**Десять способов мошенничества с банковской картой**

Пользоваться пластиковыми картами, как кредитными, так и дебетовыми, удобно. Вам не приходится носить с собой большое количество наличных денег, при этом средствами можно распоряжаться по своему усмотрению в любой момент, как для совершения покупок и оплаты услуг, так и для переводов родственникам и друзьям. Однако пластиковые карты, являясь удобным способом доступа к деньгам на карточном счете, неизбежно становятся и объектом внимания злоумышленников, выдумывающих все новые и новые способы эти деньги похитить. Для того чтобы не лишиться своих средств, необходимо знать, какими приемами пользуются преступники. Мы подготовили небольшой обзор, десятку самых популярных способов мошенничества с кредитными картами. Надеемся, знание этих приемов позволит и клиентам, и сотрудникам банков избежать неприятностей и проблем при пользовании кредитками.

**1. Скримминг**

Этот способ доступа к чужому банковскому счету был настоящим бичом всей системы карточных платежей еще несколько лет назад, и до сих пор попытки его использования остаются популярными. Преступники, выбравшие этот способ, вооружаются достаточно продвинутыми техническими приспособлениями. Первое из них – это скриммер, портативный сканер, считывающий данные с карты жертвы. Выглядит это устройство как накладка, устанавливаемая на щель приема карты банкомата. Скриммер пропускает через себя карту и проталкивает ее дальше, в банкомат, считывая при этом данные с магнитной ленты.

После чего мошенники легко изготавливают копию карты, так скопировать информацию с магнитной полосы не труднее, чем сделать копию с магнитофонной кассеты, такие были популярны не так давно (принцип хранения информации на магнитной ленте тот же). Но для того, чтобы воспользоваться такой картой-копией («белым пластиком», как говорят специалисты по информационной безопасности), преступники должны знать пин-код, который вводится на клавиатуре банкомата. Считывают этот код при помощи видеокамеры, установленной неподалеку, или при помощи тонкой накладной клавиатуры, устанавливаемой на клавиатуру банкомата.

Чтобы не стать жертвой этого вида мошенничества, достаточно внимательно осмотреть банкомат перед тем, как доверить ему свою карту: накладные устройства нетрудно заметить, так как они меняют стандартный вид аппарата. Вводя пин-код, стоит также прикрывать его от возможного подглядывания – учтите, что камера с мощным объективом может быть установлена на большом расстоянии, в том числе и на верхних этажах зданий. Но лучше всего защищает от скримминга использование карты с чипом, поддерживающим аппаратное шифрование информации. Сделать копию такой карты в «полевых» условиях практически невозможно.

**2. Фишинг**

Слово фишинг переводится с английского как рыбная ловля, и одноименный метод мошенничества действительно имеет много общего с древним искусством добычи пропитания. Так же, как и на рыбалке, используется наживка, и жертва так же должна самостоятельно заглотить ее, попавшись на крючок. Только вместо червячка используется сайт-ловушка, а вместо крючка – данные о карте, которые жертва сама вводит на странице такого сайта.

Злоумышленники-фишеры создают сайт, имитирующий официальный сайт банка. Для этих целей используется доменное имя, похожее на имя банка, но зарегистрированное в одной из доменных зон Южной Америки, Африки или другого удаленного региона. Расчет прост: Не все люди внимательно смотрят на адресную строку браузера и не все понимают, что сайт только похож на привычный сайт, на самом деле являясь совершенно другой страницей. Заманивают жертву на такую подставную страницу, как правило, письмом, также имитирующим официальное письмо от техподдержки банка. Только ссылка, которая содержится в таком письме, ведет на сайт-ловушку. Под предлогом проверки информации жертве предлагают ввести все данные о карте на подставной странице, в том числе CCV и пин-код. Некоторые подставные страницы даже перенаправляют жертву после получения нужных сведений на настоящую страницу банка, и даже заподозривший неладное человек видит уже реальный сайт финансовой организации.

Рецепт борьбы с фишинг-атакой прост: внимательно смотрите, что за сайт открыт в вашем браузере, и ни в коем случае не отправляйте в Сеть информацию, которая у настоящего банка и так есть. Лучше всего, если происходит что-то странное, позвонить в свой банк и уточнить, что случилось. Только, ради Бога, не набирайте номер, который опубликован на подставной интернет-странице, будьте внимательны!

**3. Пoдставной магазин**

Одна из разновидностей фишинга – использование интернет-магазина, специально созданного для сбора сведений о картах жертв. Помните, что чудес не бывает, и если товар предлагается по цене, в несколько раз ниже рыночной, то что-то здесь не так. Часто сайт с «привлекательными» предложениями, будь то реальные или виртуальные товары, является просто «прокладкой» между вами и вашим банком, отфильтровывая информацию о платеже и перенаправляя его на другой счет. При этом даже код подтверждения платежа, направленный банком на ваш мобильник, не спасет – вы сами введете его в специальное окошко на сайте мошенников.

Бороться с подобной атакой непросто – нужно уметь отличить настоящий интернет-магазин от фишинговой ловушки. Чтобы обезопасить себя, достаточно просто поискать информацию о магазине в Сети, почитать отзывы о нем. Помните, что все нормальные магазины дают возможность выбрать вариант оплаты, среди которых есть и оплата курьеру при доставке товара. И внимательно читайте, что написано в СМС с кодом подтверждения платежа – банк четко приводит сумму покупки и  название организации, выставившей счет.

