С банковских карт украдено 8 миллионов сомов. Как себя обезопасить?

- Александр Шабалин

Банковские платежные карты, безналичные платежи во всем мире активно используются уже очень давно. В Кыргызстане пока еще предпочитают работать с наличными, однако с каждым годом многие осознают удобство работы с банковскими картами.

Естественно, там, где концентрируется большое количество денег, традиционно появляются те, кто хочет ими завладеть. Не исключение в данном случае и Кыргызстан.

Электронное мошенничество

Как сообщили **Zanoza.kg** специалисты Нацбанка КР, оценочная сумма по спорным транзакциям на данный момент составляет около 8 млн сомов. Всего за минувший год главный финансовый регулятор страны получил информацию о 1 300 подозрительных операциях с использованием банковских платежных карт.

"В 2016 году наблюдалось учащение фактов установки скимминговых устройств на банкоматы, что является причиной резкого увеличения количества мошеннических операций и проведение несанкционированных транзакций через интернет. По случаям скимминговых операций банками проведены внутренние расследования с привлечением правоохранительных органов. К другим причинам мошеннических транзакций можно отнести несоблюдение держателями карт и торгово-сервисными предприятиями правил безопасности пользования картой и терминалом, а также нарушение условий договора с банками", - сообщил специалист управления платежных систем НБ КР Улан Кулманбетов.

Для защиты от несанкционированного использования платежных карт необходимо строго следовать правилам пользования и условиям соглашения с финансово-кредитным учреждением, выдавшим карту.

Мошеннические операции в платежных системах Кыргызстана

8 000 000

сомов

Оценочная сумма по спорным транзакциям

1300

подозрительных операций с банковскими платежными картами зафиксировано за 2016 год

600

банковских платежных карт заблокировано

Держатель платежной карты сам несет ответственность за сохранность данных о реквизитах платежной карты, ПИН-кода и самой карты

Если потеря произошла не по вине держателя карты, банки обычно восполняют ущерб своим клиентам

