

# Онлайн-мошенничество с банковскими картами



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.

## 1. 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.



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.



## 1. 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.



Если странные сообщения через социальные сети шлет ваш друг, как можно скорее позвоните ему и выясните, действительно ли ему нужна помощь.

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.

## 1. ЭЛЕКТРОННАЯ ПОЧТА

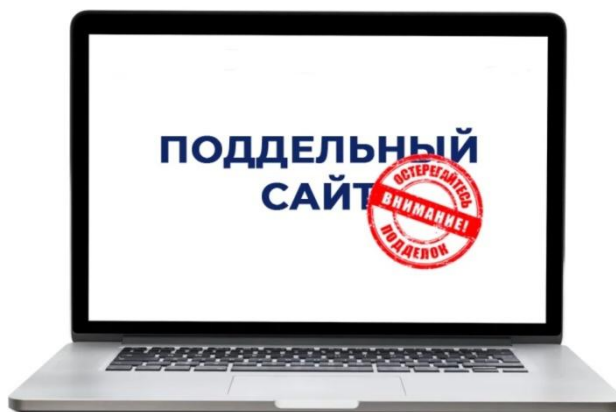
Вам на почту присылают письма с обещанием подарков, денег и кредитов. Мошенники пытаются заманить вас чем угодно: предлагают работу с большой зарплатой, которую вы не искали. Пишут, что вы выиграли машину. Присылают ответ на якобы ваше письмо.

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.



**ВАЖНАЯ  
ИНФОРМАЦИЯ!**

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.



## 1. ПОДДЕЛЬНЫЙ САЙТ

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.

**ВАЖНАЯ  
ИНФОРМАЦИЯ!**

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.

## 1. ВАШ СМАРТФОН

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

**ВАЖНАЯ  
ИНФОРМАЦИЯ!**

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

