МЧС России

Департамент ГОЧСиПБ г. Москвы

УФСБ по г. Москве и Московской области

ГКУ ЦОДД

РОЦИТ

Корпорация «Российский учебник»

УЧЕБНЫЙ МАТЕРИАЛ по теме «ЦИФРОВАЯ ГРАМОТНОСТЬ И ШОПИНГ В ИНТЕРНЕТЕ»

УРОКБЕЗОПАСНОСТИ.РФ

СОДЕРЖАНИЕ

1. ЧТО ТАКОЕ БЛОКЧЕЙН

Блокчейн – технологическая инновация, которая в будущем значительно повлияет на развитие финансовых услуг, бизнеса и промышленности. Разбираемся, что это такое.

Дословно ***блокчейн*** означает «цепочка блоков». Блок транзакций – это специальная структура для записи нескольких транзакций в системе. Чтобы транзакция считалась достоверной («подтверждённой»), она проверяется и записывается в блок. Каждый блок всегда содержит информацию о предыдущем. Первая транзакция в блоке – получение комиссии за созданный блок, потом идут все остальные.

Все блоки можно выстроить в цепочку, которая содержит данные обо всех когда-либо совершённых с ними операциях. Информацию в блоках можно быстро перепроверить, а для записи данных в новый блок понадобится подтверждение всех участников транзакции.

Понятие ввёл в 2008 году Сатоши Накамото, создатель цифровой валюты – биткоинов, где блокчейн служит публичной «бухгалтерской книгой», в которой записаны все финансовые операции цепочки. То есть он полностью прозрачен: каждый может просматривать (но не редактировать!) все транзакции цепи.

Блокчейн может выполнять проверку идентичности для предотвращения мошенничества и фиксировать законные сделки быстрее и точнее, чем сейчас это делает банк.

ВАЖНО! Блокчейн выполняет функцию, которую при традиционном переводе несёт банк: подтверждает финансовую ценность информации и позволяет установить доверие.

Также блокчейны отлично подходят для записи событий.

Для примера представьте себе электронную медицинскую карту. Для понимания течения болезни и процесса лечения важно, чтобы данные были понятными и неизменными. Каждый блок записей в карте имеет метки («Анализ крови Кузнецовой А.В., 23/04/2016, доктор Фролов»). Изменить запись задним числом нельзя, а доступ к информации можно получить только с

помощью ключа, который нужно запросить у доктора или пациента. То есть данные защищены от посредников и третьих лиц.

А теперь представьте, что врач или пациент дают ключ устройству мониторинга глюкозы в крови, чтобы оно автоматически записывало уровни сахара и в случае необходимости давало команду устройству введения инсулина.

Это называется «умным контрактом»: при наступлении определённых условий наступает определённое действие. Как в нашем примере: уровень глюкозы упал – сработало устройство впрыскивания инсулина.

Сейчас мы используем для обмена информацией интернет, который по сути – децентрализованная онлайн-платформа. Но когда нам нужно передать деньги, мы вынуждены прибегать к посредникам. Даже электронные кошельки, как правило, интегрированы с банковской картой или счётом. Блокчейн-технология, будучи надёжной и прозрачной, поможет устранить любых посредников и повысить эффективность процессов.

2. ЧТО ТАКОЕ БИТКОИНЫ

Биткоин (btc) – новая форма цифровой валюты, которая работает только в интернете. Главное отличие от обычных денег – децентрализация (их вообще никто не контролирует). Эмиссия и транзакции происходят по сложному математическому алгоритму с участием множества компьютеров.

Первым концепцию новой формы денег описал Вей Дай в 1998 году. Он предложил создать цифровую валюту, которая никому не подконтрольна, а эмиссия и транзакции защищены криптографией. Первую реализацию этой красивой киберпанковской идеи в 2009 году опубликовал некий Сатоши Накамото. Он покинул проект в конце 2010 года, а его личность так и не удалось установить. Сейчас над биткоином работает множество разработчиков со всего мира.

С точки зрения обычного пользователя, биткоин – это программа или онлайн-сервис, которые дают доступ к биткоин-кошельку. Он очень похож на обычный электронный кошелек, только вместо привычных нам рублей, долларов и евро в нём лежат биткоины. Их можно тратить на товары, услуги и переводить другим пользователям. Как и обычные деньги, биткоины торгуются на бирже. Курс меняется очень быстро. При желании можно обменять биткоины на обычные валюты с помощью онлайн-обменника.

ЛЮБОПЫТНО! Биткоин может до бесконечности делиться на более мелкие части. Единица в 0.00000001 btc называется 1 сатоши (в честь создателя).

Процесс добычи биткоинов называется **майнингом** (с англ. mining – добыча), а тот, кто ведёт процесс, – **майнером**. Раньше стать им было просто: достаточно запустить у себя на компьютере специальный скрипт, исходный код которого есть в свободном доступе в интернете. Теперь вычислительных мощностей обычной машины может быть уже недостаточно, а на обсчёт цепочки транзакций тратится довольно много времени.

Главные достоинства биткоинов:

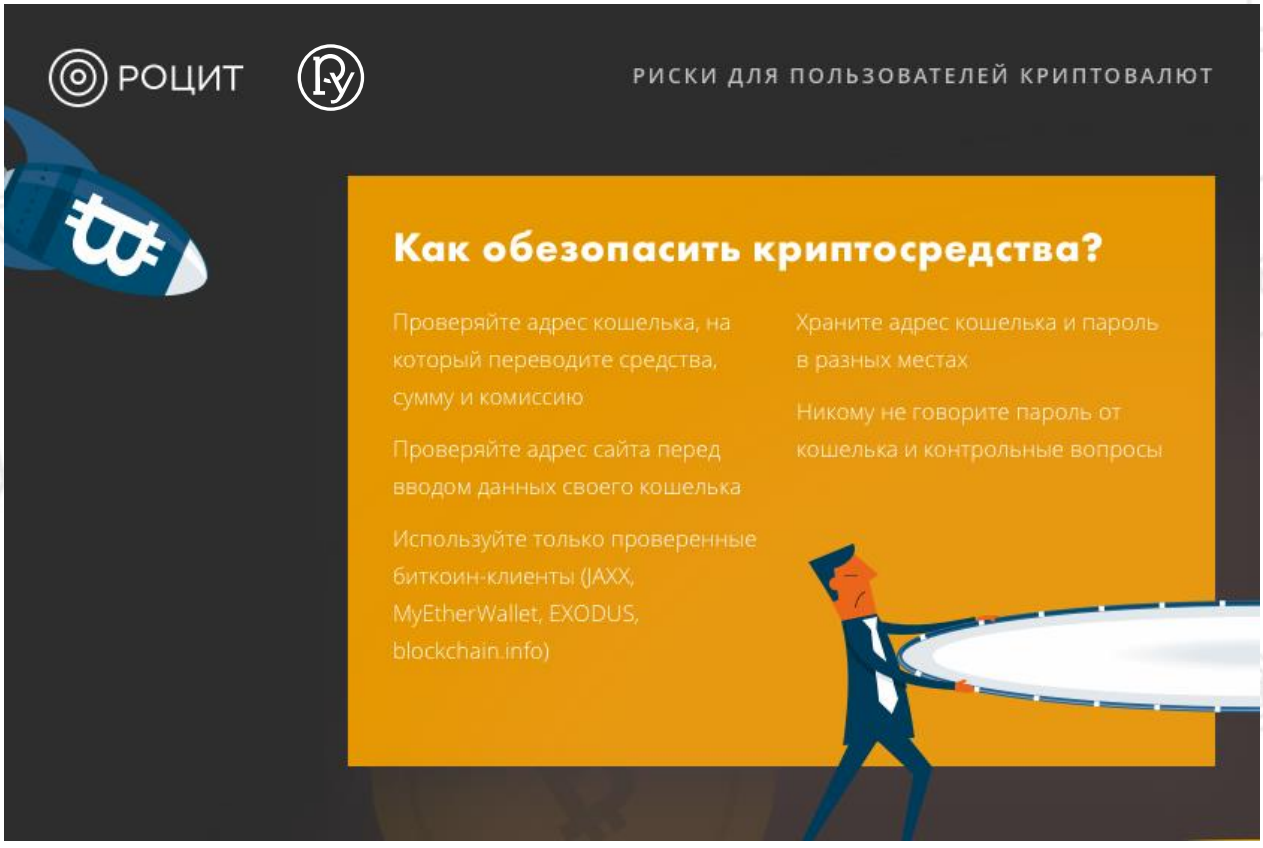
- скорость,
- анонимность,
- прозрачность расчётов.