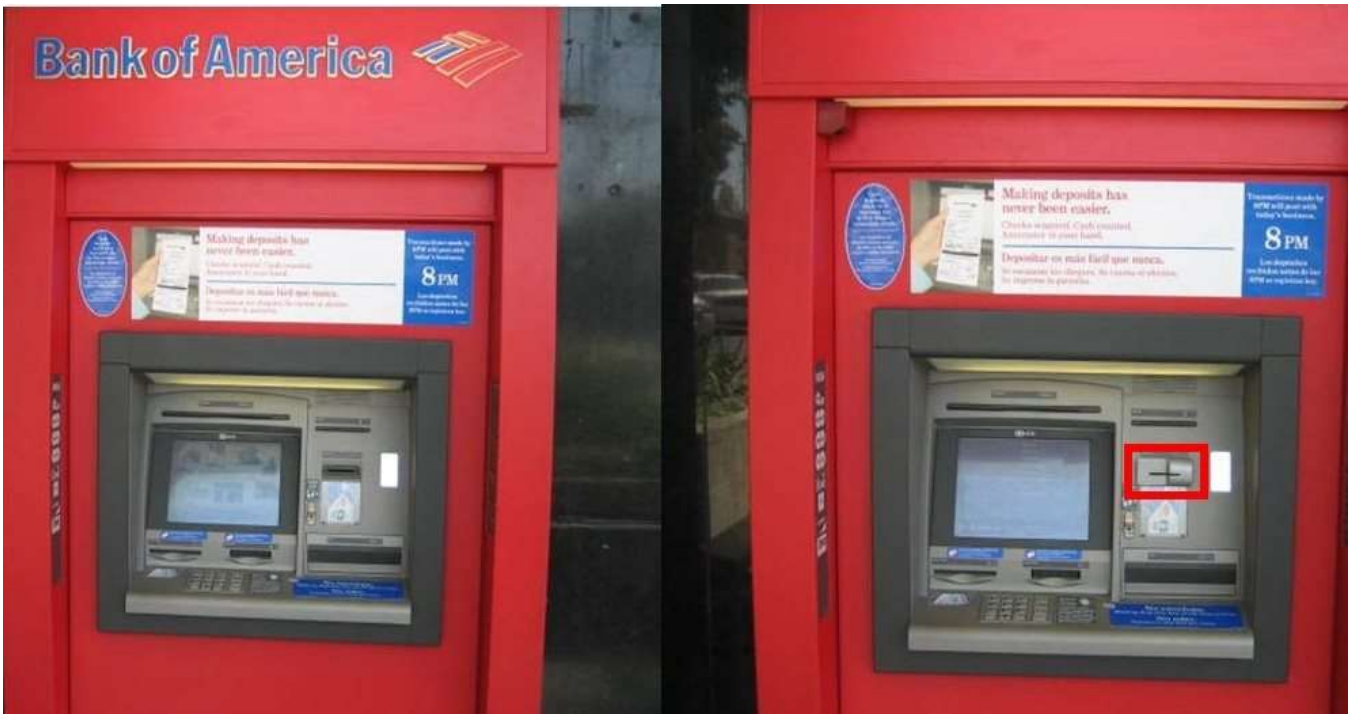
Хитроумные уловки

Как сообщают специалисты, в Кыргызстане мошенники используют различные уловки для кражи денежных средств с банковских карт. **Zanoza.kg** собрала самые распространенные способы мошенничества с пластиковыми картами.

Схема 1. Самый элементарный способ. Человек, стоящий в очереди, просто подсмотрит ПИН-код из-за спины, а затем он или его сообщник крадет вашу банковскую карту. Также мошенники могут распылить на клавиатуру специальный спрей, на котором будут четко видны нажатые клавиши, установить накладную клавиатуру. Еще один вариант – установка на банкомат микрокамеры.

Накладная клавиатура

Схема 2. Держатель карты совершает любую операцию с помощью банкомата и, ничего не подозревая, уходит по своим делам. В это время мошенники с помощью скиммера считывает информацию о карте и получают возможность изготовить ее дубликат для доступа к банковскому счету.



Слева банкомат без скиммера. Справа - со скиммером.

Чтобы не стать жертвой мошенников, прежде чем воспользоваться банкоматом, необходимо внимательно осмотреть его: на банкомате не должно быть выступающих частей, тем более отличающихся по цвету; возле экрана банкомата не должно быть подставок с буклетами. При обнаружении скимминговое оборудования или подозрении на него рекомендуется звонить по номеру телефона, указанному на карте, и сообщать об этом.

Мошенничество онлайн

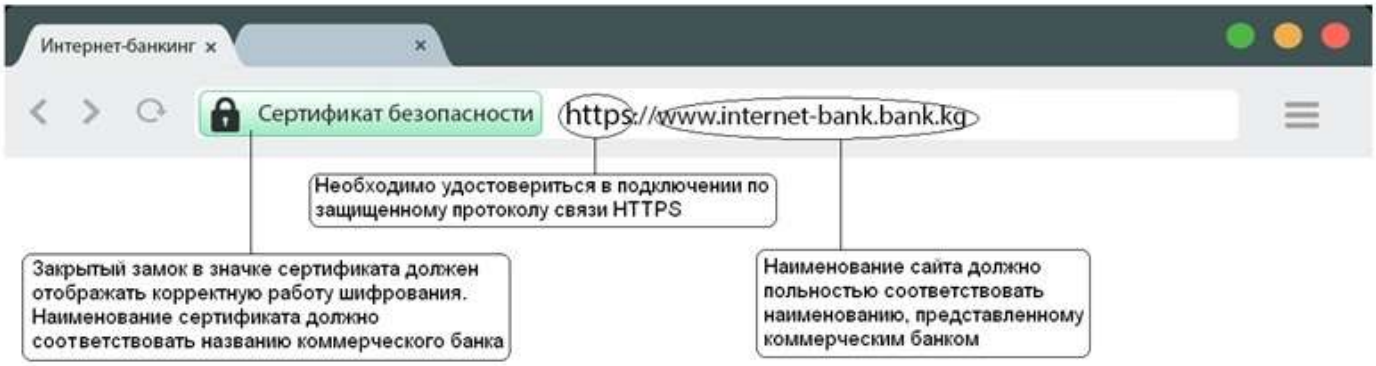
Мошенники под видом финансового института, кредитной организации рассылают "официальные" сообщения с запросом подтвердить личные данные реквизиты счета, ПИНы, пароли и другие данные. В большинстве случаев такие письма содержат информацию о проблеме со счетом или угрозе мошенничества. Данный вид мошенничества носит название "фишинг".

