Украсть деньги с банковской карточки сложнее, чем вытащить из кошелька. Тем не менее, мошенники осваивают новые технологии и научились подбирать ключи даже к банковским картам.

Какая информация о вашей карте нужна злоумышленникам?

Им нужны реквизиты вашей карты: номер карты, имя и фамилия владельца, срок действия, код проверки подлинности карты (три цифры на обратной стороне, например, CVV или CVC), ПИН-код. Также код из смс для подтверждений платежей и переводов на тех сайтах, где платежи нужно подтверждать с помощью такого кода.

Место действия: магазин или кафе

1. Вы платите обычной банковской картой

Злоумышленником может оказаться работник сферы торговли и услуг. Официант, кассир или продавец, принимая для расчета вашу банковскую карту, может сфотографировать нужные данные (номер карты, срок действия, имя владельца и код на обратной стороне), а после расплатиться ей в интернете.

Как предотвратить?

Рассчитываясь, постарайтесь не упускать из вида свою карту. И вводите ПИН-код так, чтобы он не был виден посторонним.

2. Вы платите через терминал, но оплата не проходит

В кафе официант приносит вам POS-терминал (на картинке), вы расплачиваетесь, но тут официант говорит, что оплата не прошла, и просит повторно ввести ПИН-код. Делая это, вы рискуете заплатить дважды.

Как предотвратить?

Подключите смс-уведомления о платежах. Обязательно попросите чек с уведомлением о сбое или отказе от операции (POS-терминал всегда печатает такой).

3. Вы платите картой с системой бесконтактной оплаты

Картами с системой бесконтактной оплаты можно расплачиваться мгновенно, в одно касание, если ваш платеж не превышает определенный лимит. ПИН-код при этом вводить не нужно. Злоумышленники могут похитить деньги с такой карты, прислонив считыватель или POS-терминал к сумке.

Как предотвратить?

Чтобы бесконтактная оплата не проходила без вашего ведома, карту лучше хранить в экранирующем отсеке кошелька, сумки или специальном чехле для банковских карт.

Место действия: банкомат

Самый распространенный способ кражи реквизитов карты (номер, имя и фамилия владельца, срок действия) при ее использовании в банкомате — установка на банкомат скиммера. Это специальное устройство, которое копирует данные с магнитной полосы карты. Могут украсть и ПИН-код, установив на банкомат скрытую камеру или накладную клавиатуру. Поддельную клавиатуру ставят прямо поверх оригинальной, и сам банкомат реагирует на нажатия как обычно — вы даже не заметите, что что-то идет не так. Злоумышленники, используя украденные данные, могут изготовить копию вашей карты.

«Приехал как-то к другу в Москву, около его дома заглянул в магазин — а там только наличными оплата. Побежал к банкомату, торопился. Непримечательный такой банкомат в том же магазине нашел, рядом еще крутились двое парней-«техников» в униформе, с оборудованием, настраивали что-то...»

Будьте бдительны, не наступайте на чужие грабли!

Как предотвратить?

Скиммер способен украсть информацию только с магнитной полосы, но не со специального чипа.

- Проверьте банкомат: нет ли на нем посторонних устройств. Клавиатура не должна отличаться по фактуре, а тем более шататься.
- Когда вводите ПИН-код, всегда прикрывайте клавиатуру свободной рукой, чтобы никто не подсмотрел.
- Старайтесь пользоваться банкоматами внутри отделений банков. Их чаще проверяют и лучше охраняют.

Лучше всего, если на банкомате есть «крылья» для клавиатуры — на них невозможно поставить накладную клавиатуру, а также сложнее подсмотреть ваш ПИН-код.

Место действия: где угодно

1. Вы получили тревожное смс-сообщение или звонок от родственника

С незнакомого номера вам пишет или звонит якобы родственник и говорит, что попал в беду и ему срочно нужны деньги, но времени объяснять ситуацию у него нет. В таких

сообщениях часто манипулируют срочностью ситуации, и присылают их в крайне неудобное время, например, ночью.

Как предотвратить?

Не спешите переводить деньги. Попытайтесь выяснить детали — обычно долгие разговоры не входят в планы злоумышленников. Если выяснить ничего толком не удалось, перезвоните родственнику, от имени которого обращаются, чтобы убедиться, он ли вам звонит/пишет.

