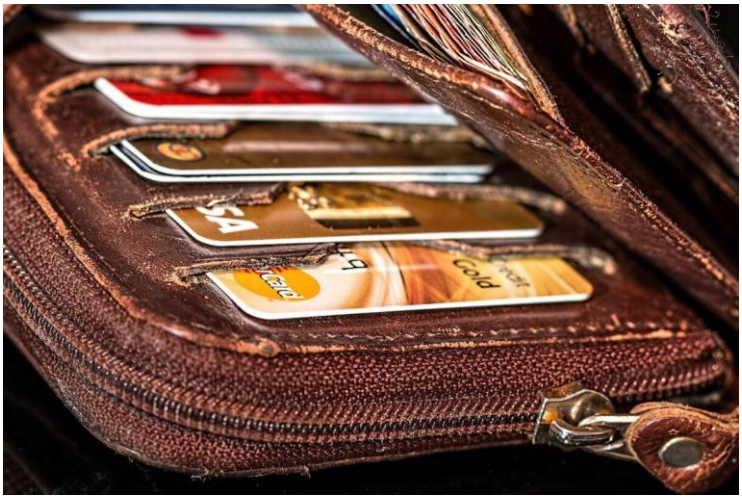
Знай правила безопасного использования банковских карт

Использованием дебетовых или кредитных карт давно уже никого не удивишь. Развитие технологий мобильного банкинга, безналичных расчетов и бесконтактных способов оплаты привело к тому, что все больше людей отдают предпочтение пластику, а не наличным в кошельке. На карту перечисляются зарплаты и пенсии, переводы с карту на карту происходят практически мгновенно, с помощью карт оплачиваются товары в интернет-магазинах, сеть банкоматов развилась до шаговой доступности и теперь чтобы снять наличные не надо ехать на другой конец города.



Картами в кошельке сейчас никого не удивишь.

Мы пользуемся картами каждый день, она стала незаменимым инструментом, всегда лежащим в кошельке. Несмотря на то, что надежность и безопасность пластиковых карт находятся на высоком уровне и сама технология постоянно совершенствуется, ежегодно мошенниками, взявшими на вооружение современные технологии и методы социальной инженерии, похищаются с карточных счетов миллиарды. Так какие опасности могут подстерегать рядового обладателя банковской карточки?

Кража банковской карты

«Классика жанра», злоумышленник, угрожая владельцу или скрытно, крадет карту и дальше использует ее в своих целях. Предварительно заранее выбрав вас в качестве цели и заглянув к вам через плечо, в то время когда вы снимали наличные в банкомате и вводили ПИН-код.

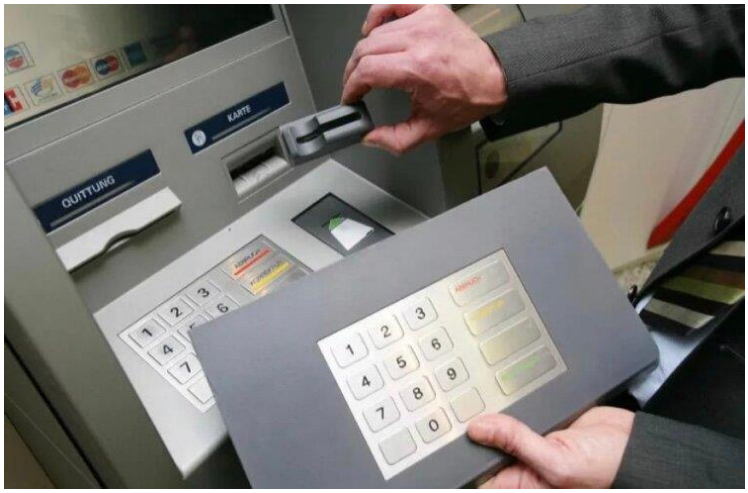
Установка поддельного банкомата

Злоумышленники устанавливают фальшивый банкомат, его не отличишь от настоящего, все атрибуты на месте – брэндинг, наклейки и инструкции. Вставив карту и введя ПИН-код, вы видите на экране сообщение о

неисправности устройства или об отсутствии наличных. Вы забираете карту и уходите на поиск другого банкомата. В это время с вашего счета списываются все деньги, ведь необходимые данные мошенниками уже считаны.