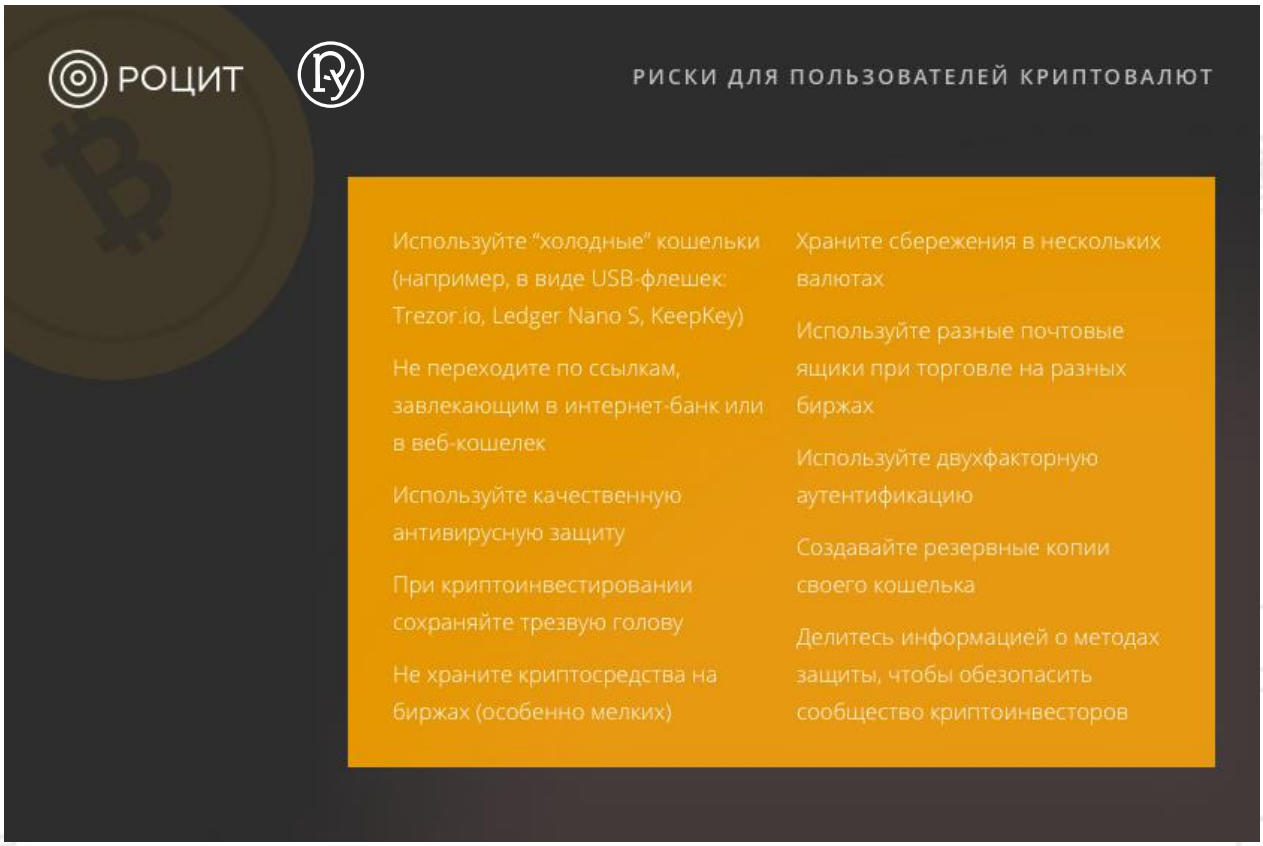
Можно создать любое количество биткоин-кошельков без привязки к кон-

кретному пользователю. Для максимальной анонимности для каждой новой сделки создают новый биткоин-кошелёк.

Тем не менее вся история транзакций прозрачна. Она сохраняется в так называемых блокчейнах, где любой желающий может посмотреть, сколько биткоинов у вас на счету и какие операции вы совершали. Но узнать, кому принадлежит счёт, нельзя (если вы сами не решите это указать).

Платежи происходят достаточно быстро, а совершать их проще простого. Всё, что нужно, – установить на устройство программу-кошелёк, ввести адрес получателя, сумму платежа и нажать «Отправить».

