Рекомендации
клиентам «Тимер Банка» (ПАО) по защите информации при пользовании пластиковыми картами, системой дистанционного банковского обслуживания

Рекомендации по защите информации от воздействия вредоносного кода.

В сети Интернет получили широкое распространение специализированные вредоносные программы (трояны), обеспечивающие возможность похищения у пользователей системы дистанционного банковского обслуживания файлов с секретными ключами электронной цифровой подписи (ЭЦП) и паролей. У держателей пластиковых карт может быть похищена информация о реквизитах карты. Трояны распространяются через электронную почту, по каналам сервисов мгновенной передачи информации через принадлежащие злоумышленникам сайты. При этом злоумышленники похищают ключи ЭЦП, пароли доступа, реквизиты банковских карт, что позволяет совершать операции от имени клиента.

При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

Пользуйтесь персональными компьютерами с установленным лицензионным программным обеспечением.

Своевременно обновляйте установленное программное обеспечение и операционную систему (установка критичных обновлений).

Обязательно установите и своевременно обновляйте на компьютере антивирусное программное обеспечение, но помните, что ни одна антивирусная программа не обеспечивает 100% защиты.

Антивирусное программное обеспечение должно запускаться автоматически, с загрузкой операционной системы. Рекомендуется полная ежедневная проверка компьютера на наличие вирусов, иного вредоносного программного обеспечения. Исключить использование зараженного компьютера, вплоть до полного излечения от вирусов.

При выходе в Интернет используйте сетевые экраны, разрешив доступ только к доверенным ресурсам сети Интернет.

При работе в Интернете не соглашайтесь на установку каких-либо сомнительных программ.

Воздерживайтесь от использования программ онлайнового общения на компьютере, использующемся для работы в системе дистанционного банковского обслуживания.

Исключите возможность установки посторонними лицами (гостями, посетителями) на компьютер специальных «шпионских» программ. В частности, хорошей практикой является работа на компьютере от имени пользователя, не имеющего полномочий администратора.

Рекомендуем ограничить информационный обмен в сети Интернет только надёжными информационными порталами и проверенными корреспондентами электронной почты.

Важно знать, что надёжным средством обеспечения подлинности является цифровая подпись, а не строка адреса браузера или электронной почты. Часто, в виде «интересной ссылки» в письме, от якобы знакомого приходит вредоносная программа. Часто вредоносная программа скрывается под всплывающим окном рекламной ссылки на сайте.

При подозрениях на наличие вирусов на персональном компьютере (в частности, неожиданных «зависаниях», перезагрузках, сетевой активности), полностью воздержаться от использования системы дистанционного банковского обслуживания и проведения платежей с помощью банковских платежных карт до исправления ситуации.

Пользователям системы дистанционного банковского обслуживания рекомендуется воспользоваться дополнительными бесплатными услугами, предоставляемыми «Тимер Банком» (ПАО), по фильтрации ip-адресов, mac адресов, с которых разрешён доступ в систему ДБО, а также услугой SMS-информирования о проводимых операциях.

Рекомендации по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет.

Просим Вас отнестись с особым вниманием к расчетам в сети Интернет. Будьте внимательны: сайты мошенников могут быть почти точной копией тех, через которые Вы планировали осуществить платеж. Они созданы специально для получения Ваших персональных данных и реквизитов банковских карт.

Если Вы обнаружили в сети Интернет ложный web-сайт «Тимер Банка» (ПАО), отличный от **https://www.timerbank.ru**, или с Вами пытаются связаться по электронной почте или иным способом лица с требованиями о предоставлении персональных идентификаторов доступа к системе дистанционного банковского обслуживания, просьба немедленно сообщить об этом в Службу безопасности «Тимер Банка» (ПАО) по телефонам: **(843) 525-74-97, 525-74-96.**

В целом, разработка и реализация комплекса мер по обеспечению информационной безопасности - сложная задача, требующая непрерывной работы квалифицированных специалистов. Однако, соблюдение перечисленных простых «гигиенических» мер позволит существенно снизить риски, связанные с использованием системы дистанционного банковского обслуживания, осуществлением платежей в сети Интернет с использованием платежных карт и, в конечном итоге, предотвратить хищение Ваших денежных средств.

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 дистанционного банковского обслуживания файлов с секретными ключами электронной цифровой подписи (ЭЦП) и паролей. У держателей пластиковых карт 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 дистанционного банковского обслуживания рекомендуется воспользоваться дополнительными бесплатными услугами, предоставляемыми «Тимер Банком» (ПАО), по ограничению ip-адресов, mac адресов, с которых разрешён доступ в систему ДБО, а также услугой SMS-информирования о проводимых операциях.

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

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

Храните ПИН-код отдельно от банковской карты, не передавайте банковскую карту для использования третьим лицам.

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).

При совершении операций с банковской картой в банкомате не используйте устройства, которые требуют ввода ПИН-код для доступа в помещение, где расположен банкомат.

При использовании банковской карты для безналичной оплаты товаров и услуг требуйте проведения операций с банковской картой только в Вашем присутствии. Это необходимо в целях снижения риска неправомерного получения Ваших персональных данных, указанных на банковской карте.

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 люди, находящиеся в непосредственной близости, не смогут его увидеть. Перед тем как подписать чек, в обязательном порядке проверьте сумму, указанную на чеке.

При совершении операций с банковской картой через сеть Интернет не требуется введение 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 звоните и не отправляйте ответные SMS-сообщения по указанным во входящем сообщении номерам, а как можно скорее свяжитесь со службой клиентской поддержки по номерам телефонов, указанным на оборотной стороне Вашей пластиковой карты и на официальном интернет-сайте, а также проинформируйте оператора службы о случившемся.

Стоит помнить, что сотрудники «Тимер Банка» (ПАО) никогда не будут по телефону, по электронной почте или в SMS-сообщениях запрашивать реквизиты Вашей банковской карты (номер карты и срок ее действия, cvv-код, ПИН-код). Это противоречит соображениям безопасности.

Обращаем Ваше внимание, что своевременное обращение в Банк позволит принять оперативные меры по предотвращению мошеннических действий.