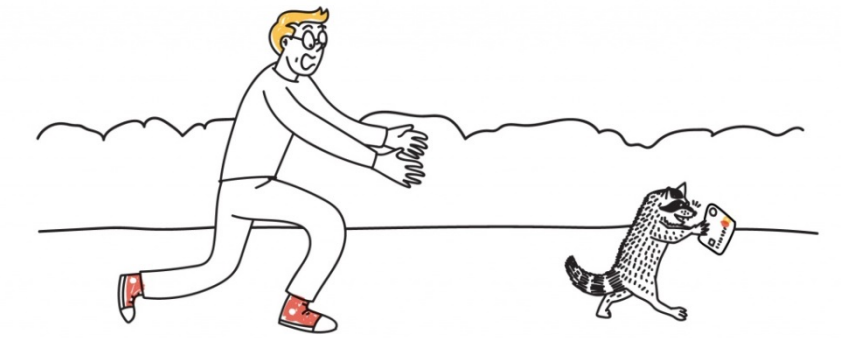
Списание денег со счета без ведома владельца, кража паролей и ПИН-кодов, легкий заработок в интернете и вклады под невероятные проценты, онлайн-казино — все это виды финансового мошенничества.

Преступники будут спекулировать на ваших чувствах, обещать золотые горы, маскироваться под сотрудников банков или государственные организации, чтобы выманить деньги. Как распознать мошенника и что делать, если вас все-таки удалось обмануть?



Стать жертвой преступников может каждый, и неважно, использует он банковскую карту или предпочитает рассчитываться наличными. Мошенники умеют выманивать деньги онлайн, с помощью звонков и СМС, в социальных сетях и офисах. Как они это делают?

Мошенничество с банковскими картами

Чтобы использовать вашу карту в своих целях, мошенникам нужно узнать ее номер, имя владельца, срок действия, номер CVC или CVV. Они могут установить скиммер на банкомат (специальное устройство, которое накладывают на приемник карты в банкомате) и видеокамеру над клавиатурой.

Номер CVC или CVV — три цифры, расположенные на поле для подписи владельца карты или рядом с ним.

Достаточно один раз воспользоваться таким банкоматом и не прикрыть рукой клавиатуру в момент набора ПИН-кода — и ваши деньги могут снять, перевести на несколько счетов и обналичить. Украсть данные вашей карты могут даже в кафе или магазине. Злоумышленником может оказаться продавец, который получит доступ к вашей карте

хотя бы на пять секунд. Сфотографировав вашу карту, он сможет воспользоваться ей для расчетов в интернете.

Как не попасться

- Перед снятием денег в банкомате осмотрите его. На картоприемнике не должно быть посторонних предметов, клавиатура не должна шататься.
- Набирая ПИН-код, прикрывайте клавиатуру рукой. Делайте это даже во время расчетов картой в кафе.
- Подключите мобильный банк и СМС-уведомления.
- Если совершаете покупки через интернет, никому не сообщайте секретный код для подтверждения операций, который приходит вам по СМС.
- Старайтесь никогда не терять из виду вашу карту.

Меня обокрали. Что делать?

1. Позвоните в банк (номер всегда есть на обороте карты или на главной странице сайта банка), сообщите о мошеннической операции и заблокируйте карту;
2. Запросите выписку по счету и напишите заявление о несогласии с операцией;
3. Обратитесь с заявлением в отдел полиции по месту жительства или отправьте обращение в управление «К» МВД России.

КТО И КАК ОХОТИТСЯ ЗА ВАШИМИ БАНКОВСКИМИ КАРТАМИ

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.

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.

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 не рассылает смс и e-mail.

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.

По материалам сайта http://fincult.info/articles/moshennichestvo-bankovskimi-kartami/kto-i-kak-okhotitsya-za-vashimi-kartami/

МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ ОНЛАЙН

Стать жертвой мошенника можно не только на улице. С развитием технологий охотники за наживой быстро освоили и виртуальное пространство. Рассмотрим, какие схемы работают в интернете и как можно обезопасить себя от кражи.

Место действия: сервис объявлений

Если вы решили купить товар с рук или продать ненужную вам вещь, будьте внимательны — мошенники нередко играют роль покупателей или продавцов. На ваш товар находится крайне заинтересованный покупатель, который готов перевести аванс на ваш счет и просит у вас не только номер карты или номер телефона, но и код проверки подлинности карты (три цифры на обратной стороне, например, CVV или CVC). Такой подход должен вас насторожить — ведь для перевода денег достаточно знать только номер карты.

Если вы покупаете товар с рук, у вас могут попросить предоплату и сообщить все данные карты. Если перед вами мошенник, то в лучшем случае вы останетесь без денег, которые отправили авансом. В худшем — если у вас попросили все данные карты — рискуете остаться и без средств на счете.

Как предотвратить?

Будьте осторожны, покупая товары с рук через социальные сети или специальные сайты. Всегда старайтесь проверить потенциального покупателя или продавца по отзывам. В сообществах и на сервисах обычно есть «черный список» (и покупателей, и продавцов) и модераторы. Проверьте профиль продавца — часто мошенники создают фальшивые страницы с минимумом информации.

