# Держите ваши денежки: популярные схемы мошенничества в интернете

**Инвестиции**

Статьи РБК

Интернет-мошенники внимательно следят за техническими новинками и происходящими в мире событиями и подстраивают под них свои методы отъема денег у населения. Чтобы свести к минимуму риск обмана, стоит проверять каждую сделку по своего рода чек-листу

Фото: Андрей Любимов / РБК

Наступает осень. За лето, как правило, многие из нас успевают поиздержаться в отпусках, да еще и детей в школу надо собирать, и нам остро нужны деньги. Нечистые на руку граждане не исключение. Шутки шутками, но ближе к сентябрю мошенники действительно активизируются. Причем своей мишенью они выбирают не только частных лиц, но и целые компании. Масштабы впечатляют: по данным ЦБ, в 2022 году розничные клиенты банков сообщили о 516 тыс. операций без их согласия, совершенных при оплате товаров и услуг в интернете, из которых половина — результат применения к ним приемов и методов социальной инженерии. Сумма хищений превысила 2,5 млрд руб. Мы расспросили экспертов, в каких ситуациях мы рискуем попасть на поле чудес и как не остаться в дураках.

## Маска, я тебя знаю

Не будем повторять столь же разумный, сколь и распространенный совет не раскрывать свои банковские данные, пароли и личную информацию малознакомым или вовсе не знакомым людям или сайтам. Когда дело касается денег, стоит под лупой разглядывать и очень старых знакомых: среди них могут оказаться мошенники, мимикрирующие под известные бренды и компании. Жулики, промышляющие фишингом (так называется мошенничество, имеющее целью получить личную информацию), постоянно используют все новые схемы, предупреждает Виктор Смирнов, основатель группы финансовых сервисов CosmoVisa (специализируется на предоставлении услуги чарджбек и на защите пользователей в сегменте e-com от мошенников). Один из таких методов — фейковые скидочные купоны. «Мошенники проводят массовую веерную рассылку по электронным адресам и настраивают агрессивную диджитал-рекламу, предлагая различные купоны, которые помогут сэкономить до 90% на покупках в интернет-магазинах и на маркетплейсах. Чтобы ими воспользоваться, нужно ввести свои данные, в том числе банковской карты, для будущей оплаты. Таким образом мошенники получают доступ к счету и переводят деньги со счета потерпевшего на свои счета или совершают онлайн-покупки». Проверяя достоверность акции и репутацию продавца, обратите внимание: рассылки настоящих компаний не содержат вложений, есть кнопка «отписаться от рассылки» и указан адрес отправителя, советует Смирнов.

Если мошенники все же получили доступ к вашим данным, прежде всего свяжитесь с вашим банком, чтобы заблокировать дальнейшие операции и начать процесс возврата средств, если это возможно. «И обязательно обратитесь в полицию с заявлением о мошенничестве. Сообщите все детали и предоставьте все доказательства, которыми вы располагаете. Банк вряд ли примет решение о возврате средств в вашу пользу, если вы не обратитесь в полицию. Если дело о мошенничестве будет возбуждено, а преступник будет найден, вы сможете попытаться отсудить у него свои деньги». Правда, нет никаких гарантий, что у владельца банковской карты, на которую вы перевели деньги, будет что вам отдать, признает Смирнов: скорее всего, это подставное лицо, на которое настоящие мошенники зарегистрировали карту.

Интернет-приложения для смартфонов тоже могут оказаться фальшивыми, продолжает эксперт. Наиболее часто подделывают те ресурсы, где у пользователя хранится финансовая информация о его счетах, сбережениях и источнике их хранения — банковские приложения или цифровые кошельки. «Злоумышленники создают внешние копии известных приложений от крупных организаций. «По данным директора центра Solar appScreener компании «РТК-Солар» Даниила Чернова, которые приводила «Лента.ру», в январе—июне 2023 года, число фейковых приложений, ворующих персональные данные, выросло на 34% год к году, — приводит данные Смирнов. — На все сомнения относительно наименования приложения, внешнего вида и т.д. мошенники убеждают потребителя, что это вынужденная мера во избежание вторичных блокировок на известных площадках». У фишинговых приложений стартовые страницы похожи на настоящие: у клиента при первом скачивании не должно возникнуть сомнений, — а по факту оно может быть пустым. Когда пострадавший вводит туда свои логины и пароли, киберпреступники получают беспрепятственный доступ к оригинальному приложению клиента.

