Пять способов потерять деньги, продавая вещи в интернете

Людям постоянно напоминают о правилах финансовой безопасности. Но далеко не все им следуют — и это приводит к потерям.

Ошибка № 1: раскрывать свои персональные данные

Жанна не хотела тратить много времени на общение с потенциальными покупателями, поэтому она сразу написала в объявлении номер своей карты, на которую надо переводить оплату за покупку. Свой мобильный она тоже решила не скрывать — ведь по телефону проще обо всем договориться. Ей действительно быстро позвонили. Но не потенциальный покупатель, а «сотрудник службы безопасности банка». Он сообщил, что по ее карте проводится подозрительная операция и чтобы ее отменить, нужно «пройти верификацию».

Номер карты «безопасник» назвал сам, Жанна должна была сказать остальные реквизиты — срок действия, имя владельца и три цифры с обратной стороны. После того как испуганная Жанна продиктовала всю информацию, с ее карты списали все деньги.

Что произошло: социальным инженерам, которые играют на чувствах людей, чтобы добраться до их счета, для начала разговора нередко достаточно и номера телефона. А Жанна оказалась настолько открытой, что им даже не пришлось выведывать номер ее карты.

По нему нетрудно определить и банк, выдавший карту, и платежную систему. Когда мошенники сами сообщают человеку эту «конфиденциальную информацию», у него часто складывается впечатление, что звонит настоящий сотрудник банка. И уже вызвав доверие, аферисты выманивают остальные, действительно секретные данные, которые открывают доступ к счету доверчивого собеседника.

! Воспользоваться персональными данными могут и недобросовестные маркетологи, которые собирают номера телефонов по открытым источникам, а потом одолевают вас рекламными предложениями.

Как стоит поступать: составляя объявление в интернете, ограничьтесь описанием товара. Не указывайте реквизиты карты и личные данные: точный адрес, номер паспорта и другую конфиденциальную информацию. Никогда не выкладывайте фотографии банковской карты и документов. Номер своего мобильного телефона тоже лучше скрыть, если портал или приложение для объявлений позволяют это сделать. Покупатели смогут позвонить на тот номер, который вам предоставит онлайн-площадка, или связаться в чате сервиса объявлений.

Ошибка № 2: обсуждать детали в сторонних мессенджерах

Как-то раз сумочка Жанны понравилась покупательнице из другого города. Она предложила обсудить, как лучше передать посылку, в популярном мессенджере.

Они обо всем договорились, и любительница сумочек скинула Жанне ссылку на «надежный и недорогой сервис доставки». Все выглядело убедительно: покупательница переводит обговоренную сумму курьерскому сервису, тот забирает посылку у Жанны и сразу же пересылает деньги на ее карту. Но когда Жанна заполнила анкету на сайте «курьерской службы», где указала, в том числе и все реквизиты своей карты, у нее украли деньги.

Что произошло: мошенники создают специальные фишинговые страницы, которые помогают им узнать данные карты пользователя. Эти страницы они маскируют под сайты служб доставки, платежные страницы сервисов объявлений, системы денежных переводов.

Если ввести на этих поддельных страницах полные реквизиты своей карты, включая секретный код с ее обратной стороны, аферисты фактически получат ключ от вашего счета.

Чаты сервисов объявлений обычно блокируют фишинговые ссылки. Именно поэтому мошенники стараются увести вас с защищенного сайта на стороннюю площадку.

Как стоит поступать: не отказывайтесь от услуги «безопасная сделка», которую часто предлагают крупные сервисы объявлений. В таком случае покупатель оплачивает товар банковской картой, деньги резервируются на счете онлайн-площадки и поступают на карту продавца, как только покупатель получит посылку.

Известные российские и международные курьерские компании тоже позволяют провести оплату по такой схеме. Если нет возможности рассчитаться с покупателем лично, можно отправить посылку наложенным платежом. Получатель оплатит ее в почтовом отделении, заберет товар, а почта переведет деньги вам.

Ошибка № 3: сообщать покупателю конфиденциальную информацию о банковской карте

Жанна решила купить домашний кинотеатр, а свой телевизор — продать. Практически сразу ей позвонили из телеателье и сказали, что готовы выкупить его — им как раз нужна именно такая модель. И даже предложили сразу же перечислить ей аванс.

