Памятка по информационной безопасности при хранении ключей ЭП на USB-токене.

Уважаемые клиенты.

В целях повышения безопасности работы с системой «iBank 2» обращаем Ваше внимание на необходимость соблюдения следующих мер предосторожности:

Немедленно извлекайте USB-токен из USB-порта персонального компьютера, после завершения сеанса работы**.**

Ключи, имеющие право подписи и находящиеся в одном из сочетаний подписей, сохраняйте на разные USB-токены и при формировании платежных документов используйте их последовательно.

При каждом входе в систему проверяйте предыдущие сеансы работы.

Помните, что программное обеспечение системы Интернет-Банкинга «iBank 2» **никогда** не выводит на экраны компьютера сообщение о временной неработоспособности системы. Сообщения типа: ***«На сервере банка ведутся профилактические работы»,*** свидетельствуют о том, что Ваш компьютер заражен вредоносным ПО. При возникновении любых подозрений на наличие в компьютере вредоносных программ **немедленно** позвоните в банк и заблокируйте ключи, прекратите использование данного компьютера для работы в системе «iBank 2» до ликвидации вирусного заражения.

Используйте и регулярно обновляйте антивирусное ПО, персональные файрволлы, средства защиты от несанкционированного доступа и т.п. Проводите полное сканирование компьютера на наличие вирусов на регулярной основе и при смене персонала, имевшего доступ к нему.

Не устанавливайте на компьютере, используемом для работы в системе, средства удаленного управления компьютером.

Соблюдайте правила информационной безопасности при работе в Интернете – не посещайте подозрительные сайты, не устанавливайте программы из недостоверных источников, не открывайте файлы от неизвестных отправителей и пр.

Используйте системное и прикладное ПО, полученное из источников, гарантирующих отсутствие вредоносных программ.

Ограничьте физический доступ к компьютерам, используемым для работы с «iBank 2»**.**

Не передавайте личный USB-токен сотрудникам или иным лицам. Храните в тайне пароли от ключей ЭП. При осуществлении настроек взаимодействия с банком и т.п., проводимых ИТ-специалистами, владелец ключа ЭП должен сам подключить USB-токен к компьютеру и лично ввести пароль, исключая возможность его подсматривания**.**

При увольнении ответственного сотрудника, имевшего доступ к ключу ЭП, обязательно заблокируйте ключи проверки ЭП и сгенерируйте новые.

Если у Вас возникли подозрения, что доступ к компьютеру и USB-токену могли получить неуполномоченные лица, немедленно позвоните в банк и заблокируйте ключи.

Телефон службы технической поддержки +7(861)279-17-46.