Безопасность при работе в интернете

Убедитесь, что ваш компьютер не заражён какими-либо вирусами. Установите и активизируйте антивирусные программы, старайтесь их постоянно обновлять. Только постоянное обновление антивирусных программ позволит вам своевременно обнаружить и предотвратить появление вируса.

Рекомендуется использовать программное обеспечение, которое отслеживает и борется с программным обеспечением Spyware. Spyware — вид программного обеспечения, который пытается запомнить ваши клавиатурные последовательности и передать их третьим лицам.

Настоятельно рекомендуется использование виртуальной клавиатуры при вводе пароля на всех этапах работы с Интернет-банком. Использование виртуальной клавиатуры позволит избежать компрометации пароля в случае заражения ПК программным обеспечением Spyware.

Рекомендуется использовать межсетевой экран (firewall) при входе в интернет или установить персональный межсетевой экран (firewall) на вашем компьютере. При использовании межсетевого экрана (firewall) несанкционированный вход в систему вашего компьютера через интернет будет весьма затруднен или предотвращён.

Используйте программное обеспечение (операционные системы, приложения) из проверенных и надёжных источников. Откажитесь от использования и инсталляции программного обеспечения из непроверенных источников.

В случае подключения через модем обратите, пожалуйста, внимание на набираемый номер. В случае обнаружения несовпадения номера удалите неизвестный вам номер.

Сконфигурируйте ваш обозреватель таким образом, чтобы установки настройки кэширования не допускали сохранения конфиденциальных страниц (SSL-page).

Контролируйте свою электронную почту, не открывайте сообщения от неизвестных адресатов, не передавайте свои личные данные. Никогда не открывайте подозрительные файлы, присланные вам по электронной почте. Не отвечайте на электронные письма, в которых якобы от имени банка, вас просят предоставить персональную информацию. Никогда не следуйте по ссылкам в таких письмах (даже на сайт банка), т.к. они могут вести на мошеннические сайты.

Проверяйте адреса интернет-сайтов, к которым вы подключаетесь, т.к. злоумышленники могут использовать похожие названия для создания мошеннических ресурсов.

Избегайте пользоваться услугами интернет-ресурсов сомнительного содержания; зачастую они создаются специально для получения информации о банковских картах и последующего ее неправомерного использования.

Совершайте покупки только со своего компьютера, не пользуйтесь интернет-кафе и другими доступными средствами, где могут быть установлены программы-шпионы, запоминающие вводимые вами конфиденциальные данные.

Выбирайте нетривиальные пароли, которые не связаны с вашим днем рождения или другими персональными данными. Если возможно, выбирайте символьно-цифровые пароли. Не записывайте пароли и никому не сообщайте их. Если вы боитесь забыть свой пароль, придумайте понятную только вам систему его записи (например, в виде номера телефона или адреса в телефонной книжке).

Банк никогда не осуществляет рассылку электронных писем с просьбой предоставить конфиденциальную информацию, или таких, которые содержат компьютерные программы.

Если вы получили письмо от имени банка, содержание которого вызывает подозрение, либо с вами связались по телефону от имени банка, с просьбой установить некоторое программное обеспечение, просьба связаться со службой поддержки банка и уточнить ситуацию. Всегда используйте контактную информацию служб поддержки банка, указанную в официальных источниках информации, и не используйте контактную информацию, указанную в полученном письме или полученную в ходе телефонного разговора.

Любые электронные сообщения, отправленные с бесплатных почтовых служб интернета (@mail.ru, @yandex.ru, @rambler.ru, @gmail.com, @yahoo.com и т.п.), не являются почтой, отправленной банком.