Скимминг

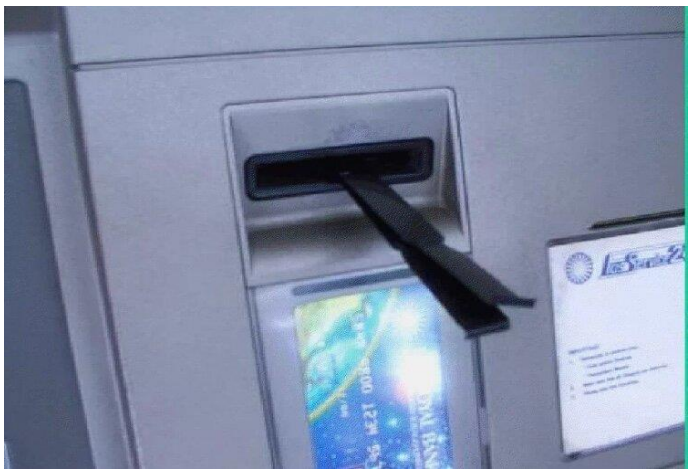
Скиммером называется устройство для считывания данных карты. Он может устанавливаться в виде накладки на кардридер банкомата, при этом он маскируется как часть конструкции или находится в руках кассира, вступившего в сговор с мошенниками.
ПИН-код в данном случае узнается при помощи установки накладной клавиатуры, которая запоминает порядок нажатия клавиш, или скрытой камеры, направленной так, чтобы зафиксировать ввод ПИН-кода владельцем карты.



Скиммер и накладная клавиатура. Будьте бдительными

Траппинг или «ливанская петля»

В кардридер банкомата вставляется кусок пластика с прорезью, который при попадании в нее карты, блокирует возврат. Задача мошенника в этот момент подойти и внушить вам, что он уже был в такой ситуации, его цель – дать вам совет о том, что необходимо ввести ПИН-код. Когда это не помогает, вы уходите в не лучшем настроении, ну а ваш случайный знакомый достает карту и отправляется за добычей, ведь ПИН-код он уже знает.



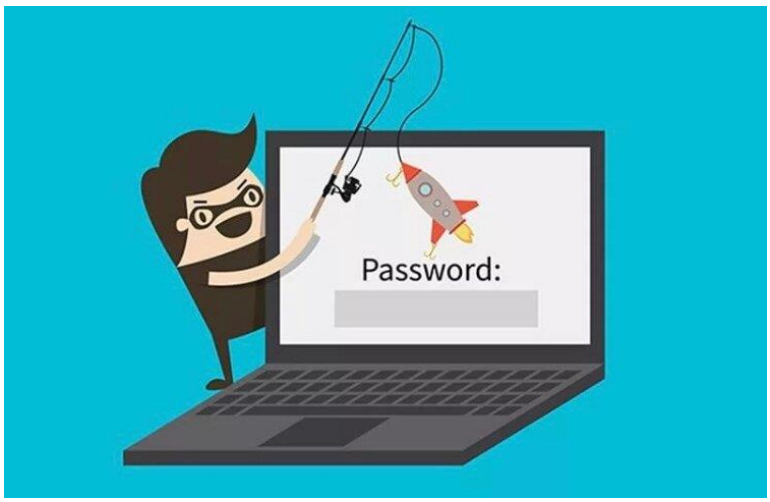
Так выглядит "ливанская петля"

Развод с помощью телефона

Используя методы социальной инженерии, мошенники манипулируют жертвой с целью получения информации о карте. Это могут быть звонки о выигрыше в лотерею, в этом случае вам предлагают передать реквизиты для перечисления денег; под видом службы безопасности вам могут сообщить о том, что с карты списаны средства и для отмены операции надо сообщить ее данные.
Злоумышленник говорит поставленным голосом, уверен в себе и имеет подготовленные ответы на ваши вопросы. Сюда же относятся всевозможные СМС-рассылки, попавшихся на крючок просят сообщить данные карты, подойти к банкомату и ввести ПИН-код или сообщить коды доступа к мобильному банку.

Фишинг и интернет-мошенничество

Преступники создают так называемый фишинговый сайт, выдавая его за настоящий. Наполнение страницы полностью копируется с оригинала кроме незаметной опечатки в адресной строке. В дальнейшем через социальные сети и онлайн-мессенджеры распространяются ссылки с просьбой перейти и уточнить (проверить) свои данные по карте. Цель мошенников – доступ к вашему мобильному банку, в личном кабинете которого они моментально переведут деньги на свои счета.
Аналогичную цель преследует создание ложных интернет-магазинов и распространение вирусных программ. Сюда же можно отнести и мошенничество с помощью известных интернет-площадках бесплатных объявлений.



