Рекомендации клиентам по защите информации при использовании системы «Интернет-Банк» и проведении операций с банковскими картами в сети Интернет

1. Рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносного кода) в целях противодействия осуществлению переводов денежных средств без согласия клиента.

В сети Интернет получили широкое распространение специализированные вредоносные программы (трояны), обеспечивающие возможность похищения у пользователей системы дистанционного банковского обслуживания (далее - ДБО) «Интернет-Банк» (далее - Системы) секретные данные клиента (учетные записи доступа/идентификаторы - пароль, логин, данные карты переменных кодов и т.п.), с последующим формированием удаленного доступа и перехватом управления компьютером.

Во исполнение «Условий банковского обслуживания клиентов с использованием системы «Интернет-Банк» клиент подключается к Личному кабинету в Системе самостоятельно через Интернет (https://ib.apkbank.ru), путем введения Логина и Пароля. При первом обращении к Системе ДБО Банк обязывает изменять текущий клиентский пароль на новый, известный только клиенту. Для предотвращения компрометации и несанкционированного использования злоумышленниками данных клиента необходимо предпринимать меры предосторожности и тщательно оберегать личные идентификаторы и учетные записи. В случае возникновения подозрений о компрометации секретных данных, клиенту необходимо незамедлительно поставить в известность Банк обо всех случаях подозрений или инцидентах с защищаемой информацией. Обращаем внимание, что компрометацией считается также передача третьим лицам информации о личных идентификаторах/учетных записях доступа, реквизитов банковских карт.

Вредоносные коды и вирусные программы распространяются через различные ресурсы Интернета, такие как: электронная почта, каналы сервисов мгновенной передачи сообщений, зараженные сайты и т.п. Инфицированный вредоносным кодом компьютер может быть источником утечки различных защищаемых данных: личная информация пользователя, идентификаторы, пароли доступа, реквизиты банковских карт и т.п. Использование украденных/скомпрометированных личных данных позволит злоумышленникам совершать платежные операции от имени Клиента.

Необходимо помнить, что при работе с электронной почтой не следует открывайте письма и вложения к ним, полученные от неизвестных отправителей, и переходить по содержащимся в таких письмах ссылкам.

Для обеспечения бесперебойной работы и надежной защиты персональных компьютеров необходимо использовать только лицензионное программное обеспечение и официальные антивирусные программы с регулярным обновлением.

Требования к конфигурации устройства, посредством которого совершаются действия по исполнению электронных поручений Клиента с использованием Системы, приведены в «Условиях банковского обслуживания клиентов с использованием системы «Интернет-Банк»:

1. Антивирусное программное обеспечение должно запускаться автоматически, с загрузкой операционной системы. Рекомендуется полная ежедневная проверка компьютера на наличие вирусов и иного вредоносного программного обеспечения. Необходимо исключить использование зараженного компьютера, вплоть до полного излечения от вирусов.
2. При выходе в Интернет необходимо использовать сетевые экраны, разрешив доступ только к доверенным ресурсам сети Интернет.
3. При работе в Интернете запретить установку каких-либо сомнительных программ.
4. Исключить использование программ онлайнового общения на компьютере, использующемся для работы в системе дистанционного банковского обслуживания.
5. Запретить доступ к компьютеру третьих лиц и установку любых программных продуктов посторонними лицами.
6. Обеспечить информационный обмен в сети Интернет только с надёжными информационными порталами и проверенными корреспондентами электронной почты.
7. Надёжным средством обеспечения подлинности является цифровая подпись либо значение переменного кода, предоставленного Банком.
8. Исключить просмотр электронных сообщений и активацию ссылок от незнакомых адресатов.
9. При подозрениях на наличие вирусов на персональном компьютере (в частности, неожиданных «зависаниях», перезагрузках, сетевой активности), полностью воздержаться от использования Системы и проведения платежей, в том числе с помощью банковских платежных карт до исправления ситуации. Незамедлительно проинформировать Банк о возможных нарушениях в Системе.
10. Пользователям системы «Интернет-Банк» и держателям банковских карт рекомендуется использовать услуги SMS-информирования либо E-mail-информирования, а также регулярно формировать выписку по счетам в Системе в целях получения своевременной информации о совершаемых операциях по счетам и банковским картам.

***2.* Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет или в случае утраты, потери, хищения средств идентификации для совершения действий в целях осуществления банковской операции.**

Необходимо помнить и соблюдать меры безопасности при формировании расчетов в сети Интернет.

Следует быть внимательным при обращении к личным электронным платежным кабинетам и ссылкам на сайты Банка, так как, зачастую, мошенники подделывают официальные интернет страницы известных сайтов, формируя точные копии с целью получения персональных данных и реквизитов банковских карт клиентов.

В случае, если клиентом были обнаружены: ложный web-сайт Банка, отличный от ссылки - http://apkbank.ru или мошенники пытаются связаться по электронной почте или иным способом лица с требованиями о предоставлении персональных идентификаторов доступа к Системе, необходимо незамедлительно сообщить об этом в Call-центр Банка или Службу поддержки ДБО или держателей банковских карт АО КБ «АГРОПРОМКРЕДИТ» по телефонам:+7(495) 755-80-08, 8-800 –100–80–08, направить электронное письмо Службе технической поддержки по адресу: ibank@apkbank.ru.

