Рекомендации

по мерам информационной безопасности при использовании системы дистанционного банковского обслуживания «iBank2»

АО «Тагилбанк» использует современные механизмы обеспечения безопасности, и предоставляет удобство пользования услугой дистанционного банковского обслуживания, обеспечивая при этом высокий уровень надежности и безопасности. Вместе с тем эффективность данных механизмов зависит от выполнения Вами простых правил:

1. Проверяйте web-адрес в адресной строке вашего браузера.

Сайт системы «iBank2» расположен на защищенном сервере, канал связи между Вашим компьютером и системой «iBank2» шифруется.

Адрес системы «iBank2»: https://ibank.tagilbank.ru/ (адрес начинается с «https://», а не с «http://»). Настоятельно рекомендуется переходить на данную страницу только по ссылке с официального сайта АО «Тагилбанк»: http://www.tagilbank.ru/.

Не используйте ссылки с других интернет-ресурсов или поступившие по электронной почте.

2. Подключайте носитель с ключами электронной подписи только на время работы в системе.

Не храните файл ключей электронной подписи на жестком диске компьютера. Используйте в качестве носителя ключа электронной подписи - съемный носитель (флеш-диски). При использовании в качестве носителя ключей электронной подписи флеш-дисков, не используйте их для хранения или переноса другой информации. Не оставляйте носитель ключа подключенным к компьютеру после завершения работы в системе «iBank2». Если злоумышленники получили удаленный или физический доступ к Вашему компьютеру и к нему подключен носитель ключа, они смогут самостоятельно составить платежный документ и подписать его в Ваше отсутствие и без Вашего ведома.

3. Никому не передавайте носитель с ключами и не сообщайте пароль от ключа и одноразовый пароль.

Не сохраняйте Ваш пароль в текстовых файлах на компьютере либо на других носителях информации, т.к. при этом существует риск его кражи и компрометации. Разрешите доступ к рабочему месту, только лицам, которые допущены к работе с системой "iBank2". Максимально ограничьте число сотрудников, допущенных к работе с ключами электронной подписи и местам хранения носителей ключей. Помните, что сотрудники АО «Тагилбанк» никогда и ни в какой форме не просят сообщить или ввести куда-либо Ваш пароль.

4. Включите услугу SMS-оповещение, которая позволит Вам отслеживать движение средств по счету.

5. При увольнении сотрудника, имевшего доступ к ключам электронной подписи:

- немедленно заблокируйте ключ и произведите его внеплановую смену,

- при необходимости измените номер телефона / адрес электронной почты, на которые настроено SMS-оповещение о входе в систему и о движении средств по счету,

- при необходимости предоставьте в АО «Тагилбанк» информацию об актуальных контактных данных, используемых для уведомления о совершении операций с использованием системы «iBank2».

6. Ограничьте работу с другими Интернет-ресурсами с компьютера, используемого для доступа к системе «iBank2».

Исключите на компьютере, на котором осуществляется подготовка и отправка платежных документов в АО «Тагилбанк», использование систем удаленного управления. Не привлекайте для администрирования и обслуживания данного компьютера персонал на условиях предоставления ему удаленного доступа. Исключайте посещение с компьютера, 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 ограничьте “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, серверы обновлений системного и антивирусного ПО. Риск хищения и дальнейшего неправомерного использования ключа электронной подписи и паролей к нему значительно увеличивается при доступе к системе «iBank2» с гостевых рабочих мест (интернет-кафе, общедоступные точки доступа и т.д.)

7. Используйте современное лицензионное антивирусное программное обеспечение.

Регулярно, перед началом работы с системой «iBank2», обновляйте антивирусные базы. Проводите регулярную (не реже одного раза в неделю) полную антивирусную проверку Вашего компьютера для своевременного обнаружения вредоносных программ. Любое антивирусное программное обеспечение эффективно только при выполнении данных рекомендаций.

8. Устанавливайте самые последние обновления Вашего браузера и операционной системы.

Используйте только лицензионное программное обеспечение. Помните, использование нелицензионного программного обеспечения это не только правонарушение, но и лазейка в системе Вашей безопасности, которой могут воспользоваться мошенники.

Выполнение Вами данных мероприятий позволит значительно снизить риски совершения несанкционированных операций в системе «iBank2».

При любых подозрениях на компрометацию ключа электронной подписи, а также при возникновении любых необычных ситуаций при работе, проблем с доступом к системе «iBank2» – немедленно обратитесь в АО «Тагилбанк» по телефонам:

+7 (3435) 977-000 (многоканальный номер с голосовым меню),

+7 (3435) 977-602,

+7 (3435) 977-616,

либо по телефонам сотрудников операционного отдела АО «Тагилбанк», выполняющих обслуживание Вашего счета.