От: BankN[mailto: Service@BankN.com]
Отправлено: Пятница, Февраль, 24, 2016 8:37 AM
To: держатель карты
Тема: Внимание! Потеряна база данных кредитных карт BankN!

Здравствуйте, к сожалению, в виду того, что некоторые базы данных были взломаны хакерами, Банк установил новую систему безопасности. Вам следует проверить Ваш остаток, и в случае обнаружения подозрительных трансакций обратиться банк. Если Вы не обнаружите подозрительных трансакций, это не означает, что данные карты не потеряны и не могут быть использованы. Возможно, Ваш банк-эмитент еще не обновил информацию. Поэтому мы настоятельно рекомендуем Вам посетить наш Интернет-сайт и обновить Ваши данные, иначе мы не сможем гарантировать Вам возврат украденных денежных средств. Спасибо за внимание. Нажмите сюда для обновления Ваших данных.

Хрестоматийный пример фишинга.

Чтобы не попасться на удочку мошенникам, до проведения каких-либо операций с безналичными платежами в интернете, необходимо удостовериться в безопасности интернет-странички.



За глупость деньги не возвращают

Важно знать, что держатель платежной карты сам несет ответственность за сохранность данных о реквизитах платежной карты, ПИН-кода и, собственно, самой карты. Банки в каждом случае отдельно рассматривают мошенническую транзакцию. Если можно точно установить, что потеря произошла не по вине держателя карты, идут навстречу своим клиентам и могут восполнить ущерб.

Специалисты Нацбанка КР подготовили рекомендации, которые позволят минимизировать риск стать жертвами мошенников и сохранить свои деньги в безопасности.

Меры безопасности, которые должны знать пользователи платежных карт

1. Быть внимательными к условиям хранения и использования платежных карт.
2. Телефон банка - эмитента платежной карты (кредитной организации, выдавшей карту) указан на оборотной стороне банковской карты. Также необходимо всегда иметь при себе контактные телефоны эмитента карты и номер карты на других носителях информации: в записной книжке, мобильном телефоне и/или других носителях информации, но не рядом с записью о ПИН.
3. С целью предотвращения неправомерных действий по снятию всей суммы денежных средств с банковского счета целесообразно установить суточный лимит на сумму операций по платежной карте и одновременно подключить электронную услугу оповещения о проведенных операциях (например, оповещение посредством SMS-сообщений или иным способом).

Меры безопасности, которые должны знать пользователи дистанционных платежных услуг

1. Обязательно проверять правильность адресов интернет-сайтов, с которых требуется совершать покупки, т. к. похожие адреса могут использоваться для осуществления неправомерных действий.
2. Рекомендуется совершать покупки только со своего компьютера в целях сохранения конфиденциальности персональных данных и (или) информации о банковской(ом) карте (счете).
3. 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).

4. Установить на свой компьютер антивирусное программное обеспечение и регулярно производить его обновление и обновление других используемых программных продуктов (операционной системы и прикладных программ). Это может защитить от проникновения вредоносного программного обеспечения.