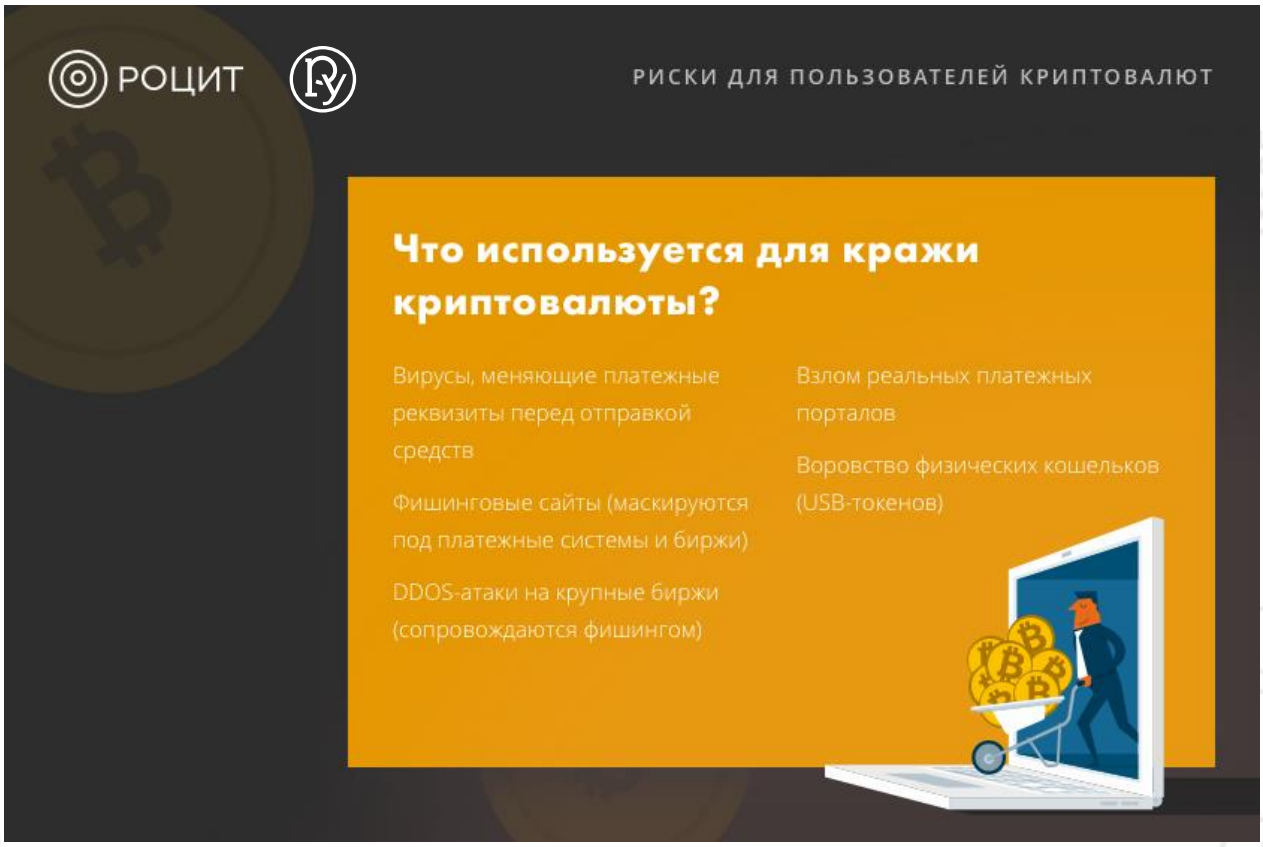




Главная уязвимость криптовалюты – ошибки пользователей, которые могут случайно удалить или потерять критично важные файлы биткоин-кошелька.

Сегодня биткоин – это децентрализованная вычислительная сеть, которая в восемь раз мощнее суммарной производительности всех суперкомпьютеров в мире. Чтобы попробовать получить над ней контроль, понадобятся гигантские вложения времени, сил и сотни миллионов долларов.

Впрочем, случаи взлома биткоин-бирж были. Один из самых нашумевших – взлом японской биткоин-биржи Mt.Gox, которая до конца 2013 года лидировала по объёму транзакций во всём мире. В начале 2014 года стало известно, что за несколько предыдущих лет с Mt.Gox было украдено биткоинов более чем на 460 млн долларов США.



В России запрещён оборот фиатных денег (коими и являются биткоины). Но, поскольку чётких законов нет, запрет просто игнорируют. ***Биткоин-сайты и обменные биржи регулярно вносят в реестр запрещённых по решению суда.***

В Японии биткоины признаны легальным платёжным средством с налогом на покупку. ***Целый ряд компаний по всему миру принимает биткоины наряду с обычными валютами.***

Повсеместное распространение биткоинов не очень удобно государству. Поскольку криптовалюта по своей сути анонимна и децентрализована, её можно использовать для противоправных сделок: отмывания денег, покупки оружия и наркотиков, финансирования терроризма.

3. ПОКУПАЕМ В ИНТЕРНЕТЕ: БЕЗОПАСНО И ПРОСТО

Покупать онлайн удобно. Цены в интернет-магазинах часто ниже, а выбор больше. Не надо тратить время и силы на дорогу и общение с консультантами, можно внимательно изучить товар и сравнить стоимость у нескольких продавцов, есть время обдумать и решить, нужна ли вам эта покупка.

Недостатки у интернет-шопинга тоже есть. Во-первых, вас могут обмануть мошенники. Во-вторых, реальный товар может оказаться гораздо хуже, чем его виртуальный светлый образ.

Какие бывают онлайн-покупки?

Купить онлайн можно не только товары (гаджеты, продукты, цветы), но и услуги (например, вы можете заказать поездку на такси и оплатить её онлайн, а не наличными водителю, купить абонемент на какой-нибудь квест или бьюти-процедуры, онлайн-курс или музыкальный трек).

Сегодня существует множество площадок, где вы можете совершить покупки, среди них есть ***ключевые***.

Интернет-магазины. Покупки в интернет-магазинах очень похожи на покупки в реальных магазинах, только происходят на специализированном сайте. Вы можете открыть сайт магазина в своём браузере или сделать заказ через мобильное приложение: сформировать заказ на покупку, выбрать способ оплаты и доставки заказа, оплатить заказ.

Социальные сети. Многие интернет-магазины заводят свои аккаунты ещё и в социальных сетях, чтобы привлекать больше покупателей и получать их отзывы. Однако к этой площадке нужно относиться с особенной осторожностью. Очень часто в социальных сетях за красивыми фото могут скрываться мошенники, которые просят перевести деньги на личную карту, а товар потом так и не доставляют, потому что его у них на самом деле нет.

Сайты объявлений. Как правило, на таких площадках торгуют частные продавцы, продающие штучный товар. Но и полноценные интернет-магазины тоже часто имеют там представительства.

Магазины игр и приложений. Сегодня далеко не все мобильные приложения бесплатные. Чтобы установить, их нужно оплатить через свой аккаунт.

Игры и приложения. Платными бывают не только мобильные приложения, но и отдельный функционал внутри них. Например, какие-то определённые

фильтры в фоторедакторе продаются отдельно либо какие-то игровые атрибуты (например, жизни в онлайн-игре).

Виды обмана в интернет-магазинах

Не доставить покупку. Некоторые интернет-магазины работают по полной предоплате. Иногда после этого вы можете получить некачественный товар или вовсе не увидеть свою покупку.

Привезти заведомо неисправный товар. Часто курьер торопится, поэтому вы не можете внимательно осмотреть приобретение. А когда позже обнаруживаете, что товар бракованный, вам отказываются его менять под предлогом, что вы сами испортили вещь.

Подписать на спам. Недобросовестные онлайн-продавцы требуют указать не только номер телефона для связи, но и другую личную информацию, которая к покупке никак не относится. А потом подпишут вас на спам и рекламные звонки.

Фишинговый сайт. Некоторые сайты лишь маскируются под интернет-магазин. На самом деле всё, что им нужно, – выманить данные вашей банковской карты вместе с секретным кодом, чтобы украсть ваши сбережения.

Нелегальные товары. Некоторые товары, которые продаются в иностранных интернет-магазинах, в России могут быть запрещены, например Google Glass или ручка со встроенным диктофоном. Поэтому будьте внимательны, прежде чем покупать то, что у нас вообще не продаётся. Возможно, это не случайно.