«Распознать фишинговое приложение легче, чем фишинговый сайт: приложения размещаются на определенных площадках, которые уже собрали первичную информацию о них. Во-первых, разработчик приложения должен быть прямо или косвенно связан с основными функциями, заложенными в приложении. Во-вторых, стоит задуматься, если на него мало отзывов: в финансовом секторе количество клиентов измеряется в миллионах», — перечисляет Смирнов. Если же вы уже стали пользователем фишингового приложения, срочно меняйте все логины и пароли в настоящем. Эффективнее всего будет временно заблокировать счета до смены всех паролей или даже вывести все имеющиеся средства со скомпрометированных приложений и завести новые счета, рекомендует эксперт.

## Утром в газете — вечером в куплете

Как ни странно, один из способов вовремя заподозрить обман — следить за повесткой дня: мошенники часто пользуются актуальными инфоповодами. **«Во время пандемии COVID-19, когда закрывали границы и отменяли полеты, они прозванивали людей, предлагая обналичить деньги за авиабилеты, возвращенные на спецсчет, привязанный к ваучеру. Далее схема предполагает звонок под видом сотрудника авиакомпании и получение данных карты и СМС-кода, верифицирующего пользователя при входе в личный кабинет, — рассказывает Борис Богоутдинов, управляющий партнер консалтинговой компании «2Б Диалог». — Аналогичная ситуация имела место с людьми, которые попадали в категорию малоимущих. Им звонили под видом сотрудников банков и сообщали, что государство выделило им финансовую помощь, которую можно получить, назвав реквизиты банковской карты. Более того, создавали клоны сайтов Госуслуг и других ведомств с целью якобы перевода пособий для семей с детьми. Жертвы вводили банковские реквизиты, что развязывало мошенникам руки».**

Иногда преступники даже не утруждают себя созданием фейков — главное, чтобы их «услуги» оказались для жертв злободневными. «Наша компания невольно стала участником схемы обмана потребителей — обман с использованием чужого фирменного наименования. «В последний месяц нам часто стали приходить звонки и запросы на электронную почту с уточнением, работает ли у нас тот или иной сотрудник. Каждый раз люди называли разные имена и фамилии. Выяснилось, что все спрашивающие в прошлом были участниками криптофинансовых пирамид и потеряли значительные вложения. В надежде найти способ вернуть их люди искали помощи в интернете и находили рекламу о возврате денежных средств, вложенных в пирамиды.

Рекламный баннер вел на интернет-сайт, на котором незаконно использовано наименование нашей компании и действующий юридический адрес, — рассказывает Илья Комиссаров, старший партнер и руководитель судебно-арбитражной практики юридической компании VILEX GROUP. — Люди обращались за юридической помощью, неизвестный голос на другом конце провода обещал вернуть вложенные деньги, но для этого нужно было оплатить комиссии, услуги обменника и пр. Потерпевшим гражданам от имени нашей компании присылались якобы подписанные гарантийные письма и договоры об оказании юридических услуг. Договоры содержали ИНН, ОГРН, КПП и юридический адрес нашей компании. Отличались

лишь печать и подпись генерального директора. В среднем каждый обманутый гражданин потерял на такой «юридической помощи» от 100 тыс. до 300 тыс. руб. Все денежные средства перечислялись на банковские карты неизвестных физических лиц в различные банки. Никакие вложенные средства, конечно, возвращены не были. Примечательно, что наш офис находится в Казани, а все обманутые люди находились в других регионах и даже странах: нам звонили из Казахстана, Узбекистана, Армении... Скорее всего, это было сделано, чтобы люди не могли лично обратиться по указанному юридическому адресу и раскрыть обман». Компания обратилась в правоохранительные органы по факту мошенничества и подделки документов. Сейчас стоит вопрос о возбуждении уголовного дела.

