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?

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

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

Место действия: сайт-двойник

Мошенники копир
сайты, используя пох
компаний 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 программы — в официальных банковских приложениях указан сам банк.

Внимательно читайте описание и не скачивайте приложения сторонних разработчиков.

Мошенники научились списывать все деньги с карты под видом продажи билетов на концерты и в театр

Аферисты рассылают фейковые предложения о продаже билетов. Но вместо пропуска на мероприятие человек покупает подписку, которая позволяет мошенникам списать все деньги с его карты. О новой схеме обмана сообщает РБК.

Такие рассылки от псевдопродавцов билетов приходят людям по электронной почте, через мессенджеры, соцсети или сайты знакомств. Фишинговая ссылка из сообщения ведет на страницу оплаты, где нужно вбить персональные сведения и реквизиты карты.

Если человек вводит данные, он фактически оформляет подписку на «услуги» мошенников. С карты жертвы тут же списываются деньги — несколькими транзакциями на суммы от 5000 до 20 000 рублей. Перерывы между такими списаниями составляют всего несколько секунд. Так что к моменту, когда владелец карты успеет что-либо предпринять, преступники уже опустошают его счет.

Вернуть деньги, украденные мошенниками, вряд ли удастся. Ведь в случае, когда пользователь нарушил правила безопасности и сам передал аферистам секретную информацию, банк не обязан ничего компенсировать.

Как защитить свои деньги и данные?

1. Не переходите по ссылкам из электронных писем, сообщений в мессенджерах, СМС или рекламных объявлений. Безопаснее самостоятельно найти официальный сайт компании, услугами которой вы хотите воспользоваться. В поисковых системах «Яндекс» и Mail.ru настоящие сайты театров, а также сервисов по продаже билетов маркируются специальными галочками.
2. Для онлайн-покупок лучше завести отдельную карту и каждый раз вносить на нее необходимую для покупки сумму либо установить лимит по количеству и размеру операций.

Мошенники придумали новую легенду для кражи данных с Госуслуг

Пользователи портала «Госуслуги» начали получать сообщение о техническом сбое, из-за которого их якобы открепили от поликлиники. Чтобы заново прикрепиться, им предлагают перейти по ссылке, ввести свои регистрационные данные от портала и оплатить пошлину. На самом деле эти уведомления рассылают мошенники, чтобы выманить деньги и доступ к чужим личным кабинетам. О новой схеме обмана сообщает агентство «РИА Новости».

В письме аферисты пугают пандемией и призывают действовать как можно быстрее. Таким образом они пытаются помешать людям спокойно оценить ситуацию и проверить информацию.

Ссылка из мошеннического письма ведет на фишинговый сайт– двойник портала «Госуслуги». На поддельной странице посетителя просят заполнить анкету с личными данными, в том числе указать логин и пароль от аккаунта на портале. Затем человеку предлагают выбрать медицинское учреждение из списка и заплатить за повторное прикрепление пошлину – до нескольких тысяч рублей.

В итоге вместе с деньгами преступники получают доступ ко всем персональным данным пользователя портала. Они могут продать эту информацию на черном рынке другим мошенникам, использовать в схемах социальной инженерии , а в худшем случае – набирать займов и кредитов на имя владельца учетной записи.

Вернуть деньги, переведенные мошенникам, почти невозможно: если пользователь нарушил правила кибергигиены и сам сообщил аферистам секретную информацию, банк не обязан ничего компенсировать.

В случае, когда злоумышленники добрались до ваших личных данных и набрали долгов на ваше имя, их можно оспорить. Но придется запастись терпением: отстаивать свои права часто приходится через суд.

Если вы получили уведомление «об откреплении от поликлиники», для начала стоит проверить, есть ли оно в вашем личном кабинете на Госуслугах. Обязательно нужно самостоятельно набрать адрес портала, а не переходить по ссылке из сообщения от незнакомцев.

Чтобы не было сомнений, стоит также связаться с вашей поликлиникой. В любом случае за прикрепление к государственному медучреждению ничего платить не нужно.

Всегда необходимо тщательно проверять адресную строку сайта, на котором вы вводите свои платежные или личные данные. Еще лучше – сохранить в закладках страницы, которыми вы пользуетесь, или заходить в них через проверенные приложения.