На что следует обратить внимание

На адресную строку браузера. Страницы ввода конфиденциальных данных любого серьёзного сервиса всегда защищены, а данные передаются в зашифрованном виде. Адрес сайта должен начинаться с «https://», рядом с которым нарисован закрытый замок зелёного цвета.

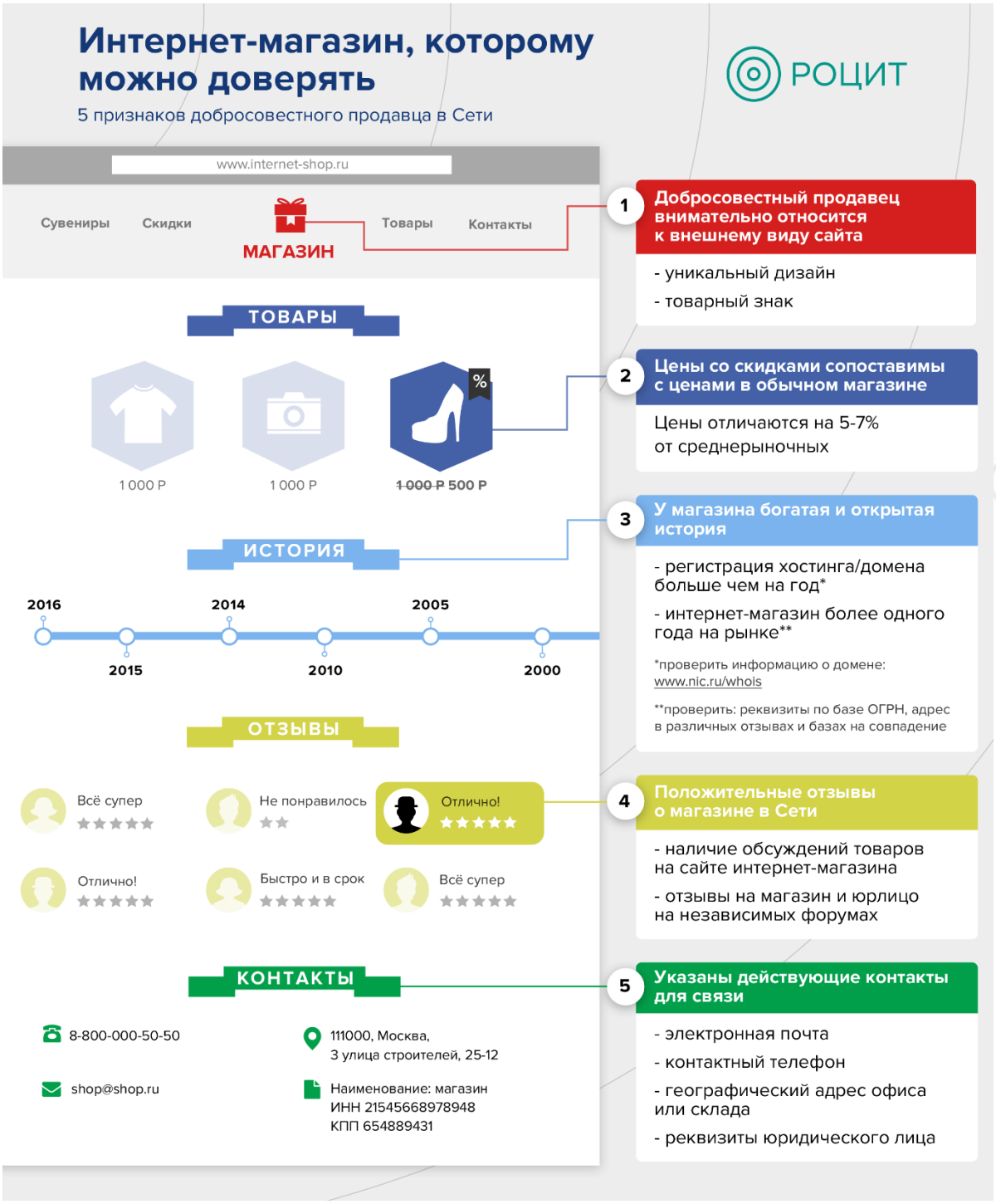
На отзывы покупателей. Всегда читайте отзывы о магазине, в котором хотите сделать покупку. На «Яндекс.Маркете» можно посмотреть рейтинг торговой площадки. А крупные зарубежные интернет-магазины (например, Amazon и eBay) настолько дорожат своей репутацией, что у них даже есть собственные программы защиты покупателей, по которым можно вернуть деньги, если посылка, например, потеряется.

На наличие чека. Без чека вы точно не сможете обменять бракованный товар или вернуть деньги.

Что вы сообщаете о себе. Для курьера достаточно адреса, имени и номера телефона для связи. Некоторые службы доставки (например, Boxberry) требуют обязательно вводить паспортные данные. Без этого вы не сможете завершить оформление заказа, да и получать посылку нужно только лично с паспортом.

На фотографии товара. Чаще всего магазины сами делают фотосессии, чтобы показать товар с наилучшей стороны. Украденные на других ресурсах изображения – повод насторожиться.

На слишком низкую цену. Не спешите радоваться, что нашли смартфон последней модели по цене в два раза ниже рыночной стоимости. Скорее всего, товар проблемный: поддельный, с дефектами или даже краденый. А ещё невероятно низкая цена – любимая уловка мошенников, и вас просто заманивают, чтобы потом обмануть.



Цифровая грамотность населения зависит от каждого пользователя Рунета.
Интернет может быть безопасным, достаточно соблюдать правила по использованию персональных данных и внимательно относиться к покупкам в Сети.

При возникновении проблем, связанных с покупками в Интернете, обращайтесь на Горячую линию Рунета hotline.rocit.ru

Горячая линия

Дополнительные меры защиты

Внимательно читайте условия. Обязательно прочтите об условиях обмена и возврата товара, уточните, какие подтверждающие покупку документы вам выдадут. Проверьте, указаны ли контакты для связи. Чем больше информации о себе предоставляет торговая площадка, тем она надёжнее.

Избегайте предоплаты. По возможности оплачивайте товар курьеру при получении и только после того, как проверите покупку. Если предоплата – обязательное условие торговой площадки, пользуйтесь проверенными платёжными системами с программой защиты покупателей (например, PayPal) или заведите специальную виртуальную карту для онлайн-шопинга.

ПОЛЕЗНО! Виртуальная банковская карта выдаётся специально для покупок и платежей онлайн. Часто она даже не имеет материального носителя: банк сообщает вам только номер, срок действия и код проверки подлинности карты (CVC2/CVV2). Бывает в пластике, но оплачивать покупки офлайн и снимать наличные с её помощью нельзя.

Тщательно проверяйте покупку при получении от курьера магазина или логистической компании. Никогда не подписывайте акт получения товара или накладную, не проверив товар. Даже если курьер утверждает, что очень спешит, распечатайте и проверьте своё приобретение в его присутствии. Это ваше законное право. Если вы уже поставили подпись, а открыв коробку, увидели, что полученный товар повредился при транспортировке, вы не сможете это доказать.