**4. «Проверка безопасности»**

Самый простой способ завладеть данными о карте пользователя – это просто попросить жертву поделиться этими сведениями. Звучит это фантастически, но это работает: из сотни клиентов банков найдутся несколько, которые все расскажут незнакомцу по телефону. Обычно мошенник представляется сотрудником банка, который проводит проверку безопасности, или просто уточняет необходимые сведения.

В повседневной жизни люди, как правило, не бдительны, они не ждут нападения в любой момент. А такой звонок – это и есть внезапная атака на ваш банковский счет. Некоторые преступники действуют настолько нагло, что даже просят прочесть код подтверждения, который вы сейчас получите в смс. Не сомневайтесь: в этот момент мошенник производит оплату, используя полученные от вас сведения, и до расставания с деньгами остаются считанные секунды.

**5. «Спасение» денег**

Более совершенная разновидность предыдущего способа – перевести жертву  стрессовое состояние. «С вашей карты сейчас происходит списание денег, нам нужно срочно проверить информацию. Назовите номер, срок действия и последние три цифры, напечатанные на обороте карты». Варианты могут быть разными, но смысл один: решать нужно быстро, вашим деньгам грозит опасность, срочно продиктуйте всю информацию. Доказано, что в состоянии стресса и тревожности человек склонен к необдуманным поступкам и не пытается анализировать ситуацию.

**6. «Мама, у меня проблемы, не звони, переведи деньги на этот счет»**

Даже если ваш ребенок сидит на диване рядом с вами, вы испугаетесь, получив такое сообщение. Так уж устроены родители: они беспокоятся о своих детях, и реакция на возможную угрозу им очень сильна. А если ваш ребенок где-то в городе? Простая, эффективная и наглая схема, использующая сильные чувства и базовые, фундаментальные инстинкты.

**7. Пoдставной покупатель**

Многие из нас продают ненужные вещи, разместив объявление на страницах газет или в интернете. Мошенник, представившись покупателем, просит продиктовать номер карты, чтобы якобы перевести на нее деньги. При этом просит продиктовать и срок ее действия, и назвать платежную систему, и прочесть три цифры на обороте карты. Не каждый человек, обрадовавшись удачной сделке, сразу догадывается, что его просят поделиться сведениями в несколько большем объеме, чем этого требуется для совершения перевода.

**8. Продажа карты с нулевым балансом**

Нередко мошенники предлагают купить банковские карты с нулевым балансом. Вместе с картой покупают и персональные некоторые персональные данные. Казалось бы, что может плохого случиться, если на карте все равно нет денег? Но неприятности могут быть достаточно серьезными, если карту будут использовать для преступной деятельности. Например, на нее могут принимать платежи от жертв мошеннических схем, ее могут использовать для обналичивания краденых денег. В любом случае полиция и налоговые органы, расследующие мошеннические схемы, выйдут на владельца этой карты.

**9. Грабеж у банкомата**

Старый, как мир, способ «кошелек или жизнь» трансформировался в способ «карта и пин-код или жизнь». Будьте внимательны, подходя к банкомату в неблагополучном районе и в темное время суток.

**10. Нигерийский принц**

Схема, ставшая настоящей классикой мошенничества благодаря толковым парням из Нигерии, в свое время организовавших масштабный международный «бизнес» по отъему денег у доверчивых белых. Впрочем, нигерийские завсегдатаи местных интернет-клубов просто были первыми, сейчас такие «принцы» могут быть из любой страны и с любым цветом кожи. Схема работает благодаря вере людей в чудо и желанию быстро разбогатеть, используя подвернувшийся случай. Жертва получает письмо от незнакомца, который рассказывает о том, что он является представителем богатой семьи из далекой страны (в классическом варианте – нигерийский принц).

Этой семье грозит опасность, «принца» преследуют по политическим или иным причинам. Нужно срочно бежать, но есть проблема – накопленные миллионы необходимо вывести из страны. Вам нужно лишь открыть счет, и миллионы скоро окажутся на нем, с жертвой обещают щедро поделиться за помощь.

Ослепленные возможностью фантастической скорой наживы, люди открывают счета, и поддерживают переписку с «принцем», следя за его драматическими приключениями в далекой стране. В результате все сводится к одному: для какой-либо цели (залог за авиабилет, почтовый сбор – что угодно) с вашей кредитки необходимо перевести небольшую сумму, никак ни сравнимую с миллионами, которые сулит все предприятие. В результате некоторые жертвы умудряются переводить тысячи долларов, помогая своему новому другу и ожидая миллионов.

**Ценнoсть информации**

Схем мошенничества с кредитками много, многие из них уже не актуальны, но преступники постоянно придумывают новые. Чтобы использование банковских карт было не только удобным, но и безопасным, помните: самое дорогое в современном мире – это информация. Отдать персональные сведения, сведения о кредитке посторонним – это все равно, что отдать свой кошелек.

Пользуйтесь современными пластиковыми картами с чипом, поддерживающим аппаратное шифрование. Если вы часто оплачиваете в интернете товары и услуги, заведите для этого отдельную карту, переводя на нее лишь средства для следующего платежа.

И будьте внимательны, доверяя информацию о вашей карте людям, которых вы не знаете.