Памятка пользователей системы «Сбербанк Бизнес Онлайн».

В системе «Сбербанк Бизнес Онлайн» используются современные механизмы и средства обеспечения информационной безопасности, направленные на то, чтобы сделать работу с системой максимально удобной при поддержании высокого уровня безопасности. Вместе с тем, соблюдение приведенных рекомендаций позволит максимально безопасно работать с Системой и свести риски мошенничества и, как следствие, финансовые потери к минимуму:

Общие рекомендации:

- Пароль для входа в «Сбербанк Бизнес Онлайн» это Ваша личная конфиденциальная информация, ни при каких обстоятельствах не раскрывайте свой пароль никому, включая сотрудников Сбербанка России. При обращении от имени Банка по телефону, электронной почте, через SMS-сообщения лиц с просьбами сообщить конфиденциальную информацию (пароли, кодовые слова, и пр.) ни при каких обстоятельствах не сообщайте данную информацию.
- Первоначальная страница доступа в личный кабинет содержит только поля ввода логина и пароля. В случае если на данной странице от Вас требуется ввод любой другой персональной информации (номеров банковских карт, мобильного телефона, других личных данных), следует прекратить пользование услугой и связаться с сотрудниками Банка.
- Не сохраняйте Ваш пароль и ПИН-код в текстовых файлах на компьютере либо на других электронных носителях информации, т.к. при этом существует риск его кражи и компрометации.
- При любых подозрениях на компрометацию пароля или ПИН-кода посторонними лицами (в т.ч. представившимися сотрудниками Банка), следует незамедлительно остановить работу и обратиться в Банк по телефону 8-800-555-55-50.
- Используйте современное антивирусное программное обеспечение и следите за его регулярным обновлением.
- Регулярно выполняйте антивирусную проверку на своем компьютере для своевременного обнаружения вредоносных программ.
- Своевременно устанавливайте обновления операционной системы своего компьютера, рекомендуемые компанией-производителем в целях устранения выявленных в нем уязвимостей.
- Используйте дополнительное программное обеспечение, позволяющее повысить уровень защиты Вашего компьютера – персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от «спам»-рассылок и пр.
- Завершение работы с системой выполняйте путем выбора соответствующего пункта меню.
- Регулярно контролируйте состояние своих счетов и незамедлительно сообщайте сотрудникам Банка обо всех подозрительных или несанкционированных операциях.
- По возможности, исключите работу в Системе и подготовку платежных документов на ПК с общедоступным доступом (в т.ч. Интернет-кафе, бесплатный Wi-Fi и пр.).
- Исключайте на ПК, на которых осуществляется подготовка и отправка документов в Банк, использование систем удаленного управления ПК. Не привлекайте для администрирования и обслуживания данного ПК ИТ-персонал на условиях предоставления ему удаленного доступа.
- Исключайте посещение с ПК, на которых осуществляется подготовка и отправка документов в Банк, сайтов сомнительного содержания и любых других Интернет-ресурсов непроизводственного характера (социальные и пиринговые сети, конференции и чаты, телефонные сервисы и т.п.), чтение почты и открытие почтовых

вложений от недоверенных источников, установку и обновление любого ПО не с сайтов производителей. Настройками сетевого оборудования, корпоративных и персональных сетевых экранов выход в сеть Интернет ограничивайте «белым списком» со всех рабочих мест, на которых осуществляется подготовка, подписание и отправка платежных документов. В «белый список» должны включаться исключительно доверенные сайты и хосты самой организации, банков, налоговой службы, других государственных органов, необходимых в производственном процессе, сервера обновлений системного и антивирусного ПО.

- При наличии проблемы с подключением к системе следует немедленно обратиться в службу поддержки Банка.

Рекомендации для клиентов с sms-паролем:

- При подтверждении операций одноразовым SMS-паролем необходимо контролировать соответствие реквизитов операции и реквизитов в полученном sms-сообщении.
- Не пользуйтесь системой «Сбербанк Бизнес Онлайн» с того же мобильного телефона, иного устройства, на который приходят sms-сообщения с подтверждающим одноразовым паролем.
- При утрате мобильного телефона, на который Банк отправляет SMS-сообщения с подтверждающим одноразовым паролем, а также в случае, если у Вас неожиданно перестала работать телефонная sim-карта, следует оперативно обратиться к своему оператору сотовой связи для блокировки абонентского номера и замены sim-карты, а также обратиться в Банк для выявления возможных несанкционированных операций.
- Не устанавливайте на мобильный телефон, на который Банк отправляет SMS-сообщения с подтверждающим одноразовым паролем, приложения, полученные от неизвестных Вам источников. Помните, что банк не рассылает своим клиентам ссылки или указания на установку приложений через SMS/MMS/Email - сообщения.
- При работе с Системой убедитесь, что защищенное ssl-соединение установлено именно с официальным сайтом услуги (https://sbi.sberbank.ru:9443/ic), настоятельно не рекомендуется переходить на данную страницу по ссылке с Интернет-ресурсов (за исключением официальных ресурсов банка, например, www.sberbank.ru) или из поступивших по электронной почте писем.

Рекомендации для клиентов, использующих TLS-токен:

- Требования к хранению ПИН-кодов TLS-токена аналогичны требованиям к хранению ПИН-кодов банковских карт: никто кроме Вас не должен иметь доступ к конверту с ПИН-кодами. В случае их утери или кражи Вам следует незамедлительно обратиться в Банк.
- Используйте TLS-токены только в период работы с Системой, после окончания отключайте их от компьютера.
- Выполняйте незамедлительную блокировку и смену ключей ЭЦП в случаях их компрометации, а также по истечении срока действия ключей с периодичностью, установленной договорами и документацией.
- Заменяйте ключи ЭЦП во всех случаях увольнения или смены руководителей юридического лица, которые подписывали распоряжения (доверенность) о предоставлении полномочий по подписи электронных документов ЭЦП, а также при любом подозрении на компрометацию ключа ЭЦП.