

ПАМЯТКА О МЕРАХ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Уважаемый Клиент!

Напоминаем Вам о необходимости соблюдать принципы обеспечения информационной безопасности с целью защиты информации от воздействия вредоносного кода и исключения случаев несанкционированного доступа к Вашим счетам, с целью недопущения осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами.

Средства и методы защиты информации, применяемые в Банке, позволяют обеспечить необходимый уровень безопасности при осуществлении переводов денежных средств и предотвратить мошеннический вывод денежных средств со счетов клиентов при условии выполнения клиентами рекомендаций, изложенных в данном документе. Однако по-настоящему безопасными сервисы Банка делаете именно Вы – наши Клиенты.

Помните, что при работе со своими счетами в системах Банка следует быть настолько же внимательными и бдительными, как при обращении с наличными деньгами в Вашем кошельке!

Рекомендации для безопасной работы с системой ДБО на компьютере

1. Используйте, по возможности, отдельный персональное устройство, которое будет использоваться исключительно для работы с системой ДБО.
2. Обеспечьте безопасность компьютера, на котором установлена система ДБО:
 - Используйте на компьютере только лицензионное программное обеспечение, дистрибутивы которого получены из надежных источников.
 - Установите на компьютер лицензионное антивирусное программное обеспечение, обеспечьте автоматическое обновление антивирусных баз. Настройте еженедельное проведение полной антивирусной проверки компьютера.
 - Организуйте автоматическую установку обновлений безопасности операционной системы и другого установленного на компьютере программного обеспечения по мере их выпуска производителями из надежных источников.
 - В связи с возникающими новыми угрозами рекомендуем использовать операционные системы и прикладное программное обеспечение российского производства.
 - Минимизируйте состав установленного на компьютере программного обеспечения, исключите установку на него любых программ, не требующихся для работы с системой ДБО.
 - Не допускайте установку на компьютер никаких программ для удаленного управления (Team Viewer, Ammyu Admin, AnyDesk, VNC и т.п.), заблокируйте на нем работу встроенного сервиса удаленного доступа к рабочему столу.
 - Минимизируйте количество пользователей компьютера, установите для них надежные пароли, обеспечьте периодическую смену этих паролей.
 - Не работайте на компьютере под учетными записями, имеющими административные права. Административная учетная запись может использоваться только для установки программного обеспечения, необходимого для работы с системой ДБО, и средства криптографической защиты информации.
 - Настройте в BIOS компьютера возможность загрузки операционной системы только с основного жесткого диска, установите пароль на загрузку компьютера и вход в настройки BIOS.
 - Исключите использование с этого компьютера иных Интернет-ресурсов, не относящихся к работе в системе ДБО, обновлению программного обеспечения и обновлению антивирусных баз. Использование компьютера для посещения посторонних Интернет-ресурсов значительно повышает риск его заражения вредоносными программами.

- Используйте средства электронной почты на этом компьютере только для целей, относящихся к работе в системе ДБО.
 - Не используйте на компьютере программы обмена мгновенными сообщениями, сайты социальных сетей. Злоумышленники часто используют эти сервисы для рассылки вредоносных вложений, ссылок на сайты, распространяющие вредоносные программы или фишинговые сайты.
 - Блокируйте компьютер в случае ухода с рабочего места (одновременным нажатием клавиш Ctrl+Alt+Delete и в диалоговом окне выбирать «Заблокировать» или одновременным нажатием клавиш Windows+L), в случае длительного отсутствия и по окончании рабочего дня обязательно выключайте компьютер.
3. При работе с облачной электронной подписью самостоятельно генерируйте в системе ДБО свой пароль для ключа электронной подписи, никому не доверяйте выполнение этой процедуры.
 4. В случае внезапного нарушения работы системы ДБО или компьютера, незамедлительно проинформируйте об этом Банк и проконтролируйте полученные Банком от Вашего имени платежные документы. Зафиксированы случаи, когда злоумышленники, отправив с компьютера «жертвы» платежный документ, выводили компьютер из строя для сокрытия следов преступления и уничтожения улик. После совершения хищения они стараются помешать «жертве» своевременно узнать о произошедшем и принять меры к остановке мошеннического платежа.
 5. Будьте бдительны. Если к Вам обращаются по телефону или электронной почте и, представляясь сотрудниками Банка, просят сообщить ваши реквизиты для входа в систему ДБО, отправить пароль для ключа облачной электронной подписи или текст входящих SMS-сообщений – не делайте этого, незамедлительно сообщите о произошедшем в Банк. Если к Вам обращаются с просьбой отправить по системе ДБО платежный документ, для того, чтобы «вернуть ошибочно перечисленные средства» – сначала позвоните в Банк чтобы подтвердить легитимность данного запроса.