Проверьте интернет-страницу. По ссылке http://www.tcinet.ru/whois/ можно узнать, когда был создан сайт и на кого он зарегистрирован. Домен, зарегистрированный давно и на собственное юрлицо торговой площадки, – хороший знак. А вот злоумышленники обычно создают страницы-однодневки, которые очень быстро закрывают.

Изучите гарантийные условия и таможенные правила. Покупаете технику в зарубежном интернет-магазине? Обязательно изучите условия её гарантийного обслуживания у нас в стране: есть ли официальные мастерские, какие документы вам потребуются, чтобы обратиться туда, можно ли при необходимости обменять товар в России. При этом гарантийные условия стоит проверять и при покупке в отечественном интернет-магазине.

Дорогостоящие товары могут облагаться таможенной пошлиной. Обязательно уточните этот вопрос перед покупкой. Иногда таможенный сбор сильно увеличивает цену приобретения.

Онлайн-аукционы, доски объявлений и социальные сети

Как правило, на таких площадках торгуют частные продавцы, продающие штучный товар. Но и полноценные интернет-магазины тоже часто имеют там представительства.

Шопинг на подобных сайтах может быть вполне безопасен, особенно с программой защиты покупателей – такая точно есть у eBay.

Виды опасностей на сайтах объявлений и в социальных сетях

На этих площадках ***актуальны все опасности***, которые встречаются в интернет-магазинах, но есть и ***специфические.***

Перевод денег на карту физического лица. Поскольку, помимо официально оформленных магазинов, в социальных сетях и на сайтах объявлений свои товары продают частные лица, то есть обычные люди, бизнес которых официально не зарегистрирован, никогда не спешите, когда планируете такую покупку. Не стоит гнаться за красивыми фото и низкой ценой и сразу переводить полную сумму покупки на карту продавца. Изучите отзывы на этого продавца и при возможности договоритесь об оплате товара при получении. Или же проведите оплату через платёжную систему сайта объявлений.

Интересная и манящая, но нечестная реклама. Речь идёт не только о рекламных баннерах с активной ссылкой сразу на оформление заказа, но и о проплаченной рекламе недобросовестных блогеров. Даже если кто-то известный в социальной сети рекламирует что-то, не стоит этому слепо и безоговорочно верить. Проведите своё маленькое исследование: изучите товар на сайте производителя, ответьте себе на вопрос, точно ли он вам нужен и подходит ли он вам.

Псевдоуникальный товар и завышенная цена. Иногда частные продавцы завышают ценность своего товара, отмечая, что он уникален и продаётся только у них. Если вы наткнулись на такое описание, включите своё критическое мышление. Как и в прошлом примере, обратитесь за помощью к возможностям интернета. Можете сохранить фото товара, загрузить его в один из поисковых сервисов и попробовать найти похожие изображения. Может оказаться, что этот товар не такой уж и уникальный, возможно, где-то его можно купить значительно дешевле.

РОЦИТ

МОШЕННИЧЕСТВО НА ДОСКАХ ОБЪЯВЛЕНИЙ

Чего хотят мошенники?

Получить доступ к вашей банковской карте, банковскому счету

Получить от вас предоплату или залог и ничего не продать

Заставить вас позвонить на платный номер

Отправить не тот товар, который вы купили, или поддельный товар

Заставить вас оплатить покупку через терминал (Qiwi), чтобы вы не смогли вернуть деньги в случае мошенничества

Заставить вас снять жилье, которое принадлежит не им

Заставить вас подписаться на платные смс-рассылки или подать платную анкету

РОЦИТ

МОШЕННИЧЕСТВО НА ДОСКАХ ОБЪЯВЛЕНИЙ

Как защититься от мошенников?

Общие советы

Не сообщайте незнакомому лицу паспортные данные

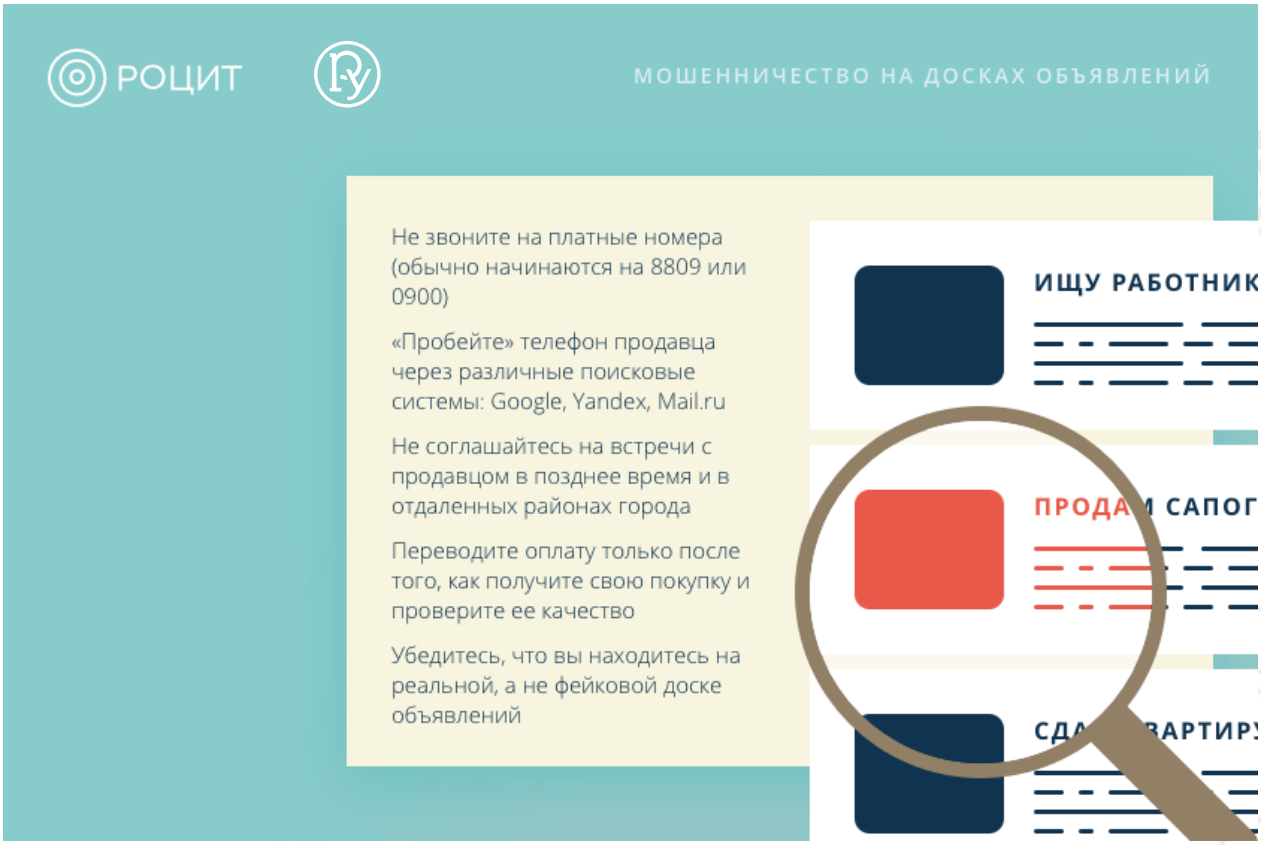
Никому не говорите CVC-код (3 цифры с обратной стороны) с вашей карты