Место действия: социальные сети и мессенджеры

Ваш друг прислал вам личное сообщение с просьбой одолжить денег или со странной ссылкой. Это значит лишь одно — аккаунт вашего друга взломали.

Незнакомый человек пишет вам личное сообщение, в котором предлагает стабильный и высокий доход за некую несложную работу. В сообщении нет конкретной информации, но есть ссылка, по которой вы якобы найдете подробности. По такой ссылке нет работы мечты — разве что компьютерный вирус.

Часто мошенники представляются сотрудниками известных брендов и компаний из любых областей. Вам обещают кредиты под низкий процент, большие скидки, бесплатные товары или говорят, что вы выиграли в конкурсе. Чтобы получить приз или скидку, от вас требуется всего ничего — сообщить данные вашей карты, паспорта или все сразу.

Как предотвратить?

Если странные сообщения через социальные сети шлет ваш друг, как можно скорее позвоните ему и выясните, действительно ли ему нужна помощь. Или мошенники взломали его аккаунт — и могут обмануть кого-то еще. Например, его бабушку!

Ссылки из сообщений незнакомцев — не лучший способ искать заработок в интернете, потому что бесплатный сыр бывает только в мышеловке.

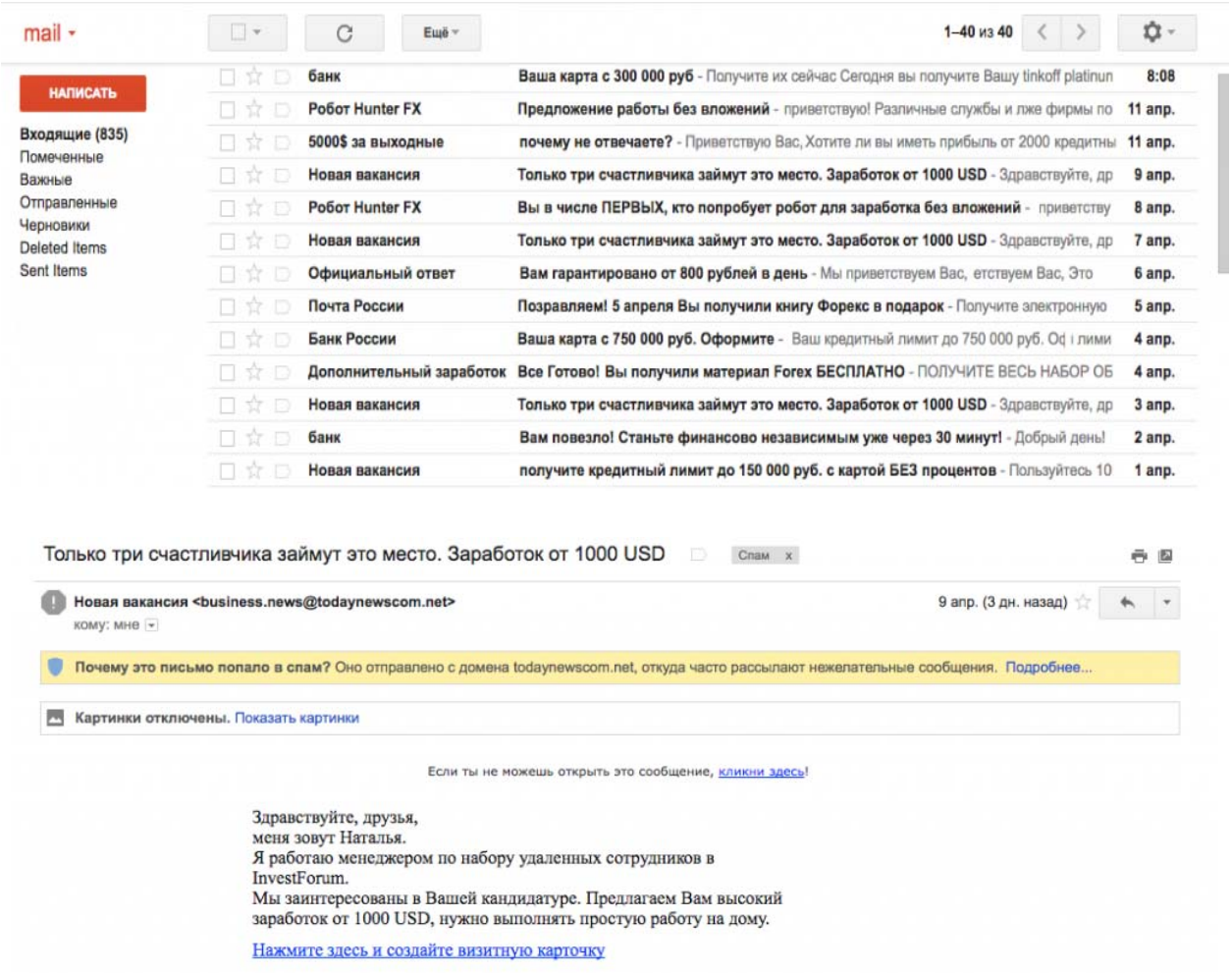
Если незнакомцы пишут вам от лица компании или бренда, лучше уточнить информацию на официальном сайте компании или ее странице в социальной сети — крупные компании редко проводят конкурсы, в которых вы можете победить, даже не участвуя, и никогда просто так не запрашивают ваши личные данные, а тем более данные карты.