Горячая линия службы поддержки: 8(800) 550-51-37

Рекомендации для безопасной работы с системой ДБО на мобильном телефоне

1. Для доступа к мобильному устройству установите пароль и настройте автоматическую блокировку устройства.
2. Загружайте и устанавливайте программное обеспечение только из проверенных и надежных источников – Google Play, App Store, AppGallery.
3. Производите своевременное обновление операционной системы и используемых программ (браузера и иных прикладных программ) из надежных источников.
4. Рекомендуем использовать браузеры с поддержкой российской системы доверия tls-сертификатов (например, Яндекс.Браузер, Atom).
5. Установите на свое мобильное устройство лицензионное антивирусное программное обеспечение, обеспечьте регулярное обновление антивирусных баз и антивирусную проверку мобильного устройства.
6. Для работы с системами ДБО используйте защищенные мобильные устройства – не пытайтесь обходить установленные производителем защитные механизмы (например, через джейлбрейк (Jailbreak) или рутинг (Rooting)). Не перепрошивайте свое мобильное устройство прошивками сторонних лиц, не являющихся производителями устройства, т.к. это может сделать устройство уязвимым к заражению вредоносным кодом.
7. Используйте защищенные точки доступа к Wi-Fi-сети, а также отключайте Wi-Fi и Bluetooth, если в данный момент они не используются.
8. Не храните на мобильном устройстве конфиденциальную информацию о Вашем логине и пароле для доступа к системе ДБО. Если такая необходимость все же есть, не храните информацию в явном виде.
9. Удалите конфиденциальную информацию в случае передачи мобильного устройства другим лицам (продажа устройства, передача в ремонт). Воспользуйтесь функцией восстановления заводских настроек.
10. После окончания работы в системе ДБО, обязательно завершайте сеанс, используя кнопку «Выход».
11. Ни при каких условиях не сообщайте /не передавайте информацию о Вашем логине, пароле, одноразовых паролях из SMS-сообщений и иных сведениях, используемых для авторизации в системе ДБО никому, включая сотрудников Банка.
12. При возникновении подозрений, что Ваши данные для доступа к системе ДБО стали известны посторонним и/или в случае утери мобильного устройства незамедлительно обратитесь в Банк для их блокировки.

Горячая линия службы поддержки: 8(800) 550-51-37

Рекомендации по защите информации от воздействия вредоносного кода

1. Установите на персональные компьютеры и мобильные устройства лицензионное антивирусное программное обеспечение.
2. Регулярно обновляйте антивирусное программное обеспечение.
3. Настройте полную проверку устройства на предмет наличия вирусов и вредоносного программного кода не реже одного раза в неделю в автоматическом режиме. Такая проверка будет осуществляться согласно расписанию, выставленному в настройках антивирусного средства.
4. Подвергайте антивирусному контролю любую информацию, получаемую и передаваемую по телекоммуникационным каналам, а также информацию на съемных носителях (магнитных, CD/DVD дисках, USB-накопителях и т. п.). При наличии технической возможности, осуществляйте сканирование в автоматическом режиме.
5. Применяйте антивирусное ПО, разработанное специально для почтовых клиентов, при использовании сети Интернет для обмена почтовыми сообщениями.
6. При возникновении подозрения на наличие вируса (нетипичная работа ПО, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках, увеличение исходящего/входящего трафика и т. п.) рекомендуется приостановить работу устройством до полного устранения неисправностей.
7. Работайте под учетной записью с ограниченными правами (не используйте учётную запись администратора) – так вирусу будет сложнее внедриться и закрепиться в систему.
8. Разграничьте устройства, с которых Вы осуществляете переводы денежных средств и которые используете для общения в социальных сетях, посещения развлекательных сайтов и сайтов сомнительного содержания (игровые, сайты знакомств, сайты, распространяющие ПО, музыку, фильмы и т. п.), т. к. именно через эти ресурсы сети Интернет чаще всего распространяются компьютерные вирусы.
9. Не открывайте файлы и не переходите по ссылкам, приходящим в почтовых сообщениях, SMS-сообщениях из недостоверных источников, в том числе на известные сайты.
10. Не загружайте и не устанавливайте на компьютер и мобильное устройство программное обеспечение, полученное из недостоверных источников: Интернет-сайтов, ссылок в SMS-сообщениях и т.п.