От английского fishing - «рыбная ловля, выуживание»

Чтобы обезопасить ваш капитал от посягательств мошенников рекомендую соблюдать простые правила обращения с банковскими картами:

1. Получив ПИН-код, запомните его и храните отдельно от карты. Ни в коем случае не пишите его на самой карте. Самый надежный способ хранения ПИН-кода, это выучить его наизусть и держать в голове.

2. Не передавайте карту в руки посторонних и не оставляйте в общедоступных местах, для своих родственников всегда можно выпустить дополнительную карту с привязкой к счету с установленными лимитами.

3. Запишите телефонные номера служб поддержки клиентов банка в свой сотовый телефон, это позволит вам отличать телефоны мошенников и оперативно осуществлять блокировку карты.

4. Сотрудники банка никогда не спрашивают конфиденциальные сведения и не рассылают письма с предложениями перейти на адрес сайта.

5. Подключите услугу смс-информирования о балансе на карте и произведенных операциях, установите ограничения по сумме снятия и перевода наличных.

6. Пользуйтесь банкоматами, установленными в крупных общественных местах, в первую очередь в отделениях банка.

7. Вводя ПИН-код, закрывайте клавиши рукой от посторонних глаз или камер. Карта в кардридер должна вставляться без усилий, если она «не идет» найдите другой банкомат.

8. Расплачивайтесь безналичным способом только в проверенных магазинах крупных сетей. В обычном ларьке лучше рассчитаться наличными.

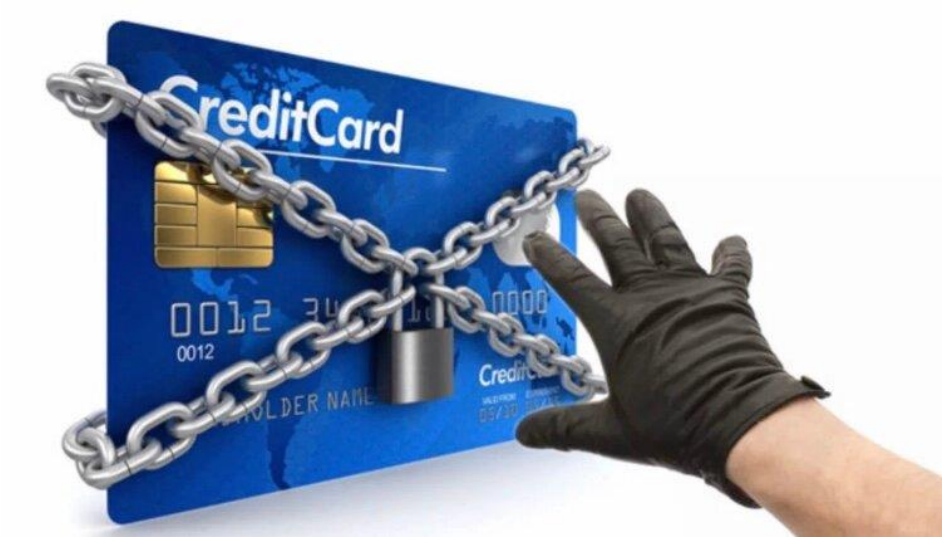
9. Передавая карту продавцу, не упускайте ее из вида и ни в коем случае не сообщайте ему ПИН-код. Можно озвучить только последние 4 цифры номера карты, в случае если она без чипа.

10. Для оплаты покупок в интернет-магазинах используйте отдельную карту, переводите на нее сумму покупки непосредственно перед совершением операции.

11. Проверяйте адрес интернет-ресурса, не пользуйтесь сайтами вызывающими подозрение. Делайте покупки только на известных интернет-площадках.

12. установите на компьютер антивирусную программу, оплачивайте товары только со своего компьютера.

13. ПИН-код в интернет-платежах никогда не используется, в таких случаях используют код CVV/CVC,который указан на обороте карты.



Соблюдение правил использования карт - надежная преграда на пути мошенников. Все фото взяты с интернет-просторов

Если же мошенникам каким-то образом удалось списать деньги с карты, необходимо выполнить следующее:

1. Звоним в банк и блокируем банковскую карту, получаем информацию о последних операциях по счету и остатке средств.

2. Не позднее 24 часов после списания средств, в отделении банка пишем заявление на возврат средств в двух экземплярах. Свой экземпляр визируем у сотрудника банка.

3. Заявляем в полицию.

4. Банк может отказать в возврате средств лишь в том случае если сможет доказать, что имело место нарушение порядка использования карты. Если этого не произошло, ожидаем возврат средств.