В этот раз никаких секретных кодов у Жанны не спрашивали. Нужно было сказать только номер карты и срок ее действия. Но когда она их сообщила, с ее карты снова списали крупную сумму.

Что произошло: в некоторых онлайн-магазинах для покупки не нужно вводить трехзначный код с обратной стороны карты и коды подтверждения от банка. Мошенники этим пользуются. Они оплачивают счет чужой картой, зная только ее номер, срок действия и имя владельца.

Как стоит поступать: для перевода денег достаточно номера карты или счета. Никакую другую информацию сообщать нельзя.

Ошибка № 4: отдавать товар раньше, чем покупатель его оплатил

Жанна купила дорогие туфли, но не смогла в них ходить — каблук слишком высокий. Срок возврата в магазин уже закончился, так что она решила продать их. Покупательница с сайта объявлений приехала к ней домой, туфли ей понравились, и она сразу же перевела Жанне деньги через телефон. Жанна своими глазами видела, как девушка в приложении своего банка перекинула нужную сумму ей на карту. Вот только уведомление о поступлении денег Жанне почему-то не пришло.

«Такое бывает, что перевод с небольшой задержкой приходит, — убеждала ее покупательница. — Иногда через несколько минут. Но вы же сами видели — я все отправила. А сейчас извините, мне пора бежать». Девушка с туфлями скрылась, а Жанна своих денег так и не получила.

Что произошло: иногда аферисты используют демоверсии банковских приложений. Там можно сымитировать перевод — экран просто показывает, как перечисление денег будет выглядеть в приложении, но на самом деле суммы со счета на счет не переходят. В некоторых случаях мошенники создают сайты-дубликаты, которые похожи на настоящие онлайн-банки.

Как стоит поступать: так же, как в магазине. Сначала покупатель должен оплатить товар и только потом его забрать. С карты на карту перевод проходит буквально за минуту. Обязательно дождитесь, когда банк пришлет вам сообщение о зачислении денег.

Когда вам дают наличные, убедитесь, что деньги настоящие. Или попросите при вас снять сумму в банкомате. Опять же, может выручить услуга «безопасная сделка» сервиса объявлений или проверенной курьерской службы.

Ошибка № 5: переходить по ссылкам от незнакомцев

Жанна продавала старый диван. В этот раз она решила все расчеты проводить через приложение сервиса объявлений. Ей пришло СМС-сообщение, что покупатель уже перечислил депозит за ее диван, а в сообщении — верная сумма и ссылка.

Жанна перешла по ссылке и увидела страницу своего объявления с пометкой об оплате. А ниже была кнопка — обновить приложение, чтобы перевод прошел корректно. Жанна нажала эту кнопку, у нее открылось приложение, но потребовалось заново ввести контактные данные и реквизиты карты. А потом (ну вы уже поняли) — ее банковский счет обнулили.

Что произошло: мошенники создали поддельную страницу, которая повторила дизайн оригинального приложения. На эту страницу они вставили скриншот объявления Жанны, дорисовали пометку об оплате и добавили кнопку со ссылкой. Когда Жанна перешла по ссылке и скачала «обновленную версию приложения» сервиса объявлений, на самом деле она загрузила себе на телефон вирус. Вредоносные программы не только крадут данные карты, но и воруют пароли и коды от онлайн-банка. Так мошенники получают доступ ко всем банковским счетам и выводят с них деньги.

Как стоит поступать: нужно установить антивирусные программы на все свои гаджеты и регулярно их обновлять. Никогда нельзя переходить по ссылкам из писем и сообщений незнакомых пользователей.

Когда заходите на сайт известного вам онлайн-сервиса, магазина, банка или другой организации, крайне внимательно проверяйте адресную строку. Поддельные сайты бывают очень похожи на настоящие, а их адреса могут различаться всего одним-двумя символами.

Для получения бесплатной консультации о защите прав в сфере финансовых услуг, помощи в составлении документов Вы можете обратиться:

по телефону: + 7(3547)2-02-04

прислать обращение на электронную почту: Gossank@chel.surnet.ru

Наш адрес:
456110, Челябинская область,
г. Катав-Ивановск, ул. Дм.Тараканова, 32

**Памятка разработана с использованием материалов сайта https://fincult.info /*