Не говорите никому пароли, которые приходят на ваш телефон в виде СМС

Не вводите в банкомат никакие данные, полученные от других людей

Не торопитесь при совершении сделки

Записывайте все телефонные разговоры и номера продавцов/ покупателей



Виды опасностей в магазинах игр и приложений, а также внутри игр и приложений

Вредоносные приложения. Через вредоносное приложение злоумышленники могут воровать денежные средства и личную информацию с устройства. В большинстве случаев вредоносное ПО попадает на устройство из альтернативных источников, поэтому очень важно совершать покупки только в официальных магазинах приложений.

Платные подписки. Приложение может подписать вас на услугу с ежемесячной оплатой, при этом подписка не будет отменена, если вы перестанете пользоваться приложением или удалите его. Платные подписки нужно отменять вручную.

Специальные предложения в приложениях. Если приложение обещает вам бонусы за отправку СМС-сообщений на короткий номер или звонок на платный номер телефона, ни в коем случае не отправляйте СМС и не звоните, удалите это приложение.

Советы по безопасному пользованию мобильными приложениями и подписками

Устанавливайте только проверенные приложения и из надёжных источников.

Не платите дважды. Вы купили новый телефон и хотите перенести на него приложение, приобретённое в официальном магазине и установленное на старом телефоне с такой же операционной системой. Вам не нужно ещё раз покупать это приложение, так как оно уже привязано к вашей учётной записи внутри магазина. Для бесплатной загрузки достаточно использовать ту же учётную запись в магазине приложений.

Следите за тем, какие разрешения просит приложение при установке. Если приложение запрашивает доступ к вашей телефонной книге, функции отправки СМС или совершения звонков, будьте осторожны. Такое приложение может без вашего ведома отправлять СМС на платные номера и тратить ваши деньги.

Аккуратнее с платными подписками. Если вы скачали платное приложение с бесплатным пробным периодом, а потом поняли, что оно вам не подходит и вы не будете им больше пользоваться, отмените подписку на приложение в магазине. Это можно сделать в настройках вашей учётной записи. В противном случае по истечении бесплатного периода с вашей банковской карты будут списаны деньги.

4. ОНЛАЙН-ПЛАТЕЖИ: ОСНОВНЫЕ ПОНЯТИЯ

Электронные деньги работают так же, как и обычные наличные, – ими можно оплатить товар или услугу. Разница в том, что они лежат на электронном носителе: банковской карте, счету электронной платёжной системы или в электронном кошельке.

Банковская карта – пластиковая карта, которая привязана к одному или нескольким расчётным счетам в банке. Ей можно оплачивать товары и услуги, в том числе онлайн, и снимать наличные деньги в банкоматах и операционных кассах. По сути, это физический символ вашего банковского счёта, который можно потрогать и предъявить.

С **дебетовой** карты можно потратить только то, что есть у вас на счету. А вот израсходованные с **кредитной** карты средства вы автоматически берёте у банка в кредит и обязаны вернуть с процентами.

ВАЖНО! Если у вас украли деньги с карточки, сразу же позвоните в банк, чтобы сообщить об этом и заблокировать карту.

По закону (№ 161-ФЗ, статья 9) обратиться с заявлением о несанкционированном списании нужно сразу же, как только это произошло, максимум на следующий день после получения уведомления о совершённой операции. Если опоздаете, банк не будет нести никакой ответственности за ваши пропавшие средства.

Виртуальная банковская карта выдаётся специально для покупок и платежей онлайн. Часто она даже не имеет материального носителя: банк сообщает вам только номер, срок действия и код проверки подлинности карты (CVC2/CVV2). Бывает в пластике, но оплачивать покупки офлайн и снимать наличные с её помощью нельзя.

Мобильный и интернет-банкинг – услуга, которая позволяет клиенту банка совершать операции по собственным счетам с мобильного устройства или через браузер на специальном сайте. Необходимо иметь доступ в интернет и знать логин и пароль для входа в личный кабинет.

Электронный кошелёк – это специальная программа или интернет-сервис, с помощью которых можно хранить электронные деньги и платить ими. По сути, это аналог банковского счёта. Самые известные: «Яндекс.Деньги» и кошелёк платёжной системы QIWI. Бывают и в виде физических носителей: карта московского метро «Тройка» и сим-карта сотового оператора – это тоже электронные кошельки. Пополнять их можно через терминалы, с банковской карты или со счёта мобильного телефона. Напрямую снять деньги с такого кошелька нельзя. Придётся сначала перевести их на банковскую карту и дойти до банкомата.

Электронная платёжная система – это система расчётов через интернет. Самые известные – WebMoney и PayPal. Чтобы использовать такую систему, и отправитель, и получатель денег должны быть в ней зарегистрированы. Переводить деньги можно с электронного кошелька или напрямую с банковской карты. При покупке с рублёвой карты в зарубежном магазине происходит автоматическая конвертация в валюту продавца по собственному курсу платёжной системы. ***Главная задача электронной платёжной системы – гарантия безопасности операции для обеих сторон.*** PayPal, например, возвращает деньги, если покупку не доставили или товар не соответствует описанию.

5. ПЛАТЕЖИ В ИНТЕРНЕТЕ: ПРАВИЛА БЕЗОПАСНОСТИ

Теперь онлайн можно перевести деньги близким, оплатить услуги ЖКХ, сотовую связь, налоги и штрафы, купить одежду, технику, билеты на самолёт или поезд, в кино, на концерт и в театр.

Чтобы онлайн-платежи были не только удобными, но и безопасными, нужно запомнить ***несколько простых правил***.

Где могут обмануть?

На фишинговом сайте. Злоумышленники тщательно подделывают дизайн и адрес веб-страницы, который может отличаться всего одним символом (например, paypa1.com вместо paypal.com). Отличить такой сайт от официального на глаз непросто. Вы либо сразу попадаете на поддельную страницу – клон оригинала, либо переходите по подменной ссылке, которую злоумышленник встраивает в официальный сайт. Кликнув по ней, вы оказываетесь на имитации платёжной страницы, после ввода данных на которой ваши деньги попадут к мошенникам. Сбивает с толку то, что все остальные ссылки на сайте – настоящие.

В фишинговых письмах. Вам присылают письмо от имени вашего банка, популярного интернет-магазина, платёжной системы или социальной сети с просьбой перейти по ссылке изменить свой пароль или ввести номер банковской карты и секретный код подтверждения. Естественно, веб-страница оказывается поддельной.

