# Памятка клиента по обеспечению безопасности при работе в системах дистанционного банковского обслуживания

Для минимизации рисков при работе в системе дистанционного банковского обслуживания (далее ДБО) просим Вас:

- 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;
- не хранить пароль на вход в систему ДБО непосредственно на компьютере;
- не используйте функцию автозаполнения в Вашем браузере, это позволит не сохранять конфиденциальную информацию о логине и пароле в памяти браузера, что предотвратит возможность ее использования посторонними лицами;
- обязательно сменить пароль в систему ДБО при первом входе;
- при работе с Системой убедитесь, что соединение с ней осуществляется в защищенном режиме. Признаком использования защищенного соединения является наличие справа или слева от адресной строки, либо справа вверху/внизу строки браузера изображения значка закрытого замка.
- не использовать ПИН при заказе товаров и услуг через сеть Интернет, а также по телефону/факсу.
- рекомендуется совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и (или) информации о банковской(ом) карте (счете).
- в случае если покупка совершается с использованием чужого компьютера, не рекомендуется сохранять на нем персональные данные и другую информацию, а после завершения всех операций нужно убедиться, что персональные данные и другая информация не сохранились (вновь загрузив в браузере web-страницу продавца, на которой совершались покупки).
- осуществляйте 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);
- незамедлительно информируйте Банк при возникновении подозрений о компрометации пароля на вход в систему или осуществлении попытки несанкционированного доступа к системе Интернет-банк под Вашей учетной записью, об утере карты, о пришедших SMS -сообщениях по операциям которые Вы не совершали;
- используйте современные средства обеспечения информационной безопасности при работе в сети интернет (программное обеспечение защиты от вредоносного кода, персональные межсетевые экраны и т. п.);
- желательно при плановом длительном неиспользовании системы ДБО блокировать работу в ней;
- корректно завершайте работу в Системе. Завершение работы выполняется путем выбора соответствующего пункта меню «Выйти из системы» - это удалит из браузера информацию о параметрах Вашей работы в Системе
- сотрудничайте с Банком в принятии мер, направленных на минимизацию рисков при дистанционном банковском обслуживании, в том числе выполняйте рекомендации банка, касающиеся обеспечения безопасности работы в системе ДБО.

**Рекомендации по защите от вредоносного кода**

- использовать лицензионное и регулярно обновляемое программное обеспечение для защиты от вредоносного кода, установить автоматический режим обновления программного обеспечения и баз сигнатур;
- установить автоматическое обновление других используемых Вами программных продуктов (операционной системы, браузеров и прикладных программ);
- установить режим автоматической проверки на вредоносный код, в том числе ежедневное сканирование файлов и программных модулей;
- при подозрении на наличие вредоносного кода запустите полную проверку Вашего компьютера;
- отключите автозагрузку с внешних носителей, таких как флешки, компакт-диски и др. ;
- не посещайте сомнительные сайты;
- для работы в Интернет используйте пользовательские учетные записи, а не учетную запись администратора компьютера;
- не отключайте настройки средств обеспечения информационной безопасности.

**Рекомендации для защиты от несанкционированного доступа с использованием злоумышленниками ложных ресурсов Интернет**

Обязательно убедитесь в правильности адресов интернет-сайтов, к которым подключаетесь и на которых собираетесь совершить покупки, т.к. похожие адреса могут использоваться для осуществления неправомерных действий.

При совершении попыток неправомерного получения персональной информации пользователей систем ДБО клиентам кредитных организаций по системам электронной почты направляются сообщения, в которых под какими-либо предлогами (техническое перевооружение организации, обновление или сверка баз данных кредитной организации и т.п.) предлагается ввести с клавиатуры компьютера указанные коды в поля экранных форм в ходе имитируемых сеансов информационного взаимодействия с кредитной организацией (к примеру, через созданный дубликат ее web-сайта). Одновременно на компьютер клиента с web-сайта могут передаваться вредоносные программы, являющиеся компьютерными вирусами или "закладками", выполняющими в фоновом режиме работы скрытые функции, связанные с неправомерным получением персональной информации пользователей систем ДБО.

В целях неправомерного получения персональной информации пользователей систем ДБО заинтересованные лица используют также различные варианты телефонного мошенничества. В частности, отмечаются случаи направления мошенниками на мобильные телефоны клиентов кредитных организаций SMS-сообщений о необходимости позвонить по номерам телефонов, которые в действительности не принадлежат этим организациям. Также имеют место звонки клиентам с сообщением автоинформаторов о предоставлении продуктов и услуг банка с предложением нажать определенные клавиши на телефоне для подтверждения согласия в их приобретении и т.п. Тем самым клиенты банка провоцируются к вступлению в контакты с мошенниками, целью которых в том числе может являться получение конфиденциальной клиентской информации (например, номера банковской карты и ПИН-кода).