**Как минимизировать риск при сделках в Сети**

Не стоит оформлять покупки онлайн, будучи подключенным к общественному Wi-Fi. Через него мошенникам очень просто получить доступ к личной информации: Ф.И.О, адресу, номеру телефона, данным карт и т.д. Общественная сеть не использует шифрование, поэтому возможен перехват сообщений между устройством и сервером. В этом случае все логины и пароли, введенные пользователем, попадают к третьей стороне. Мошенники могут создать дублер общественной сети с тем же названием, и подключившиеся к такой сети пользователи рискуют невольно передать им все данные, которые они вводят во время оформления и оплаты покупки или захода в мобильный банк. Обращайте внимание на название Wi-Fi и избегайте подключения в местах, где есть сети с одинаковым названием.

Сайт добросовестного продавца имеет сертификат безопасности (SSL/TSL-сертификат) и предоставляет всю контактную информацию о себе. Сертификат безопасности, как правило, автоматически проверяется браузером, поэтому важно не игнорировать уведомления о его подлинности.

Важно обращать внимание на название сайта в адресной строке — URL-адрес. Мошенники стараются давать своим подделкам почти идентичные названия, заменяя или вкрапливая в URL похожую букву или знак. Именно эта деталь выдает даже самый филигранно воспроизведенный фишинговый сайт. У сайта должен быть сертификат безопасности: его название в адресной строке должно начинаться с HTTPS. Оплачивать покупки следует только через систему безопасных платежей, связанную с банком. Обращайте внимание, какие реквизиты сайт просит ввести для оплаты: это могут быть только номер карты, Ф.И.О. держателя и CVC-код для подтверждения оплаты. Если в форме оплаты вас просят ввести остаток по карте и номер телефона, сайт однозначно фишинговый.

Виктор Смирнов, CosmoVisa

## Утром деньги, вечером ничего

Отдельную инфраструктуру мошенники создают, чтобы порезвиться на торговых интернет-площадках. Покупатель находит товар по очень выгодной цене (это должно стать первым тревожным звоночком) и связывается с продавцом. Тот в какой-то момент предлагает перенести общение в сторонний мессенджер вроде WhatsApp, а там информирует, что находится в другом городе и уже готов отправить товар, но вместо сервиса хочет воспользоваться сторонней курьерской службой доставки, поскольку это удобнее/дешевле. «Продавец спрашивает у покупателя Ф.И.О., адрес доставки, номер телефона, после чего присылает заранее заготовленную ссылку на сайт курьерской службы (например avito-oplata3428.ru; yuola-oplata7185.ru), где нужно оплатить товар банковской картой. После этого мошенники реализуют сценарий в зависимости от доверчивости покупателя. Например, если после первого перевода

денежных средств мошенникам жертва этого не осознала, то ей под предлогом сбоя первого платежа предлагают провести операцию отмены и возврата денежных средств на карту, что по факту является очередным платежом мошенникам. Что делать? Читать СМС-сообщение от банка, в котором написано, что за операция была совершена и для какой операции направлен одноразовый пароль, и не сообщать никому код из СМС», — рекомендует Лилия Шароватова, генеральный директор Fuzzy Logic Labs (занимается транзакционным и кросс-канальным антифродом в России и СНГ). Еще один вариант — когда потенциальный покупатель интересуется товаром, продавец предлагает его забронировать или продать с выплатой аванса. **«После перевода денег продавцы исчезают. Оптимальный способ не стать жертвой — не вносить предоплату», — предупреждает Богоутдинов.**

Впрочем, жуликов полно и с другой стороны сделки, и тогда страдает продавец. Бич маркетплейсов и продавцов, торгующих на популярных онлайн-платформах, — подмена товара. **«Продавцы на «Авито», пользуясь «Авито Доставкой», отправляют бывший в употреблении товар. Покупатель в процессе приемки подменяет на такой же, только сломанный. Товар он не принимает и отправляет обратно, деньги продавец не получает, а при возврате получает не свой, а испорченный товар», — рисует ситуацию Богоутдинов.** Проворачивают мошеннические схемы как покупатели, так и сотрудники пунктов выдачи заказов (ПВЗ), комментирует Денис Ветренников, CEO экосистемы сервисов для продавцов маркетплейсов SellerDen. «Сотрудники заказывают товар в свой же пункт выдачи, не забирают его, а потом по истечении срока хранения отправляют коробку обратно на склад. Только внутри уже может оказаться что-то совсем другое. Покупатели умудряются подменить вещь прямо в примерочной, где нет камер видеонаблюдения. К счастью, и тех и других обычно удается вычислить полиции». К тому же Ассоциация компаний интернет-торговли сейчас разрабатывает единые стандарты для ПВЗ и маркетплейсов. В частности, документ должен определить ответственность работников пунктов при совершении противоправных действий — подмены или недовложения товара, рассказывает он.

