Уважаемый клиент!

Интернет-банк, мобильные приложения и другие различные сервисы дистанционного банковского обслуживания являются постоянной мишенью для различного рода злоумышленников. Распространяемые ими вредоносные программы нацелены на хищение денежных средств со счетов клиентов путём создания и отправки в различные банки платёжных документов якобы от имени клиентов, которые практически неотличимы от документов, создаваемых самими клиентами. Эти программы создаются профессионалами высокого класса с учётом особенностей конкретных информационных систем.

Мы максимально защищаем вашу информацию и денежные средства на счетах, но всегда существуют риски получения доступа злоумышленников к осуществлению переводов денежных средств, если Вами не будут соблюдаться правила безопасного использования сервисов. Описанные в этом буклете меры информационной безопасности позволят повысить безопасность ваших финансов, которыми вы управляете с помощью сервисов дистанционного банковского обслуживания в интернет-банке, мобильных приложениях и других системах.

Памятка о мерах безопасного использования системы дистанционного банковского обслуживания АО Банк ЗЕНИТ Сочи

1. Общие принципы обеспечения безопасности

1.1. Помните, что ни одна программа и (или) техническое решение не даёт 100% гарантии защиты Вашего компьютера, планшета, смартфона или иного устройства, с которого вы осуществляете операции в системе ДБО, и (или) на которые вы получаете SMS-пароли или услуги SMS-информирования (далее – Устройство) от несанкционированного использования злоумышленниками, поражения вирусом или иным вредоносным программным кодом. Старайтесь использовать указанные в настоящей Памятке защитные меры в комплексе.

1.2. Регулярно самостоятельно контролируйте состояние своих банковских счетов и операций по ним.

1.3. Осуществляйте информационное взаимодействие с Банком только с использованием средств связи (телефоны, факсы, веб-сайты, обычная и электронная почта и пр.), реквизиты которых оговорены в документах, полученных непосредственно в подразделениях Банка.

1.4. Ни при каких условиях не сообщайте третьим лицам, включая любых работников Банка, Вашу конфиденциальную информацию и секретные реквизиты для взаимодействия с Банком и работы с использованием Устройств, с системой ДБО (логины, пароли, кодовые слова), а также номер Вашей банковской карты, ее CVC/CVV- и ПИН-коды. Исключите возможность неправомерного получения информации о паролях к системе ДБО и (или) кодам доступа, SMS-паролям.

1.5. Не сохраняйте конфиденциальную информацию в файлах (включая графические изображения) или в памяти Устройств, в справочниках или «облачных» сервисах хранения информации и ресурсах в сети Интернет. Не фиксируйте конфиденциальную информацию на бумажных носителях (листы для записей, распечатки документов и т.п.), доступ к которым могут получить несанкционированные лица.

1.6. Исключите возможность неправомерного доступа к Устройствам для доступа к системе ДБО. Не передавайте их неуполномоченным лицам, храните в надёжном и недоступном для третьих лиц месте. Обязательно установите пароль на доступ к Устройству и никому его не раскрывайте. Помните, что посторонние люди могут, в том числе и не преднамеренно, нарушить работоспособность Устройств, занести вредоносные программы как со своих носителей информации, так и путём посещения вредоносных интернет-сайтов.

1.7. Не используйте чужие компьютеры или мобильные устройства для доступа к системе ДБО, не работайте с системой ДБО с «гостевых» рабочих мест (в интернеткафе и т.д.) и(или) при использовании публичных сетей беспроводного доступа. При этом возрастает риск хищения и(или) дальнейшего неправомерного использования аутентификационной информации при доступе к системе ДБО.

1.8. Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций. При необходимости обратитесь к сотрудникам подразделения банка или позвоните по телефонам, указанным на устройстве или на обратной стороне Вашей карты.

2. Обеспечение безопасности на Устройствах, используемых для взаимодействия с Банком

2.1. Не доверяйте администрирование (установку и настройку аппаратного и программного обеспечения) Ваших Устройств случайным людям. Приходящий администратор для своего удобства или злонамеренно может установить программу удалённого управления и получит возможность тайно от Вас на Вашем Устройстве выполнять различные программы, в том числе и вредоносные.

2.2. Используйте на Устройствах только лицензионное программное обеспечение, полученное из надёжных источников. Программы, полученные с непроверенных

