Коммерческий Международный Профильный Банк

Рекомендации по снижению рисков повторного осуществления перевода денежных средств без добровольного согласия клиента

1. Отключать, извлекать носители с ключами электронной подписи (usb- токены), если они не используются для работы с Системой «iBank2».

2. Не пользоваться Системой «iBank2» с гостевых рабочих мест. При использовании гостевых рабочих мест повышается риск несанкционированного использования ключей электронной подписи и паролей.

3. Ограничить доступ к компьютерам, используемым для работы с Системой «iBank2» и исключить к ним доступ персонала, не работающего с Системой «iBank2». По возможности исключить/ограничить удаленное управление компьютером с Системой «iBank2».

4. На компьютерах, используемых для работы с Системой «iBank2», исключить посещение интернет-сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения. Указанные сайты и программное обеспечение могут содержать вредоносное программное обеспечение, предназначенное для кражи денежных средств. По возможности, полностью запретить все соединения (входящие и исходящие) с сетью Интернет, разрешив только доступ к необходимым ресурсам.

5. Убедиться перед вводом своих данных на сайте Банка, что соединение установлено с официальным сайтом Банка в информационно – телекоммуникационной сети «Интернет» (далее – Сайт Банка) по адресу https://profitbank.ru/. Для этого необходимо проверить правильность указания адреса Сайта Банка в строке браузера и наличие сертификата безопасности (https в адресной строке).

6. Использовать только лицензионное программное обеспечение или свободно распространяемое программное обеспечение с официальных сайтов (операционные системы, офисные пакеты и пр.).

7. Обеспечить автоматическое обновление системного и прикладного программного обеспечения.

8. Применять на рабочем месте лицензионные средства антивирусной защиты, обеспечить возможность автоматического обновления антивирусных баз, а также еженедельную полную антивирусную проверку.

9. Исключить обслуживание компьютеров, используемых для работы с Системой «iBank2», случайными сотрудниками технической поддержки.

10. При обслуживании компьютера сотрудниками технической поддержки обеспечивать контроль за выполняемыми ими действиями.

11. Никогда не передавать ключи электронной подписи сотрудникам технической поддержки для проверки работы Системы «iBank2», проверки настроек взаимодействия с Банком и т.п. При необходимости таких проверок владелец ключа электронной подписи лично должен подключить носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентской части Системой «iBank2», и лично ввести пароль.

12. При увольнении ответственного сотрудника или сотрудника технической поддержки, имевшего доступ к ключу электронной подписи, обязательно позвонить в Банк с уведомлением о приостановлении использования электронного средства платежа (ключа электронной подписи). При необходимости, выпустить новый ключ электронной подписи.

13. При увольнении сотрудника технической поддержки, осуществлявшего обслуживание компьютеров, используемых для работы с Системой «iBank2», убедиться в отсутствии вредоносных программ на компьютерах.

14. При общении с сотрудниками Банка пользуйтесь только теми телефонами, которые указаны на Сайте Банка по адресу https://profitbank.ru/.