Еще одной схемой поделился селлер-подписчик телеграм-канала Ветренникова. «По его словам, мошенническая схема работает на модели доставки rFBS (порядок работы, при которой продавец сам отвечает за хранение и доставку товара. — РБК). Суть вот в чем. Сейлер, торгующий на крупном маркетплейсе, отправляет заказ одной из этих логистических компаний, трек-номер передает в личный кабинет онлайн-платформы. При окончании срока хранения товара маркетплейс считывает статус заказа как «Отменен» и возвращает деньги покупателю. Но товар еще хранится в отделении логистического оператора, и покупатель, дождавшись возврата денег, забирает и товар тоже. В итоге сейлер остается без денег и без товара, а покупатель возвращает деньги и забирает товар. Маркетплейс получает комиссию, переводит стрелки на логистическую компанию, мол, «виноваты они, пишите им претензию, мы же со своей стороны попросим покупателя все же оплатить товар». Логистическая компания сообщает: «Мы приняли у вас товар, оказали услуги по перевозке и выдали товар получателю. Статус «окончание срока хранения» не подразумевает отмену заказа, и пока товар не покинул стены пункта выдачи, мы можем его выдать». Крайним остается сейлер». Стопроцентных вариантов избежать такой ситуации у него

нет, но в случае заказов дорогостоящих товаров или нескольких штук одного и того же товара по rFBS лучше будет отменить заказ, советует Ветренников.

Еще одно поле чудес — социальные сети. Например, сейчас есть множество телеграм-каналов, которые торгуют товарами в обход комиссии и некоторых правил площадок, рассказывает Иван Родионов, основатель и директор консалтингового агентства Rodionoff Group. «Суть схемы такова. Вам предлагают товар, который очевидно выгодно купить через магазин в соцсети или канале в мессенджере, а не напрямую с маркетплейса, дополнительно продавец обещает бесплатную доставку. Доставка осуществляется с использованием одного из маркетплейсов, что обеспечивает быструю логистику и удобное для клиента расположение пункта вывоза. Вы переводите на карту «продавца-мошенника» всю сумму за товар за исключением 100 руб., а на эти 100 руб. заказываете товар по ссылке, которую вам отправляют: как правило, какую-то мелочь. Через несколько дней вы идете забирать заказ, но вас ждет только безделушка за 100 руб. Деньги остаются у мошенника.

Даже если общение происходит через самые что ни на есть официальные ресурсы официальных площадок, есть шанс попасть в переплет. В последнее время мошенники, притворяясь кем-то из родных, просят помочь якобы попавшему в беду родственнику, передав наличные деньги или ценности через сервисы доставки. Как правило, жертвы — пожилые люди. «Курьеры, сотрудничающие с «Яндекс.Доставкой», регулярно проходят инструктаж, как распознать мошеннические схемы и как правильно действовать в подозрительных ситуациях. Недавно, приехав по адресу, с которого нужно было забрать заказ, отправитель, пожилая дама, передала пакет с вещами и сказала, что это вещи в больницу. Курьер обратил внимание, что в деталях заказа точка, куда нужно доставить посылку, вовсе не больница, а торговый центр. Он понял, что дело нечисто, поэтому вернул женщине пакет с вещами, предупредил, что это мошенники, вызвал полицию по адресу отправителя и дождался ее приезда», — рассказали в пресс-службе «Яндекс.Доставки».

Но рассчитывать на ресурсы платформ и внимательность их сотрудников все же не следует. Чтобы ненароком не профинансировать мошенников, стоит каждый раз, имея дело со сделками в Сети, личными или по долгу службы, внимательно изучать все детали. Даже опытные пилоты проверяют себя по чек-листу перед каждым полетом, и хотя здесь ставки ниже, бдительность лишней не будет. Иначе есть риск побить печальный рекорд прошлого года: согласно данным ЦБ, россияне передали мошенникам 14 млрд руб., а вернуть смогли всего 4,4% украденных средств, или 618,4 млн руб.