В начале июля транспортная полиция обнаружила в столичных аэропортах Внуково и Шереметьево фальшивые банкоматы. Еще один «чужак» был найден в торговом центре «Охотный ряд». Известно, что банкоматы когда-то принадлежали «Внешинвестбанку» и были ликвидированы в далеком 1999-ом. Но злоумышленники переделали аппараты под свою нужду.

Создание фальшивых машин

Постоянный рост количества обычных банкоматов провоцирует преступников на создание фальшивых машин. Псевдобанкоматы могут быть сделаны по «спецзаказу», а также переделаны из старых. В любом случае их очень трудно отличить от настоящих, потому что основное отличие внутри. Пользователь банковской карты находит нужный ему банкомат, вставляет в него карту. Далее идет типичная операция: ввод пин-кода. Только фальшивые машины используют их не для идентификации владельца, а для передачи данных злоумышленникам. После того, как вы ввели данные, машина их сканирует и запоминает. А владельцу карты выдается информация, что «нет связи с банком, попробуйте позже». Или невозможно выдать деньги из-за якобы только что возникшей неисправности. Но чаще всего отказ наступает из-за «отсутствия» нужной суммы. После неудачно проведенной операции, он возвращает вашу карту и извиняется за причинённые неудобства.

Размещаются такие банкоматы, как правило, в наиболее оживленных местах на несколько дней, после чего демонтируются и переносятся в новое место, чтобы избежать излишнего внимания со стороны правоохранительных органов.

Не суй куда попало!

В полиции рекомендуют использовать для снятия наличных денег проверенные банкоматы, расположенные в отделениях банка или крупных торговых цент-рах. При внимательном осмотре часто можно заметить, что банкомат «какой-то не такой». У него может быть несколько искажены или вообще отсутствовать логотипы банка, отсутствовать обычная в данном случае информация о банке, контактные телефоны банка и экстренных служб, информация о ближайших банкоматах, набор функций в меню может быть сокращённый по сравнению с обычным.

Если же вы наткнулись на подозрительный аппарат или же провели эту самую «неудачную» операцию, лучше позвоните в круглосуточную службу помощи банка (телефон указан на обороте карты) и уточните, зарегистрирован ли банкомат, которым вы только что пытались воспользоваться, сообщите о своих подозрениях. Если такого банкомата в банке не значится, попросите оператора немедленно заблокировать карту. Сотрудник банка при этом даст Вам инструкции по дальнейшим действиям. Скорее всего экстренная блокировка будет временной, и в ближайшие 3-5 дней вам предложат посетить с паспортом отделение банка, выдавшего карту, и написать заявление на её перевыпуск. При этом деньги со счёта будут доступны для вас в отделении банка при предъявлении паспорта.

Но если же вы все-таки стали жертвой фальшивого банкомата и его хозяев, то в этом случае возврат денег практически невозможен. Потому что очень сложно будет доказать, что счет опустел в результате действий мошенников, а не самого клиента. Поэтому жертвы мошенников могут рассчитывать только на добрую волю банка, в котором обслуживаются.

Украинская «мода»
Впервые подобное «чудо-техники» было найдено милицией на Украине еще в 2011 году. Мошенники разместили на фальшивом банкомате в одном из киевских торговых центров объявление о беспроцентной выдаче денег по картам ряда банков. Заставка с «выгодным предложением» то и дело манила к себе покупателей.
И понеслась…
Предложение было ну очень привлекательным, да и само место, где располагался фальшивый банкомат (дело было в ТЦ «Караван») располагало к данной операции. Несмотря на то, что на самом банкомате отсутствуют как идентификатор аппарата, так и выходные данные банка, сотни людей купились на эту удочку.

Наш полуостров
Журналисты «Вестей» направили в пресс-службу камчатской полиции запрос о количестве мошенничеств, связанных с банкоматами. Мы выяснили, что на Камчатке не было зафиксировано ни одного случая скиммирования (сканирование информации с пластиковой карты в преступных целях). А уж что там говорить про целый фальшивый банкомат! Может в нашем сравнительно небольшом городе мошенникам просто не выгодно ставить псевдобанкоматы (так как их быстро вычислят). Местные преступники работают «по-старинке» и продолжают «разводить» камчадалов с помощью телефонных звонков и смс.

