систему ДБО Вам требуется вводить только ваш логин и пароль. Кодовое слово — только для общения с работником Банка по телефону, когда Вы лично обращаетесь в Банк. Не требуется вводить или дополнительно подтверждать номером Вашей банковской карты или CVV/CVC-кодом (выпущенной другими кредитными организациями) вход или дополнительную проверку персональной информации в Системе ДБО.

5. Никогда и ни при каких обстоятельствах не сообщайте никому свои учетные данные и коды для входа в Систему ДБО или для подтверждения действий, совершаемых в Системе ДБО, а также номера ваших карт и CVV/CVC коды. Не храните логин и пароль для доступа в систему ДБО на персональных устройствах, с которых осуществляете доступ в систему ДБО, не сохраняйте его в браузере для упрощения входа. Не храните его в общедоступном месте, а также в свободном виде на открытом пространстве. Не записывайте пароль.

6. Ни при каких обстоятельствах не передавать и не сообщать никому (в том числе родственникам, друзьям, правоохранительным органам) Ваши учетные данные, коды доступа и SMS-коды, полученные при использовании ДБО, и иную конфиденциальную информацию. Если Вам пришло

SMS с паролем для подтверждения действия в системе ДБО, которое Вы не совершали, известите об этом Банк. Если Вас под любым предлогом просят ввести/назвать пароль, код доступа или одноразовый SMS-код, ни в коем случае не вводите и не называйте его, кем бы ни представился Ваш собеседник.

7. Не предоставляйте звонящим данные банковских карт, учетные данные для входа в ДБО, пароли, коды доступа, SMS-коды и иную конфиденциальную информацию. Помните, что работниками Банка никогда не запрашивается подобная информация.

Не перезванивайте в ответ на подобные звонки. Для обращения в Банк используйте официальные телефоны, указанные на сайте Банка. Помните, что работники Авто Финанс Банка никогда и ни при каких обстоятельствах не звонят и не просят сообщить или ввести куда-либо персональные данные и конфиденциальную информацию, в том числе сообщить ее голосовому роботу.

8. Не выполняйте инструкции, получаемые с использованием телефонной связи при входящем звонке или сообщении электронной почты от лиц, представляющихся работниками Банка, не сообщайте им какую-либо конфиденциальную информацию. Работники Банка никогда не будут обращаться к Вам вышеуказанными способами с просьбой выполнить те или иные действия или предоставить им сведения, связанные с системой ДБО. В случае обращения к Вам с подобной просьбой незамедлительно обратитесь в Банк любым доступным способом.

9. Не предоставляйте и не подтверждайте по входящим обращениям номер сотового телефона для SMS-уведомления в системе ДБО – Банк никогда не запрашивает эту информацию и не предоставляет ее, но принимает при добровольном предоставлении Клиентом в Банк. Так же следует отнестись к требованию о предоставлении блокировочного (кодового) слова, кроме случая, когда Вы по собственной инициативе обращаетесь в Банк. Так же следует отнестись к требованию от имени Банка об установке некоего программного обеспечения, за исключением случая получения этого программного обеспечения непосредственно на официальном сайте Банке в сети «Интернет» или способом, явно предусмотренным договорными отношениями с Банком.

10. Используйте актуальные версии программного обеспечения антивирусного ПО и операционных систем, для чего регулярно их обновляйте.

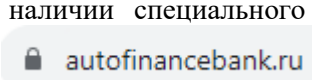
11. До входа в систему убедиться в том, что персональное устройство (компьютер, смартфон, планшет, телефон), с которого осуществляется работа с системой ДБО (в том числе при получении на него исключительно SMS-кодов), не заражено вирусами/вредоносным ПО, на нем установлено лицензионное антивирусное программное обеспечение из официальных и доверенных источников (которое не отключено и срок действия лицензии не окончился). В антивирусном ПО должно быть включено автоматическое обновление и проверка всего внешнего трафика, должны регулярно и своевременно обновляться антивирусные базы.

12. Не открывайте подозрительные файлы и ссылки на неизвестные Вам сайты, полученные от неизвестных Вам отправителей. Удаляйте, не открывая, электронную почту, полученную от

неизвестных и сомнительных отправителей, равно как и полученную от известного отправителя, но с неадекватным для него сопроводительным текстом и подозрительным вложением.

13. Заходить в систему «Интернет-банк» только с официального сайта Банка https://autofinancebank.ru/ и при переходе по ссылке , 

которая ведет на адрес (https://online.autofinancebank.ru/). Адрес страницы должен совпадать полностью, вплоть до любого знака).

14. При осуществлении входа в систему «Интернет-банк» убедиться в безопасности соединения, включая наличие символа замка в левом верхнем углу в адресной строке браузера. Чтобы проверить, что используется защищенное соединение — **https://online.autofinancebank.ru/,** необходимо перед вводом аутентификационных данных для входа убедиться в наличии специального значка (закрытый замок в адресной строке веб-браузера или рядом с ней) 

Его наличие означает, что соединение с системой «Интернет-Банк» защищено по протоколу SSL. Осуществляйте вход и ввод личной информации только убедившись, что в адресной строке веб-браузера используется защищенный протокол «https://», где «S» означает «secure» (защищенный). Убедитесь в наличии такого защищенного соединения перед использованием системы «Интернет Банк». Если в адресе не указано «https://» или указано «http://», это означает, что Вы находитесь на незащищенном веб-сайте и осуществлять вход/вводить данные нельзя. В этом случае следует незамедлительно обратить в Банк.

