Мошенничество с банковскими картами и счетами

Платежная карточка, безусловно, удобная и полезная вещь. Но крайне соблазнительная для криминальных воздействий. Весьма распространена схема воровства «на доверии». Так, телефон из объявления в интернете или СМИ о продаже любого имущества немедленно попадает в поле зрения мошенников. И владельцу звонит некий «потенциальный покупатель», готовый платить, не торгуясь, но только на карту. Для этого он просит сообщить её номер, срок действия, CVV-код с обратной стороны карты. И SMS-код из сообщения банка о проведённой операции. Даже если не удаётся получить весь набор информации, недостающие данные восполняются квалифицированными хакерами. И карточный счёт не пополняется, а опустошается путём перевода наличности на некий электронный кошелек, который немедленно исчезает из сети после вывода средств с него.

Звонки от «служб безопасности» банков

Не менее распространены звонки из «службы безопасности банка-эмитента платежной карты» о совершённой подозрительной операции или сбое в программном обеспечении, который привел к потере средств. Для восстановления счёта и возврата денег якобы необходимы вышеперечисленные данные. Для защиты от подобных инцидентов рекомендуют установить определенные программы, замаскированные под известные сервисы. Но на самом деле эти утилиты отправляют мошенникам коды доступа к счетам, полностью развязывая преступникам руки.

Самый распространённый вариант такого мошенничества — сообщение или звонок об ошибочном переводе денег на счёт мобильного телефона и просьба вернуть их владельцу. Могут быть даже угрозы обращения в полицию или оператору с требованием блокировки телефона.

Сообщения о попавшем в беду родственнике и просьбы о помощи

Панический звонок о попавшем в беду родственнике обычно случается среди ночи, полусонной жертве сообщают об автомобильной аварии, наезде на пешехода, крушении поезда или любых других происшествиях, случившихся с детьми, внуками или просто друзьями. Далее следует просьба о срочной помощи в виде перевода немалой суммы на электронный кошелек или счёт мобильника. Метод крайне жестокий, известны случаи инфарктов от подобных новостей.

Махинации с короткими номерами

В этом случае мошенники тоже используют мобильный сервис. При заказе некой услуги абонент получает сообщение, что для её подключения нужно отправить сообщение на короткий номер такой-то. После отправки со счёта списываются деньги. Механизм тот же, короткий номер тоже можно зарегистрировать как платный и не сообщать об этом абоненту.

Какую информацию нельзя сообщать собеседнику по телефону?

Мошенники стремятся получить секретные данные карты — трёхзначный код CVC/CVV с обратной стороны, коды подтверждения из SMS, логины и пароли от интернет-банков. Настоящие сотрудники банка никогда не запрашивают эту информацию — для обеспечения безопасности они используют отдельные технические средства. Для отправки платежа нужен только номер карты — другие данные для этого не нужны.

Соблюдайте осторожность!