Как опознать опасный банкомат

На днях один из клиентов Сбербанка обнаружил скимминговое оборудование (картоприемное устройство) на банкомате Приволжского отделения банка на ул. Сибирский тракт, 25 и сообщил об этом сотрудникам. Установив приметы подозреваемых, сотрудники полиции совместно с сотрудниками Сбера устроили у банкомата засаду – и в тот же вечер двое подозреваемых были задержаны. Ими оказались 17-летние студенты одного из казанских вузов, сообщает электронная газета «Бизнес-Online».

Они не впервые занимались этим видом мошенничества. В полиции подозреваемые признались, что устанавливали скимминговое оборудование на этот же банкомат 26 - 27 мая вечером и ночью. Таким образом, было скомпрометировано несколько пластиковых карт клиентов банка.

Уголовное дело полицейские возбуждать не стали – студенты, дав признательные показания, раскаялись в содеянном. Ущерб банку причинен не был. Скимминг вообще – деяние труднодоказуемое. В Уголовном кодексе такой статьи просто нет – и наказать мошенников можно, только если доказать всю цепочку: скимминг – изготовление поддельной карты – обналичивание.

Стоит отметить, что в прошлом году в Казани было зарегистрировано два таких случая, когда злоумышленники установили свое оборудование на банкоматы Сбербанка. Жертв мошенники так и не дождались – все устройства оперативно были сняты.

У злоумышленников есть несколько способов установки шпионского оборудования на банкомат. Это может быть пластиковая накладка, прикрепляемая к картридеру, либо миниатюрная видеокамера в держателе для брошюр рядом с банкоматом. В данном случае на картридер банкомата была установлена пластиковая накладка серого цвета, содержащая с внутренней стороны вмонтированную электронную плату и флеш-карту. А также плоская пластиковая штанга толщиной около 3 см и длиной 50 см, внутри которой были вмонтированы видеокамера и две аккумуляторные батарейки от сотовых телефонов, скрепленные изолентой.

Картридер считывает данные карты, а камера записывает, какие кнопки вы нажимаете, когда набираете PIN-код, именно поэтому «безопасники» советуют закрывать клавиатуру рукой. Но бывают и специальные накладки на клавиатуру, считывающие порядок набора цифр...

Многие скимминговые приспособления прикрепляются к банкоматам с помощью обычного двустороннего скотча или застежки-«липучки». Что касается клавиатуры, то если она была, скажем, вогнутой, специальная накладка сделает панель более плоской. Также скимминговое устройство может изменить сами клавиши: они будут либо утоплены в панель клавиатуры, либо, наоборот, слишком сильно выпирать. Скиммеры, установленные на кардридер, могут в точности

повторять цвет и дизайн банкомата. Единственный их отличительный признак — они слегка выдаются над основной поверхностью корпуса.

Чтобы не стать жертвой скиммеров, банкиры советуют по возможности пользоваться одним и тем же банкоматом, так проще запомнить его внешний вид. И обязательно прикрывать рукой клавиатуру во время набора PIN-кода к карте.

Определить скиммеры неопытному человеку достаточно сложно, но можно. Перед тем как воспользоваться банкоматом, следует присмотреться. Нет ли на панели с клавиатурой или рядом с экраном дополнительных устройств, допустим, лишних осветительных приборов? Нет ли поблизости зеркал или держателя для рекламных брошюр? Все эти мелочи могут свидетельствовать о наличии скиммера… Если что-либо во внешнем виде банкомата показалось подозрительным, лучше им не пользоваться.

Лучше всего использовать уже знакомый банкомат, причем в хорошо освещенном месте, желательно многолюдном. Не стоит доверять устройствам, имеющим непривычные опознавательные знаки или необычные требования инструкции – к примеру, двойное введение PIN при подтверждении операции. И доверяйте своей интуиции, советуют банкиры.