15. Не осуществлять вход в систему ДБО в местах, где услуги Интернета являются общедоступными, и/или с использованием публичных беспроводных сетей, например, в Интернет-кафе или в общественном транспорте. После подобного использования рекомендуется сменить пароль. Не использовать незащищенное Wi-Fi подключение или защищенное «простым» паролем («сложным» считается пароль, длина которого — не менее 8 символов. Такой пароль в обязательном порядке должен включать буквы верхнего и нижнего регистра, цифры и спецсимволы (@, #, $, %, <, ^, &, *), не должен быть повторяющимся и содержать слова целиком).

16. Запомните, что для входа в систему ДБО требуется только идентификатор (логин) и пароль (или одноразовый пароль, в случае дополнительного подтверждения входа). В случае, если от Вас требуют сообщить или ввести любую другую персональную информацию (персональные данные, номер и данные Вашей банковской карты), то необходимо незамедлительно прекратить сеанс использования ДБО и срочно обратиться в Банк.

17. Не оставлять без присмотра систему ДБО в активном состоянии, не осуществив выход из системы специальной кнопкой «Выход». В случае бездействия Пользователя в течение 2 минут, в целях безопасности Банк автоматически завершит сеанс использования системы ДБО. Пользователю необходимо будет заново произвести аутентификацию.

18. Не сохраняйте Ваши учетные данные (логин и пароль) в текстовых файлах на компьютере, либо на других электронных носителях информации, т.к. при этом существует риск их кражи и компрометации. При любых подозрениях на компрометацию логина и пароля посторонними

лицами (в т.ч. представившимися работниками Банка), следует незамедлительно остановить работу и обратиться в Банк по телефонам, указанным на официальном сайте https://autofinancebank.ru/**.**

19. При получении сообщений по SMS обращайте внимание на отправителя. Банк отправляет сообщения только от имени абонента – AutoFinBank .

20. Для использования системы «Мобильный банк» осуществлять скачивание и установку приложения только при переходе по ссылкам с официального сайта Банка в сети «Интернет» https://autofinancebank.ru/ или через официальные репозитории (Android: Google Play https://play.google.com, Apple: AppStore https://appstore.com).

21. Запрещается скачивать и устанавливать приложения из отличных от указанных выше мест. При этом Банк уведомляет, что распространение мошенниками неофициальных приложений, к которым Банк не имеет никакого отношения, возможны путем появления в сети «Интернет» ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемых Банком систем ДБО, и (или) использующих зарегистрированные товарные знаки и наименование Банка. Будьте внимательны, при обнаружении подобных ресурсов и приложений следует незамедлительно обратиться в Банк.

22. Запрещается использовать приложения, скачиваемые из отличных от п. 21 источников. В случае такой установки Клиент несет все риски использования системы ДБО, связанные с возможным нарушением безопасности и возможным получением несанкционированного доступа к защищаемой информации.

23. Не устанавливать на мобильный телефон, с которого осуществляется вход в систему ДБО или на который Банк отправляет Вам SMS-сообщения с подтверждающим одноразовым паролем, Приложения, полученные от неизвестных Вам источников. Помните, что Банк в одностороннем порядке, без воли и подтверждения Клиента, не рассылает своим Клиентам ссылки или указания на установку приложений через SMS/MMS/E-mail — сообщения.

24. При установке приложений обращайте внимание на полномочия, которые они запрашивают. Не разрешайте их без необходимости (например, если приложение просит права на чтение адресной книги, отправку SMS-сообщений и доступ к интернету).

25. В целях Вашей безопасности, Банк категорически не рекомендует работать с Системой ДБО или принимать одноразовые пароли для подтверждения действий на устройствах, на котором антивирусное ПО сообщает о наличии заражения или какой-либо проблемы.

26. Не подключайте телефон к устройствам, безопасность которых не можете гарантировать.

27. Регулярно проводите полную антивирусную проверку компьютера и мобильного устройства. В случае обнаружения вредоносного кода пользоваться системой ДБО запрещается до полной локализации вредоносного кода всех используемых для работы с системой ДБО устройств.

28. Старайтесь избегать регистрации номера вашего мобильного устройства, на который приходят SMS с одноразовым паролем, в социальных сетях и других открытых и доступных источниках.

29. В случае утери мобильного телефона, на который приходят SMS-сообщения с одноразовым паролем, необходимо незамедлительно заблокировать SIM-карту.

30. В случае внезапного приостановления работы SIM-карты, которая является зарегистрированным номером для направления Банком SMS-сообщений в системе ДБО, незамедлительно обратиться к оператору мобильной связи для выяснения причин блокировки (возможно незаконное изготовление третьими лицами дубликата SIM-карты). В случае необходимости, с целью осуществления блокировки ДБО, необходимо незамедлительно обратиться в Банк.

31. В качестве телефонного номера для получения одноразовых SMS-паролей указывайте только Ваш личный номер телефона.

32. Вводить одноразовые пароли (SMS-коды) следует только в том случае, если операция инициирована Вами. При получении SMS с одноразовым паролем внимательно ознакомьтесь с его содержанием, обязательно проверьте детали и составляющие операции, которую Вы подтверждаете одноразовым SMS-кодом. Вводить SMS-код в систему следует только тогда, когда реквизиты и детали Вашей операции в системе ДБО соответствуют реквизитам в полученном SMS — сообщении.

33. В целях повышения безопасности, рекомендуем не пользоваться системой ДБО с того же мобильного устройства, на который приходят SMS-сообщения с подтверждающим одноразовым паролем.

34. Используйте для звонков в Банк только номера телефонов, указанных на официальном сайте Банка в сети Интернет https://autofinancebank.ru/**.** Никогда не обновляйте список банковских телефонных номеров по входящему телефонному звонку, электронной почте и иным недоверенным каналам связи. Часто мошенники на поддельных сайтах указывают неправильные номера, которые могут быть недоступны или по ним ответит оператор, с целью совершения мошеннических действий. В случае подозрения на мошенничество следует незамедлительно обратиться в Банк.