Рекомендации по защите информации от несанкционированного доступа с использованием сети Интернет

1. Внимательно читайте текст электронного письма. Электронные письма от известных компаний никогда не содержат орфографических или грамматических ошибок. Если Вы видите слова на иностранном языке, специальные символы и т. д., скорее всего это электронное письмо отправили мошенники.
2. Проверяйте личность отправителя (организации) письма через поисковые системы или официальные сайты, или не отвечайте на письма от неизвестных отправителей.
3. Установите на свое устройство лицензионное антивирусное программное обеспечение и обеспечьте регулярное обновление антивирусных баз.
4. Не переходите по ссылкам и не открывайте вложения из писем от неизвестных Вам адресатов.
5. Не сообщайте приватную информацию, запрашиваемую в письмах, приходящих по электронной почте и сообщениях в электронных мессенджерах.
6. Не сообщайте никому свои логины и пароли учётных записей, а также данные банковских карт.
7. Обращайте особое внимание на URL-адреса страниц, на которых Вы вводите свои учётные данные.
8. Проверяйте наличие **https**-соединения (значок замка в строке URL-адреса) у сайтов, работающих с персональными данными или тех, где совершаются денежные операции.
9. Проверяйте реальные адреса гиперссылок, наводя на них курсор. Адрес, куда ведёт эта ссылка, будет отображён в левой нижней части браузера.
10. Рекомендуем использовать браузеры с поддержкой российской системы доверия **tls**-сертификатов (например, Яндекс.Браузер, Atom).
11. Избегайте использования компьютеров в общественных местах, а также общественных точек доступа к Wi-Fi-сети для осуществления Интернет-платежей.

Рекомендации по предотвращению получения несанкционированного доступа третьими лицами

1. Установите на свое устройство лицензионное антивирусное программное обеспечение. Обеспечьте регулярные обновление антивирусных баз и полную антивирусную проверку мобильного устройства.
2. Используйте для систем Банка надёжные пароли.
3. При создании паролей используйте сочетания символов верхнего и нижнего регистров, цифр и специальных символов. Используйте длинные пароли, более 8 символов.
4. Избегайте использования в паролях дат, имён, номеров телефонов и другой персональной информации, которая может быть угадана или найдена в открытых источниках (пароль StB%zO2*w – надёжный, а пароль Natasha1971 – нет).
5. Используйте различные уникальные пароли для различных сайтов и систем, где Вы вводите конфиденциальные данные (пароли для системы ДБО и для социальных сетей должны быть различными).
6. Избегайте хранения паролей в открытом виде. Не записывайте пароли на бумажных листках (или в текстовых файлах на компьютере), не оставляйте их в легкодоступных местах (на рабочем столе), не передавайте их неуполномоченным лицам. Для хранения паролей используйте менеджер паролей.
7. Изменяйте существующие пароли не реже одного раза в квартал.
8. Никому не разглашайте пароли от банковских и финансовых систем (таких, как СПБ, НСПК). Банк не рассылает электронных писем, SMS-сообщений или других сообщений с просьбой уточнить Ваши конфиденциальные данные (в т.ч. пароли, PIN-коды и т.п.).
9. В том случае, если Вы обнаружили, что Ваш пароль от банковской системы скомпрометирован или ранее действующий пароль не срабатывает и не позволяет Вам войти в систему ДБО, необходимо как можно быстрее обратиться в Банк для получения дальнейших инструкций.
10. Незамедлительно обращайтесь в Банк при обнаружении несанкционированных входов в систему ДБО (успешных и неуспешных), а также если Вы получили уведомление системы об операции, которую Вы не проводили.

Горячая линия службы поддержки: 8(800) 550-51-37