На заметку
Кстати, есть такое полезное наблюдение: стандартные щели для карточек банкоматов светятся, скиммеры - нет.
Прежде всего вас должны насторожить утолщение на отверстии для ввода карты, наличие клея на клавиатуре либо торчащие провода.
На клавиатуре не должно быть никаких наклеек, прозрачных накладок, она не должна быть сильно выпуклой.
Старайтесь пользоваться одним и тем же банкоматом, и тогда его внешние изменения не останутся для вас незамеченными.
Также неплохо было бы подключить услугу смс-информирования обо всех операциях с вашей картой, можно еще установить дневной лимит снятия налички с карты. В этом случае вам будет проще отслеживать куда уходят деньги.
Как говорится, пока есть спрос, будут и предложения. Не забывайте, что мошенники оперативные, алчные хитрецы (чаще даже хитрее сотрудников банка, охранников, следователей и даже установленных видеокамер). Они не упустят ни одной возможности нажиться. Так что будьте бдительны!

Катерина АРТЕМЬЕВА.

Справка «В»:
Кардинг (от англ. carding) - вид мошенничества, при котором производится операция с использованием платежной карты или её реквизитов, не инициированная или не подтвержденная её держателем. Реквизиты платежных карт, как правило, берут со взломанных серверов интернет-магазинов, платежных и расчётных систем, а также с персональных компьютеров (либо непосредственно, либо через программы удаленного

доступа, «трояны», «боты» с функцией формграббера). Кроме того, наиболее распространённым методом похищения номеров платежных карт на сегодня является фишинг (англ. phishing, искаженное «fishing» - «рыбалка») - создание мошенниками сайта, который будет пользоваться доверием у пользователя, например - сайт, похожий на сайт банка пользователя, через который и происходит похищение реквизитов платежных карт.
Частным случаем кардинга является скимминг (от англ. skim - снимать сливки), при котором используется скиммер - инструмент злоумышленника для считывания, например, магнитной дорожки платёжной карты. При осуществлении данной мошеннической операции используется комплекс скимминговых устройств: инструмент для считывания магнитной дорожки платёжной карты - устройство, устанавливаемое в картоприёмник, и картридер на входной двери в зону обслуживания клиентов в помещении банка. Представляет собой устройство со считывающей магнитной головкой, усилителем - преобразователем, памятью и переходником для подключения к компьютеру. Скиммеры могут быть портативными, миниатюрными. Основная идея и задача скимминга - считать необходимые данные магнитной полосы карты для последующего воспроизведения её на поддельной. Таким образом, при оформлении операции по поддельной карте авторизационный запрос и списание денежных средств по мошеннической транзакции будут осуществлены со счета оригинальной, «скиммированной» карты.
Миниатюрная видеокамера, устанавливаемая на банкомат и направляемая на клавиатуру ввода в виде козырька банкомата либо посторонних накладок, например, рекламных материалов - используется вкупе со скиммером для получения ПИН - держателя, что позволяет получать наличные в банкоматах по поддельной карте (имея данные дорожки и ПИН оригинальной).
Данные устройства питаются от автономных источников энергии - миниатюрных батарей электропитания, и для затруднения обнаружения, как правило, изготавливаются и маскируются под цвет и форму банкомата.
Скиммеры могут накапливать украденную информацию о пластиковых картах, либо дистанционно передавать её по радиоканалу злоумышленникам, находящимся поблизости. После копирования информации с карты мошенники изготавливают дубликат карты и, зная ПИН, снимают все деньги в пределах лимита выдачи, как в России, так и за рубежом. Также мошенники могут использовать полученную информацию о банковской карте для совершения покупок в торговых точках.
Шимминг представляет собой разновидность скимминга. В этом случае в картридер банкомата помещается электронное устройство (шиммер), позволяющее получить информацию о банковской карте. Толщина шиммера - порядка 0,2 мм. Внешнее определение использования шиммера крайне затруднено. Защитой от шиммера является только то, что шиммер не перехватывает PIN-код.