ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

ПИСЬМО
от 7 декабря 2007 г. N 197-Т

О РИСКАХ ПРИ ДИСТАНЦИОННОМ БАНКОВСКОМ ОБСЛУЖИВАНИИ

Банк России отмечает, что в последнее время в российском сегменте сети Интернет участились сетевые атаки на сайты и серверы (далее - ресурсы) кредитных организаций, а также попытки неправомерного получения персональной информации пользователей систем дистанционного банковского обслуживания (далее - ДБО) (пароли, секретные ключи средств шифрования и аналогов собственноручной подписи, ПИН-коды и номера банковских карт, а также персональные данные их владельца).

Наиболее распространенными являются распределенные атаки типа "отказ в обслуживании", при которых большое количество компьютеров (от нескольких сотен до сотен тысяч), программное обеспечение которых предварительно специальным образом дистанционно модифицируется лицами, предпринимающими попытки неправомерного получения персональной информации пользователей систем ДБО, по команде указанных лиц начинают одновременно направлять массовые запросы на атакуемый ресурс, серьезно нарушая либо полностью блокируя его работу. При этом владелец ресурса, как правило, не может самостоятельно, без помощи провайдера Интернета, восстановить работоспособность ресурса. Продолжительность атак может составлять несколько суток, в течение которых оказывается невозможным ДБО множества клиентов кредитной организации, что может нанести прямой ущерб этой организации и ее клиентам.

В связи с изложенным Банк России считает целесообразным рекомендовать кредитным организациям включать в договоры, заключаемые с провайдерами Интернета, обязательства сторон по принятию мер, направленных на оперативное восстановление функционирования ресурса при возникновении нештатных ситуаций, а также ответственности за несвоевременное исполнение таких обязательств.

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.

Наблюдаются случаи неправомерного получения реквизитов банковских карт при проведении операций через банкоматы. При этом используются накладные устройства на клавиатуру для ввода ПИН-кода или на устройство для приема карт в банкомат, а также специально приспособленные для этих целей "фальшивые" банкоматы, которые незаконно устанавливаются, как правило, в не контролируемых кредитными организациями местах и внешне не отличаются от банкоматов, используемых для ДБО клиентов кредитных организаций.

Неправомерно полученные различными способами реквизиты банковских карт используются для изготовления поддельных банковских карт, частично (так называемый "белый пластик") или полностью имитирующих подлинные. При использовании в банкоматах поддельные банковские карты предоставляют их обладателям все возможности подлинных банковских карт.

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).

В связи с изложенным Банк России обращает внимание кредитных организаций на необходимость распространения предупреждающей информации для своих клиентов, в том числе с использованием представительств в сети Интернет (web-сайтов), о возможных случаях неправомерного получения персональной информации пользователей систем ДБО. В состав такой информации целесообразно включать описание официально используемых способов и средств информационного взаимодействия с клиентами, а также описания приемов неправомерного получения кодов персональной идентификации клиентов, информации о банковских картах и мер предосторожности, которые необходимо соблюдать клиентам, пользующимся системами ДБО. В качестве подобных мер кредитные организации могли бы, например, рекомендовать клиентам:

- исключить возможность неправомерного получения персональной информации пользователей систем ДБО (не передавать неуполномоченным лицам);
- осуществлять операции с использованием банкоматов, установленных в безопасных местах (в государственных учреждениях, подразделениях банков, крупных торговых комплексах, гостиницах, аэропортах и т.п.);
- не использовать банковские карты в организациях торговли и обслуживания, не вызывающих доверия;
- при совершении операций с банковской картой без использования банкоматов не выпускать ее из поля зрения;
- не пользоваться устройствами, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат;
- не использовать ПИН-код при заказе товаров либо услуг по телефону/факсу или по сети Интернет;
- при наличии возможности, предоставляемой кредитной организацией, использовать реквизиты карты одноразового использования (так называемой "виртуальной карты") для осуществления оплаты товаров либо услуг через сеть Интернет;
- пользоваться услугой SMS-оповещения о проведенных операциях с применением ДБО (в случае возможности получения такой услуги);
- осуществлять информационное взаимодействие с кредитной организацией только с использованием средств связи (мобильные и стационарные телефоны, факсы, интерактивные web-сайты/порталы, обычная и электронная почта и пр.), реквизиты которых оговорены в документах, получаемых непосредственно в кредитной организации.

Настоящее письмо подлежит опубликованию в "Вестнике Банка России".

Доведите содержание настоящего письма до сведения кредитных организаций.

Первый заместитель
Председателя банка России
Г.Г.МЕЛИКЬЯН