В целях предотвращения несанкционированного доступа к защищаемой информации в случае утраты, потери, хищения средств идентификации (пароля, логина, переменных кодов и т.п.) для совершения действий в целях осуществления банковской операции необходимо незамедлительно обратиться Call-центр и/или Службу поддержки ДБО или держателей банковских карт по указанным выше телефонам и/или электронному адресу в целях осуществления блокировки средств доступа или банковской карты.

После дистанционного информирования Банка, необходимо лично обратиться в ближайший офис для оформления Заявления «на блокировку/разблокировку и получение средств доступа в систему «Интернет-Банк» либо «Заявления о несогласии с транзакцией».

На основании рассмотрения заявления Банком будет проведена претензионная работа с предоставлением мотивированного суждения по операциям, совершенным с использованием утраченных, похищенных средств идентификации или банковской карты в соответствии с требованиями «Условий банковского обслуживания клиентов с использованием системы «Интернет-Банк», а также «Правил пользования международными банковскими картами АО КБ «АГРОПРОМКРЕДИТ»» (распространяются на платежную систему «Мир» и расчеты с использованием карт «Мир») либо «Правил пользования международными банковскими картами АО КБ «АГРОПРОМКРЕДИТ» с предоставлением Клиенту овердрафта с льготным периодом уплаты процентов».

В целом, разработка и реализация комплекса мер по обеспечению информационной безопасности - сложная задача, требующая непрерывной работы квалифицированных специалистов. Соблюдение перечисленных мероприятий позволит существенно снизить риски, связанные с использованием системы «Интернет-Банк», осуществлением платежей в сети Интернет с использованием платежных карт и предотвратить хищение денежных средств Клиента.

3. Рекомендации по снижению рисков получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами.

При подключении к сети Интернет велика вероятность заражения используемого оборудования вредоносными программами, которые распространены в сети, и используются злоумышленниками для кражи у пользователей Системы файлов с паролями, логинами, данными переменных кодов. У держателей пластиковых карт[1] может быть похищена информация о реквизитах банковских платежных карт, что позволит мошенникам совершать операции от имени Клиента. Использование лицензионного антивирусного программного обеспечения со своевременным автоматическим обновлением позволит существенно снизить риски потери защищаемой информации.

Пользователям системы «Интернет-Банк» и держателям банковских карт рекомендуется воспользоваться услугой SMS-информирования либо E-mail-информирования, а также регулярно формировать выписку по счетам в Системе в целях получения своевременной информации о совершаемых операциях по счетам и банковским картам.

При совершении операций с помощью банковской карты в банкоматах, в торгово-сервисных точках или сети Интернет пользуйтесь устройствами, платёжными аппаратами и сетевыми ресурсами, заслуживающими доверия.

Нельзя сообщать ПИН-код банковской карты третьим лицам, в том числе родственникам, знакомым, сотрудникам кредитной организации, кассирам и лицам, помогающим в использовании банковской карты.

Недопустимо записывать и хранить ПИН-код с банковской картой.

С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета целесообразно установить суточный лимит на сумму операций по банковской карте и одновременно подключить электронную услугу оповещения о проведенных операциях (например, оповещение посредством SMS-сообщений или иным способом).

Следует помнить, что недопустим ввод личного ПИН-кода на устройствах считывания на входе в помещения банкоматной зоны.

Для предотвращения компрометации секретных данных личной банковской карты в случае безналичной оплаты товаров и/или услуг необходимо требовать проведения операций с банковской картой только в присутствии собственника карты.

При использовании банковской карты для оплаты товаров и услуг кассир может потребовать от владельца банковской карты предоставить паспорт, подписать чек или ввести ПИН-код. Перед набором ПИН-кода следует убедиться в том, что вводимая информация будет визуально недоступна для лиц, находящихся в непосредственной близости. Перед подписанием чека, необходимо в обязательном порядке проверить сумму, указанную на чеке.

При совершении операций с банковской картой через сеть Интернет запрещено использование и ввод ПИН-кода.

С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета рекомендуется для оплаты покупок в сети Интернет использовать отдельную банковскую карту с предельным лимитом, предназначенную только для указанной цели.

При получении подозрительных SMS-сообщений, имитирующих информацию от Банка (о заблокированной банковской карте, о взломе ПИН-кода, о непогашенном кредите и т.п.), не следует звонить и отправлять ответные SMS-сообщения по указанным во входящем сообщении номерам. При выявлении подобных случаев необходимо связаться со Службой клиентской поддержки по номерам телефонов, указанным на оборотной стороне банковской карты и/или на официальном интернет-сайте Банка, а также проинформировать оператора Службы поддержки держателей банковских карт о случившемся.

Необходимо помнить, что сотрудникам Банка запрещено запрашивать реквизиты банковских карт Клиента (номер, срок действия, CVV-код, ПИН-код и т.п.).

Обращаем внимание, что своевременное обращение в Банк позволит сохранить личные средства Клиента и принять оперативные меры по предотвращению мошеннических действий.

[1] Держателям банковских карт рекомендуем ознакомиться с «Памяткой о мерах безопасного использования банковских карт»