Осторожно, мошенники!

(некоторые способы, используемые мошенниками с банковскими картами)

**Банкомат**

Для того, чтобы узнать ПИН-код, мошенники могут наклеивать на клавиатуру банкомата специальную прозрачную пленку с микросхемой, которая фиксирует вводимый ПИН-код или устанавливать жесткую накладку, полностью имитирующую клавиатуру банкомата. Специальное приспособление крепится также и на приемное устройство для карты для считывания информации с магнитной полосы. Затем, сняв «жучки», мошенники получают всю необходимую информацию о карте. Поэтому, при пользовании банкоматом не ленитесь внимательно осмотреть его и убедиться в отсутствии каких-либо «накладок». Если вы заметили что-либо подозрительное, откажитесь от использования данного банкомата.

Часто мошенники подсматривают ПИН-код в момент снятия денежных средств в банкомате держателем карты. Затем, карта похищается у держателя и с нее, в течение 10-15 минут, снимается вся оставшаяся на карте сумма. Пожалуйста, примите все меры, чтобы вводимый Вами ПИН-код был не заметен для окружающих.

Известны случаи, когда мошенники в момент выдачи денежных средств отвлекают держателя карты, тем самым давая возможность другому мошеннику, стоящему рядом забрать денежные средства, выданные банкоматом. Не отвлекайтесь, пока не получите деньги и карту из банкомата.

**Интернет**

Один из способов получения реквизитов карт, используемых мошенниками, заключается в создании «поддельного» интернет-магазина. Небольшой, недавно открытый магазин предлагает приобрести по картам товары и услуги. При этом, как в настоящем магазине, требуется ввести сведения о карте, только сведения эти передаются не в информационный центр платежной системы, а прямиком в базу данных мошенников. Чтобы избежать подобного обмана старайтесь пользоваться проверенными интернет-магазинами, в надежности которых Вы уверены.

Как правило, надежный интернет-магазин предлагает проведение платежа с использованием сертифицированных средств защиты информации: протокола SSL (Secure Socket Layer) или стандарта SET (Secure Electronic Transaction). Эта информация отражается в правом нижнем углу экрана.

В российском сегменте сети Интернет зафиксированы случаи появления Web-сайтов, на которых предлагаются различные финансовые услуги с использованием банковских карт международных платежных систем. Пользователям предлагается заполнить электронные формы и указать реквизиты банковских карт, включая ПИН-код. При этом передача конфиденциальной информации ведется без использования защищенных протоколов информационного обмена.

Этот и ряд других признаков, характеризующих работу подобных Web-сайтов, дает основания полагать, что такими предложениями могут маскироваться мошеннические действия, известные как «фишинг», т.е. заманивание пользователей с целью раскрытия конфиденциальной информации посредством использования поддельных Web-сайтов.

**Обращения к держателям карт от имени Банка (фишинг)**

Один из способов получения данных о карте и ее держателе состоит в том, что мошенники обращаются к держателю по телефону с сообщением от имени Банка или платежной системы, касающимся безопасности его карточного счета или проверки правильности данных.

Например, что с картой производятся мошеннические действия и для их предотвращения держателю необходимо как можно быстрее перезвонить по определенному номеру телефона. При звонке по этому номеру держателя просят сообщить или ввести с клавиатуры телефона данные карты и свои персональные данные.

В таких мошеннических обращениях, которые часто производятся с помощью автоответчика, отсутствует упоминание имени и фамилии держателя. Поэтому, пожалуйста, обращайте внимание на то, чтобы обращение к Вам было по фамилии, имени, отчеству. Если этого не происходит - налицо признаки мошенничества. Важно не перезванивать по номерам телефонов, указанных в подобных сообщениях. Звонить можно только по номеру, указанному на оборотной стороне карты. О подозрительных обращениях к Вам от имени Банка или платежной системы немедленно сообщайте в Банк.

Другой способ, который используют мошенники для получения конфиденциальной информации от держателя карты, заключается в направлении держателю сообщения по электронной почте от имени Банка или платежной системы, с уведомлением о подозрениях на компрометацию данных его карты, и просят подтвердить эти данные, зайдя по определенной ссылке на сайт платежной системы (на самом деле, ссылка переадресует на сайт, созданный мошенниками). Если к Вам поступило подобное сообщение, ни в коем случае не сообщайте данных своей карты и немедленно позвоните в Банк.

Для незаконной активации карт мошенники звонят клиенту от имени Банка и под предлогом уточнения персональных данных получают у клиента всю информацию, указанную в заявлении-анкете. При получении sms-сообщений о действиях, которых Вы не совершали, немедленно обратитесь в Банк по телефонам, указанным на оборотной стороне Вашей карты.

Звонки из Банка Вам могут поступать со следующих номеров:

(3466) 41-26-09

(3466) 41-26-55

(3466) 62-01-35

8-800-200-4575

При любых подозрительных обращениях к Вам от имени АО КБ «Приобье» немедленно проинформируйте об этом Банк.