интернет-сайтов или носителей информации, зачастую содержат в себе вредоносные компоненты: вирусы и троянские программы. Не устанавливайте на Устройства программы с нарушением рекомендованных производителями требований. 2.3. Своевременно устанавливайте обновления установленного на Устройстве программного обеспечения, выпускаемые его производителями.
2.4. Используйте на Устройстве современную антивирусную программу с функциями защиты от различного вида угроз. Своевременно, желательно – в автоматическом режиме, устанавливайте обновления всех компонентов и информационных баз антивирусной программы.
2.5. Следует периодически (раз в неделю) осуществлять полную антивирусную проверку Устройства, на котором работаете с системой ДБО. При возможности, используйте программы контроля конфигураций операционной системы на Устройстве – это позволит своевременно выявить вредоносные программы.
2.6. Используйте на Устройстве межсетевой экран («файервол»). Это затруднит несанкционированный удалённый доступ к Вашему Устройству из сети Интернет.
2.7. Работайте на Устройстве с системой ДБО только с правами обычного пользователя (не администратора). По возможности, не используйте данную учётную запись для действий в сети Интернет либо во внутренней сети, не связанными с работой в системе ДБО.
2.8. На Устройствах под управлением операционных систем семейства Windows не отключайте функцию «Контроль учетных записей пользователей» (UAC – User Account Control). Отключайте стандартную учётную запись администратора, предварительно назначив административные права иной учётной записи с нестандартным именем. Установите для неё сложный пароль, отличающийся от паролей остальных учётных записей. Используйте такую учётную запись только для настройки Устройства, установки доверенного программного обеспечения и т.д.
2.9. Не используйте для проведения операций или получения SMS-паролей и (или) SMS-информирования мобильные Устройства с отключёнными функциями безопасности, предусмотренными производителем (с использованием программ для получения Jailbreak или Root доступа к Устройству).
2.10. Применяйте разные пароли для различных Устройств и программ, регулярно осуществляйте их смену. Используйте пароли не менее 7 символов с применением и цифр, и специальных символов, больших и маленьких букв. Не используйте попеременно и(или) одни и те же пароли для разных Устройств и(или) программ, доступа к публичным интернет-сайтам и информационным сервисам:

- для доступа в Устройства;
- для входа в учётные записи;
- для изменения настроек программного обеспечения, прежде всего – обеспечивающего безопасность (антивирус, файервол);
- для работы с системой ДБО;
- для доступа к электронной почте, в социальные сети, службы мгновенных сообщений и т.д.
- при использовании функции доступа к устройству по отпечатку пальца (TouchID/Fingerprint), не используйте отпечатки посторонних лиц;

2.11. Делайте резервные копии Ваших данных и диски аварийного восстановления операционных систем Устройств.
2.12. Обязательно завершайте работу с системой ДБО, с интернет-браузером, с Устройством путём выполнения стандартных процедур (нажатия соответствующей кнопки в интерфейсе программ, кнопки питания Устройства).

3. Обеспечение безопасности паролей

3.1. Вы можете в любое время по своему усмотрению изменять пароль. При этом при создании нового пароля в Системе необходимо придерживаться следующих правил:

- новый пароль не должен совпадать со старым паролем;

- пароль должен состоять из последовательности символов (букв и/или цифр) длиной не менее 7 символов и не более 25 символов;
- пароль должен содержать как минимум по одному символу из любых 3-х наборов из допустимых 4-х множеств: ○ строчные буквы латинского алфавита: a, b, c, ...z; ○ заглавные буквы латинского алфавита: A, B, C, ...Z; ○ цифры: 0, 1, 2, ..., 9; ○

3.2. Следует помнить основные правила по обращению с выбираемым паролем:

- пароль должен быть сложным для невозможности его подбора злоумышленником;
- пароль необходимо хранить в тайне от всех, не хранить одновременно вместе с картой или с устройством;
- не рекомендуется использование выбранного пароля на каких-то других сайтах или в каких-то других системах.

3.3. Если вы предпочитаете использовать для входа в мобильное приложение короткий код доступа, необходимо придерживаться следующих правил:

- не создавайте простые коды доступа, например, 1234, 5555;
- не создавайте код доступа на «чужих» смартфонах и планшетах;
- периодически сбрасывайте и изменяйте код доступа.

4. Дополнительные меры по обеспечению безопасности

4.1. Используйте для оперативного контроля операций в системе ДБО SMS-информирование. В связи с возможностью круглосуточного проведения операций с использованием системы ДБО, обеспечьте постоянный контроль поступающей информации об операциях в виде SMS-сообщений и реагирование в случае несанкционированных операций. Не отключайте на своих мобильных Устройствах в ночное время звуковое уведомление о получении SMS.

4.2. Внимательно проверяйте суммы и реквизиты проводимых платежей в приходящих информационных сообщениях или сообщениях с одноразовыми паролями, не подтверждайте подозрительные операции, и незамедлительно информируйте Банк о попытках и (или) выявленных фактах мошеннических платежей.

4.3. При использовании для подтверждения операций в системе ДБО одноразовых SMS-паролей и (или) при использовании SMS-информирования, обеспечьте, чтобы мобильные Устройства, используемые для получения SMS-сообщений, не использовались Вами для проведения (инициирования и подтверждения) операций в системе ДБО.

4.4. Обеспечьте правильность указания в оформляемых Вами заявлениях и в других документах номеров телефонов для связи, номеров мобильных телефонов для получения услуги SMS-информирования и получения SMS-паролей, иных координат для связи с Вами (с уполномоченными лицами).

