Памятка клиента о мерах безопасного использования Системы Интернет-Банк

Для минимизации рисков при работе в Системе Интернет-Банк рекомендуется соблюдение следующих правил.

1.1. Никогда не передавать третьим лицам информацию, которую они могут использовать для несанкционированного доступа к Вашим данным, хранящимся в системе дистанционного банковского обслуживания, и исключить иные возможности получения указанной информации третьими лицами, в том числе сотрудниками Банка.

1.2. Не хранить пароль на вход в Систему Интернет-Банк непосредственно на компьютере.

1.3. Обязательно сменить пароль в Систему Интернет-Банк при первом входе.

1.4. Осуществлять информационное взаимодействие с Банком только с использованием средств связи, реквизиты которых оговорены в документах, получаемых непосредственно от Банка или иных официальных информационных источниках (особенно при использовании электронной почты).

1.5. Незамедлительно информировать Банк при возникновении подозрений о компрометации пароля на вход в систему или осуществлении попытки несанкционированного доступа к Системе Интернет-Банк под Вашей учетной записью.

1.6. Необходимо немедленно изменить пароль на вход в систему в случаях его компрометации или подозрения на компрометацию.

1.7. Использовать современные средства обеспечения информационной безопасности при работе в сети Интернет (антивирусное программное обеспечение, персональные межсетевые экраны и т. п.) и своевременно устанавливать обновления, выпускаемые разработчиками антивирусного программного обеспечения, операционной системы, web-браузеров (Google Chrome, Microsoft Internet Explorer, Mozilla FireFox, Opera, Safari и т.д.).

1.8. Привлекать специалистов должной квалификации для настройки работы компьютера с которого осуществляется работа с Системой Интернет-Банк и установки/настройки антивирусного программного обеспечения на нём, устанавливать и запускать только программное обеспечение заслуживающее доверие.

1.9. Желательно при плановом длительном неиспользовании Системы Интернет-Банк блокировать работу в ней.

1.10. Необходимо учитывать, что при доступе к Системе Интернет-Банк с гостевых рабочих мест (интернет-кафе и т.д.) существенно увеличивается риск хищения и дальнейшего неправомерного использования аутентификационной информации.

1.11. Сотрудничать с Банком в принятии последним мер, направленных на минимизацию рисков при дистанционном банковском обслуживании, в том числе выполнять рекомендации Банка, касающиеся обеспечения безопасности работы в Системе Интернет-Банк.

1.12. В случае отсутствия возможности подключения к веб-сайту Банка при наличии действующего соединения с сетью Интернет сообщать об этом в Банк по контактному телефону Банка.

Следует помнить и учитывать, что большинство случаев хищения логинов и паролей осуществляются:

- лицами, имевшими доступ к Вашему компьютеру, с которого осуществлялась работа в системе дистанционного банковского обслуживания;
- злоумышленниками путем заражения через сеть Интернет компьютеров клиентов вредоносными программами с последующим хищением учетных данных и паролей клиентов.

Со своей стороны Банк полностью осознаёт необходимость принятия адекватных мер по обеспечению безопасности работы клиентов с Системой Интернет-Банк и делает всё возможное для вашей безопасности, уверенности и спокойствия.