Фишинг – это вид интернет-мошенничества, цель которого – завладеть логинами, паролями и другой конфиденциальной информацией, чтобы получить доступ к деньгам и аккаунтам пользователя. Чаще всего злоумышленники присылают письмо от имени популярного интернет-магазина, социальной сети или платёжной системы с просьбой перейти по ссылке изменить свой пароль или ввести номер банковской карты и секретный код подтверждения. Ссылка ведёт на подставной сайт, внешне очень похожий на настоящий, поэтому введённые на нём данные моментально попадают к мошенникам.

Подменить платёжные реквизиты получателя. Не у всех хватает терпения проверять длинные номера счетов, особенно если вы скачали квитанцию с вызывающего доверие сайта. Этим с радостью пользуются злоумышленники, которые подделывают платёжные документы. Вы скачиваете поддельную квитанцию (или копируете подставные реквизиты) и переводите деньги со-

всем не туда, куда планировали. Кстати, в офлайне такие фальшивые платёжки тоже встречаются. Будьте бдительны!

На мошеннических сайтах продажи авиабилетов. Как правило, билеты на таких сайтах стоят значительно дешевле, чем на официальных сайтах авиакомпаний. После оплаты вы можете даже получить электронный билет на почту и только на стойке регистрации в аэропорту узнать, что вас обманули.

При краже или потере смартфона. Доступ к вашему смартфону с мобильным банкингом и номером, на который приходят коды подтверждения денежных операций, – самый лёгкий путь завладеть вашими сбережениями.

При взломе электронной почты. Взломанный почтовый ящик даёт мошенникам возможность не только рассылать от вашего имени спам, но и получить доступ к электронным кошелькам и банковским счетам, привязанным к этому адресу. Злоумышленник просто поменяет ваш пароль на свой и подтвердит его по ссылке, которая придёт на почту.

С помощью дубликата сим-карты. Некоторые банки позволяют совершать денежные переводы по СМС. И если злоумышленнику удалось получить дубликат вашей симки, например с помощью сообщника в офисе мобильного оператора или по поддельной доверенности, он легко сможет делать это вместо вас.

На что обратить внимание?

На адресную строку браузера. Страницы ввода конфиденциальных данных любого серьёзного сервиса всегда защищены, а данные передаются в зашифрованном виде. Адрес сайта должен начинаться с «https://», рядом с которым нарисован закрытый замок зелёного цвета.

HTTPS (HyperText Transfer Protocol Secure) – протокол передачи данных с поддержкой шифрования. По умолчанию используется везде, где важно сохранить конфиденциальность личной информации: в электронных платёжных системах, почтовых клиентах, интернет-банкинге и даже в социальных сетях. Специально настраивать https не нужно, он включается автоматически и поддерживается всеми современными браузерами.

На необычное поведение вашего банка или платёжной системы. Если вас просят ввести новые данные, которые раньше не запрашивали, отмените операцию и позвоните в службу поддержки банка.

На адрес сайта. Если адрес страницы отличается хотя бы на один символ (например, paypa1.com вместо paypal.com), введите его вручную самостоятельно или перейдите по ссылке из поисковика.

На стиль электронного письма. Письма серьёзных компаний должны быть написаны без орфографических и грамматических ошибок.

Ваш банк или платёжная система знают, как вас зовут, и в письмах обращаются по имени и фамилии (или имени и отчеству). Обезличенное приветствие в духе «Уважаемый пользователь» или обращение по адресу электронной почты – знак того, что письмо, скорее всего, отправили мошенники.

Призывы к безотлагательным действиям («Немедленно оплатите задолженность!», «Срочно смените пароль!») означают, что вас хотят заставить действовать быстро и необдуманно.

На внезапный сбой в работе сим-карты. Появилась надпись «Вставьте сим-карту»? Срочно зайдите в ближайший офис вашего мобильного оператора или позвоните ему с другого телефона и выясните, в чём проблема. Возможно, кто-то получил дубликат вашей симки и её нужно срочно заблокировать.

Что ещё можно сделать?

Тщательно проверьте платёжные реквизиты. Сверьте их с тем, что видите на экране. А если платите этому получателю уже не первый раз, но впервые –

онлайн, возьмите старую бумажную квитанцию и проверьте реквизиты по ней.

Проверьте адрес с помощью интернет-браузера. Наведите курсор на кнопку сайта или ссылку в левом углу адресной строки. Если адрес, который показывают по клику, не совпадает с указанным в адресной строке – закрывайте страницу.

Не переходите по ссылкам из письма. Наберите адрес самостоятельно или перейдите по ссылке из поисковика. К примеру, «Яндекс» точно знает официальные адреса сайтов крупных банков и сервисов и умеет предупреждать о подозрительных страницах. Смело звоните в банк и уточняйте, правда ли вам нужно сделать то, о чём просят в письме.

Подключите услугу СМС-оповещения. Если деньги внезапно начнут утекать с вашего счёта, вы сможете быстро заблокировать карту.

Не доверяйте неизвестным сайтам. Не вводите данные банковской карты на неизвестных веб-ресурсах и не переводите денег незнакомым получателям. Солидный интернет-сервис всегда переадресует вас на сайт вашего банка или платёжной системы.

Проверьте интернет-страницу. По ссылке http://www.tcinet.ru/whois/ можно узнать, когда был создан сайт. Злоумышленники обычно создают страницы-однодневки, которые очень быстро закрывают.

Установите лицензионный антивирус. Не только на компьютер, но и на смартфон. Многие из них блокируют не только вредоносное ПО, но и ссылки на фишинговые сайты. Если у вас MacOS/iOS – можете не беспокоиться.

Проверяйте сайты продажи авиабилетов. Поищите адрес страницы и телефон службы поддержки в поисковике, почитайте отзывы других пользователей. Зайдите на настоящийбилет.рф и удостоверьтесь в подлинности ресурса.

Блокируйте карты и симки. Потеряли телефон, к которому привязана банковская карта? Срочно блокируйте и симку, и карту. Её всегда можно разблокировать позже, а деньги будут целее.

Используйте сложные пароли. Никогда не используйте простые пароли (qwerty12345). Для каждого сервиса придумайте уникальный пароль и регулярно их меняйте.

РОЦИТ

УГРОЗЫ ПРИ ПРОВЕДЕНИИ ИНТЕРНЕТ-ПЛАТЕЖЕЙ

Как защитить свои деньги при проведении интернет-платежей?

Подключите интернет-банк и СМС-оповещение

Используйте только защищенные сайты:

Адрес начинается с https://

Иконка в виде закрытого замка возле адресной строки

Используйте 3D Secure — авторизацию платежа по СМС

Ищите на сайте надпись «Verified by Visa» или «MasterCard Securecode «

РОЦИТ

УГРОЗЫ ПРИ ПРОВЕДЕНИИ ИНТЕРНЕТ-ПЛАТЕЖЕЙ

Откройте отдельную карту для интернет-платежей

Не используйте для оплаты карты с большим кредитным лимитом

Никогда не сообщайте данные своей банковской карты другим людям

Ознакомьтесь с правилами предъявления претензий по мошенническим платежам

Если интернет-магазин вызывает подозрение, используйте платежные системы (Apple Pay, PayPal и др.)