4.5. Используйте только приложения банка ЗЕНИТ Сочи Онлайн 2.0 текущей версии, установленные из официальных магазинов приложений App Store и Google Play. Обязательно убедитесь, что в авторах приложения указан BANK ZENIT, PAO.

5. Безопасность при работе с публичными информационными ресурсами в сети Интернет

5.1. Не посещайте непроверенные интернет-сайты, особенно интернет-сайты, которые распространяют пиратское программное обеспечение или аудио/видео файлы, так как на большом количестве подобных сайтов размещён специальный программный код, заражающий Устройства различного рода вирусами и иными видами вредоносного программного обеспечения.

5.2. Не открывайте файлы или интернет-ссылки, пришедшие к Вам по публичным информационным каналам (по электронной почте, через SMS и с помощью иных служб мгновенных сообщений, из социальных сетей и т.п.) даже от знакомых Вам людей, если

только они не были присланы по Вашей просьбе или дополнительно подтверждены отправителем альтернативным способом. Сообщение может быть отправлено с подделанным адресом отправителя электронной почты, или от имени знакомого Вам человека вредоносной программой, захватившей контроль над его компьютером, мобильным устройством или учётной записью в социальной сети, в почтовой системе.
5.3. Исключите возможность запуска на исполнение получаемых файлов, включая выполняемые файлы, макросы в файлах Microsoft Office (например, в файлах Word или Excel) или скрипты с расширениями .js и .vbs.
5.4. В ряде случаев злоумышленниками могут создаваться в сети Интернет поддельные сайты, полностью имитирующие официальный сайт Банка, сайты Банковской группы ЗЕНИТ, распространяться поддельные приложения, использующие символику (зарегистрированные товарные знаки), наименование и интерфейс настоящих сайтов и приложений.
5.5. Сообщите в Банк о случае выявления Вами ложного Web-сайта, мобильного приложения Банка или о полученных сведениях подобного рода.
5.6. Схемы мошенничества, как правило, выглядят следующим образом.

- Злоумышленники распространяют вредоносные программы и подложные мобильные приложения через различные интернет-ресурсы — от социальных сетей до обычных новостных сайтов или электронной почты. Если на Устройстве отсутствуют настройки безопасности, актуальные обновления программ безопасности, интернет-браузера или другого программного обеспечения, поражение Устройства вредоносным программным обеспечением возможно даже просто при подключении Устройства к сети Интернет или к недоверенной сети.
- Клиент, Устройство которого заражено, при попытке войти в систему ДБО перенаправляется на поддельные («фишинговые») интернет-сайты, которые внешне практически не отличаются от подлинного сайта Банка.
- На поддельном сайте Вас могут попросить ввести идентификаторы и пароли, мобильный телефон и другие персональные данные, необходимые мошенникам для обмана.

5.7. Как распознать «подделку»?

- операция может проводиться в незащищённом режиме (иконки интернетбраузера, указывающие на работу в защищённом режиме, не активны);
- при входе на сайт Банка интернет-браузер может предупреждать, что сертификату безопасности сайта нельзя доверять;
- адрес может не совпадать с официальным адресом сайта Банка в сети Интернет: www.bankzenitsochi.ru
- проверяйте, что установлено защищённое SSL-соединение с официальным сайтом системы ДБО: https://i.zenit.ru

Обращаем Ваше внимание, что выполнение указанных выше рекомендаций не сможет полностью обезопасить Вас и Ваши Устройства от действий злоумышленников, но поможет существенно снизить вероятность и нежелательные последствия от таких действий.

ВНИМАНИЕ!

При подозрении или в случае:

- несанкционированного списании денежных средств со счёта,
- утраты Устройства, с которого осуществлялась работа с системой ДБО, либо мобильного Устройства, на которое получаете одноразовые SMS-пароли (потере, хищении, нарушении работоспособности), или при вынужденной срочной смене мобильного телефонного номера,
- доступа третьих лиц к Устройству с работающей системой ДБО без Вашего ведома,

- компрометации секретных реквизитов (логина, пароля, кодового слова),
- обращения к Вам от имени Банка с просьбой сообщить секретные реквизиты,
- отсутствия возможности подключения к веб-сайту системы ДБО,
- входа и(или) работы с поддельным сайтом Банка, системы ДБО,
- нестабильной и(или) нестандартной работы Устройства и(или) системы ДБО

следует незамедлительно прекратить работу в системе ДБО, выключить Устройство и обратиться в Банк с предоставлением полной информации о случившемся, что поможет оперативно приостановить возможные мошеннические операции и предотвратить финансовые потери, по следующим номерам телефонов колл-центра *2640 и +7 (862) 2640-090.

Возникли вопросы?

Контакт-центр
*2640
+7 (862) 2640-090
www.bankzenitsochi.ru/

АО Банк ЗЕНИТ Сочи. Лицензия №232 от 26.12.2014