Место действия: электронная почта

Вам на почту присылают письма с обещанием подарков, денег и кредитов. Мошенники пытаются заманить вас чем угодно: предлагают работу с большой зарплатой, которую вы не искали. Пишут, что вы выиграли машину. Присылают ответ на якобы ваше письмо. Просто хотят «познакомиться поближе».

В строке отправителя может быть как неизвестный вам человек (часто иностранец), так и известный сайт, платежная система, онлайн-сервис или банк. Ничего страшного не произойдет, если вы просто откроете письмо, но не переходите по ссылкам и не

скачивайте вложения из письма — так вы рискуете заразить компьютер вирусом, который позволит мошенникам его контролировать. И тем более не вводите данные вашей карты.



Как предотвратить?

В почте есть встроенный спам-фильтр — часть подозрительных писем всегда попадает в специальную папку. Но, несмотря на это, всегда обращайте внимание на заголовок письма, его отправителя и содержание. Компании всегда рассылают почтовые рассылки с одних и тех же адресов и редко допускают ошибки в письмах — а вот мошенники часто пишут с большим количеством ошибок, нечитаемых системой символов и перевирают название компании в адресе. Не переходите по ссылкам из таких писем и не скачивайте вложения из них.

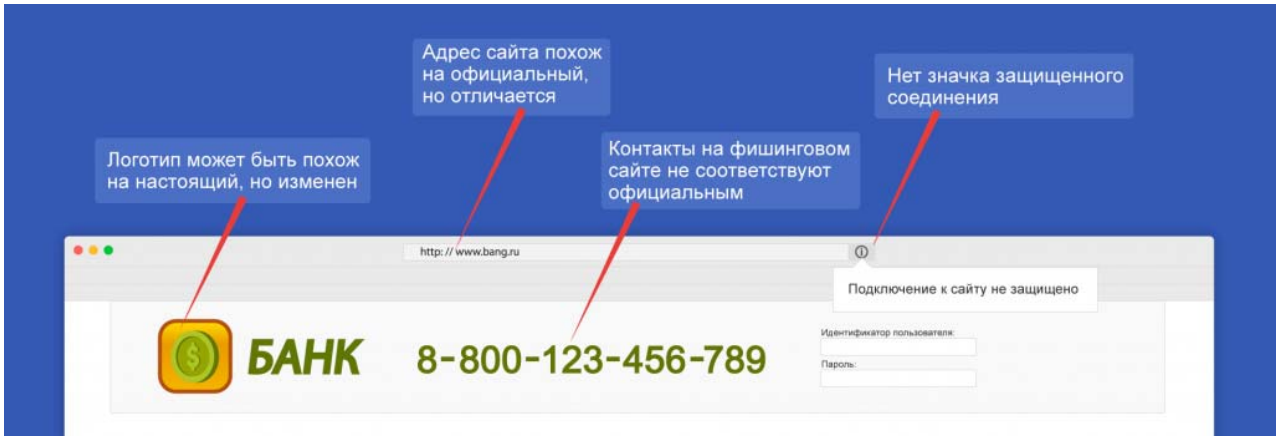
Место действия: сайт-двойник

Мошенники копируют известные сайты, используя похожее название компании и оформление. Например, вы хотите узнать, есть ли у вас штрафы в ГИБДД или как оформить кредит онлайн, а попадаете на фишинговый сайт, то есть сайт-клон. Если вы введете на таких сайтах свои данные, они попадут в руки злоумышленников.

Как предотвратить?

Всегда обращайте внимание на адресную строку браузера: на сайте-клоне будет допущена ошибка. Оплачивайте покупки только через сайты с защищенным соединением и значком платежной системы. Внимательно изучите и содержание сайта — злоумышленники часто невнимательно относятся к наполнению сайта. Добавьте в закладки сайты, которыми

часто пользуетесь, чтобы не набирать адрес вручную — так вы не ошибетесь в названии и попадете на нужный вам сайт.



Место действия: ваш смартфон

Зловредные программы умеют маскироваться под мобильные банки и таиться в разных приложениях, которые вы скачиваете на телефон.

Как предотвратить?

Скачивайте приложения на телефон только в официальном магазине. Обращайте внимание в первую очередь на разработчика приложения — в официальных банковских приложениях указан сам банк. Внимательно читайте описание приложения. Не скачивайте приложения сторонних разработчиков.

По материалам сайта http://fincult.info/articles/moshennichestvo-bankovskimi-kartami/moshennichestvo-s-bankovskimi-kartami-online/