2. Вам пришло сообщение «от банка»

С незнакомого номера приходит смс-сообщение, что ваша карта заблокирована. В смс указан номер, по которому нужно позвонить для уточнения деталей. Позвонив, вы попадете в фальшивую службу безопасности банка, где вас будут убеждать сообщить данные карты или подойти к ближайшему банкомату и произвести операции. Выполнив указания злоумышленников, вы откроете им доступ к карте и они украдут ваши деньги.

«У меня на удочку мошенников через мобильный попался отец. Сначала он получил смс якобы от меня с чужого номера, где просили ничего не спрашивать и пополнить счёт. Сообщение отец увидел, кстати, уже после того, как завершилась история, а мошенники решили долго не ждать ответа и испытать удачу другим путём...»

Будьте бдительны, не наступайте на чужие грабли!

Как предотвратить?

Не перезванивайте — сперва выясните, действительно ли звонили из вашего банка. Настоящие банки обычно присылают уведомления с одного и того же номера. Кроме того, на вашей карте указан телефонный номер для связи с банком — позвоните по нему и уточните, заблокирована ли она. Или обратитесь к сотрудникам ближайшего отделения банка.

3. Вам звонят из госучреждения

Вам звонят люди и представляются сотрудниками Банка России, прокуратуры, суда, Министерства здравоохранения, Министерства финансов и других учреждений. Они сообщают, например, о положенном возмещении ущерба от действий мошенников: о компенсации за купленные медицинские товары или услуги экстрасенсов. Если для получения обещанной компенсации «сотрудник» попросит вас что-то оплатить (подоходный налог, налог на прибыль, банковский сбор, обязательную страховку,

госпошлину, комиссию за перевод денег), а тем более попросит предоставить паспортные данные или банковские реквизиты, это — телефонный мошенник.

Как предотвратить?

Не следуйте указаниям и ничего не оплачивайте. Не предоставляйте личную информацию, у настоящих сотрудников она уже есть.

Место действия: дом

1. Вам пришло письмо или уведомление

Вы получаете по почте уведомление на бланке с реквизитами Банка России. В нем сказано, что суд постановил выплатить вам компенсацию, для этого нужно связаться с контактным лицом. И как можно скорее, иначе компенсация перейдет в пользу государства — так злоумышленники подталкивают вас действовать.

Как предотвратить?

Не спешите связываться с контактным лицом, указанным в письме, проверьте данные. Позвоните по номеру телефона для обращений, указанному на официальном сайте Банка России. Если письмо оказалось фальшивым, обратитесь с жалобой в правоохранительные органы.

Помните, Банк России присылает СМС и e-mail только в ответ на ваше обращение через Интернет-приемную.

СМС-сообщения от регулятора поступают с короткого номера 3434, электронные письма – с адреса noaddress@cbr.ru.

Любые сообщения с других номеров, особенно требующие введения ПИН-кода, подтверждения операций, предоставления личных данных и других сведений, следует расценивать как попытку мошенничества.

Защититесь от мошенников:

- Подключите мобильный банк, чтобы отследить операции, которые вы не совершали. Так вы сможете оперативно отреагировать на действия мошенников — а время в этом случае очень важно.
- Не храните крупные суммы денег на карте, которую вы носите с собой и используете для повседневных трат.

- Если вы планируете использовать карту только в России — обязательно сообщите об этом сотрудникам банка.
- Расскажите пожилым родственникам об уловках мошенников — именно они чаще всего становятся мишенью злоумышленников.

Что делать, если вы все-таки столкнулись с мошенничеством?

Если с вашей банковской карты вдруг списали деньги:

- Как можно скорее позвоните в банк (номер есть на обороте карты), сообщите о мошеннической операции и заблокируйте карту.
- Обратитесь в отделение банка и попросите выписку по счету. Напишите заявление о несогласии с операцией. Сохраните экземпляр заявления с отметкой банка о приеме.
- Обратитесь в правоохранительные органы с заявлением о хищении.

Банк рассмотрит заявление в течение 30 дней. Если операция была международной — в течение 60 дней.

Компенсация

Получив ваше заявления, банк проведет служебное расследование и решит вопрос о возмещении ущерба. Если вы соблюдали меры безопасности и обратились в банк не позже, чем через сутки после списания денег, то можете рассчитывать на возмещение. Однако если вы сами сообщили злоумышленникам ПИН-код или код из смс, необходимый для подтверждения платежей и переводов, к сожалению, банк не вернет вам денег.