**Памятка по информационной безопасности при работе**

**в системе «iBank 2» для физических лиц**

Настоящей памяткой Банк в целях повышения безопасности работы в системе «iBank 2» обращает Ваше внимание на необходимость соблюдения следующих мер предосторожности:

1. Никогда не открывать сайт системы «iBank 2» по ссылкам полученным через электронную почту или баннерным сайтам, поскольку существует множество способов фальсифицировать адрес. Необходимо использовать адрес сайта, предоставленный Банком или полученный через корпоративный сайт Банка.
2. Не отвечать на подозрительные письма с просьбой выслать номер карты, CVC или ПИН код карты, имя пользователя, пароль, номер телефона и другие конфиденциальные данные. Банк никогда не запрашивает у Клиента конфиденциальную информацию по электронной почте или посредством телефонных звонков или SMS, это действия злоумышленников.
3. Программное обеспечение системы «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 предположительно заражен вредоносным ПО. При возникновении любых подозрений на наличие в компьютере вредоносных программ немедленно прекратите использование данного компьютера для работы в системе «iBank 2».
4. Рекомендуется исключить посещение Интернет-сайтов сомнительного содержания, открытие подозрительных файлов, переход по ссылкам электронных писем от ненадежных отправителей, работу с непроверенными носителями информации и так далее.
5. Использовать на рабочих местах современные лицензионные операционные системы. Обеспечить регулярное обновление операционной системы.
6. Использовать лицензионное и оперативно обновлять специализированное ПО для защиты информации – антивирусное ПО, персональные межсетевые экраны, средства защиты от несанкционированного доступа и т.п. На регулярной основе проводить полное сканирование компьютера, либо смартфона на наличие вирусов. Не использовать скомпрометированную учетную запись.
7. По возможности не устанавливать на компьютере, используемом для работы в системе, средства удаленного управления компьютером.
8. Не сообщать никому информацию о логине и паролях, коде доступа и исключить доступ третьих лиц к средству получения одноразовых паролей, даже если представляются сотрудниками Банка. Не сообщать свой одноразовый пароль никому. Не записывайте коды и пароли на бумажных носителях, доступных другим лицам.
9. Не передавать третьим лицам SIM-карту с номером мобильного телефона, указанным в Заявлении, который используется для получения кодов, паролей. При смене телефонного номера указанного в Заявлении сообщите об этом в Банк чтобы ваши данные не попали новому владельцу номера. Подключайте СМС сервис Мобильный банк только на свой номер телефона. Переводите деньги только известным вам получателям.
10. Осуществляйте постоянный контроль за отправляемыми платежными документами посредством системы «iBank2», а также состоянием Вашего счета.