Совершайте покупки с устройств, на которых установлена антивирусная защита

6. ПРАВИЛА БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ ПЛАСТИКОВЫХ КАРТ

Чтобы обезопасить свои сбережения, нужно следовать нескольким ***простым*** *и* ***эффективным правилам*** и уметь ***правильно выбирать банкомат.***

- Никогда и никому не сообщайте ПИН-код вашей карты. Если не можете запомнить установленный банком, смените его на тот, который вам легче выучить.
- Ни в коем случае не записывайте ПИН-код, тем более на саму карту или листок, который носите в кошельке.
- Никому не позволяйте пользоваться вашей пластиковой картой.
- В магазинах и общепитах деньги с карты должны снимать в вашем присутствии. Не позволяйте уносить её в подсобные помещения, лучше пройдитесь до кассы вместе с продавцом/официантом.
- Никому не сообщайте реквизиты карты и ПИН-код.
- В любой непонятной ситуации звоните в свой банк по телефону, указанному на вашей карте, и сообщите о поступившем звонке или письме.
- Потеряли карту? Срочно свяжитесь с банком и заблокируйте её.

ВАЖНО! Запомните: серьёзные организации никогда не присылают писем и не звонят с просьбой сообщить конфиденциальные данные! Если вы получили письмо или звонок якобы из банка, не переходите по присланным ссылкам, они ведут на подставные сайты.

- Пользуйтесь только теми банкоматами, которые расположены в безопасных местах, оборудованы системой видеонаблюдения и охраной (в государственных учреждениях, банках, крупных торговых центрах и т.д.).
- Изучите картоприёмник и клавиатуру банкомата. Обнаружили накладки, странные устройства, светящиеся маячки и т.п. – не вставляйте карту. Нелишним будет также сообщить об этом в службу поддержки, телефон которой обычно указан на банкомате.
- Если банкомат слишком зависает, долго находится в режиме ожидания или самостоятельно перезагружается, не пользуйтесь им.
- Не позволяйте никому помогать вам пользоваться банкоматом.

ВАЖНО! Когда снимаете деньги в банкомате, обращайте внимание на находящихся поблизости людей. Они не должны видеть, что именно вы набираете на клавиатуре и видите на экране. Кто-то вызывает подозрения? Найдите другой банкомат или снимите деньги позже.

7. КАК ПОДГОТОВИТЬСЯ К «ЧЁРНОЙ ПЯТНИЦЕ»

«Чёрная пятница» – глобальная осенняя распродажа, во время которой розничные интернет-магазины предлагают товары со скидками 40–90%.

Чтобы выгодно купить необходимое и не пострадать от мошенников, ***нужно следовать инструкции.***

Подготовка

Составьте список покупок. Сначала запишите вещи, которые вам действительно необходимы, а в конец можно добавить всякое баловство. Купите, если останутся деньги.

Определитесь с бюджетом. Установите максимум, который вы готовы потратить на каждую покупку. Пренебрегли советом? Будьте готовы к тому, что финансы иссякнут примерно к середине списка. А вы только вошли во вкус!

Изучите цены. Потратьте день на изучение онлайн-магазинов и выясните, сколько стоят интересующие вас товары (помним про список!). Сравните цены на разных площадках и добавьте в закладки наиболее выгодные варианты.

Не забудьте промониторить магазины приложений, электронные библиотеки и платные интернет-сервисы.

ВАЖНО! Обязательно обратите внимание на актуальный ценник и сделайте пометки. Так вы сможете избежать покупок с липовой скидкой. Некоторые недобросовестные магазины в дни больших распродаж предварительно меняют ценник на более высокий, а уже потом делают «скидку». В итоге распродажная цена получается практически равна обычной.

Зарегистрируйтесь в нужных интернет-магазинах. Не спеша заполните все необходимые при регистрации поля: Ф. И. О., адрес доставки, контакты. Подтвердите электронный адрес и поменяйте дефолтные пароли на те, которые вам будет легко запомнить.

Почитайте отзывы. По возможности выбирайте крупные и известные торговые площадки (не забываем про https://realblackfriday.ru!). Проверьте, указаны ли контакты для связи: чем больше информации, тем надёжнее.

Нашли нужный товар по хорошей цене, но магазин видите впервые? Не поленитесь погуглить отзывы, чтобы заранее отсеять недобросовестные площадки и сайты мошенников.

Безопасность при покупке

Слишком низкая цена должна насторожить. Даже в «чёрную пятницу» ***цена на смартфон последней модели не может быть в два раза ниже рыночной стоимости***. Скорее всего, товар поддельный, с дефектами или даже краденый. А ещё неправдоподобно низкие цены – любимая уловка мошенников, и вас просто заманивают, чтобы потом обмануть.

Платите безопасно. Платёжные страницы и страницы ввода конфиденциальных данных любого серьёзного сервиса всегда защищены, а информация передаётся в зашифрованном виде. Адрес сайта должен начинаться с «https://», рядом с которым нарисован закрытый замок зелёного цвета. Если страница не защищена, лучше не рисковать, какой бы привлекательной ни была скидка.

Уточните про чек. Интернет-магазины обязаны приложить к посылке накладную с указанием количества и цены товаров, печатью и подписью. Без неё вы точно не сможете обменять товар или вернуть деньги.

Минимум личной информации. Для курьера достаточно адреса, имени и номера телефона. Некоторые службы доставки (например, Boxberry) требуют обязательно вводить паспортные данные. Без этого вы не сможете завершить оформление заказа, да и получать посылку нужно только лично с паспортом.

Избегайте предоплаты. По возможности оплачивайте товар курьеру при получении и только после того, как проверите покупку. Если предоплата обязательна, ***пользуйтесь проверенными платёжными системами с программой защиты покупателей*** (например, PayPal) или заведите ***специальную виртуальную карту*** для онлайн-шопинга.

Тщательно проверяйте покупку перед оплатой. Даже если курьер утверждает, что очень спешит, распакуйте и проверьте товар в его присутствии. Это ваше законное право.

Проверьте интернет-страницу. По ссылке http://www.tcinet.ru/whois/ можно узнать, когда был создан сайт и на кого он зарегистрирован. Домен,

зарегистрированный давно и на собственное юрлицо торговой площадки, – хороший знак. А вот злоумышленники обычно создают страницы-однодневки, которые очень быстро закрывают.

Доставка

Выбирайте обычную доставку. Откажитесь от соблазна оплатить экспресс-доставку: её цена может свести всю выгоду от скидок на нет.

Продумайте логистику. Если вы ходите в офис, лучше заказать доставку на работу. Часто уезжаете по делам в течение дня? Постаматы – ваш выбор!

Наберитесь терпения. Службы доставки после глобальных распродаж всегда перегружены, поэтому посылки могут сильно задерживаться. Просто расслабьтесь и ждите.

8. КАК ПРАВИЛЬНО ПОКУПАТЬ В КИТАЙСКИХ ИНТЕРНЕТ-МАГАЗИНАХ

Китайские интернет-магазины пользуются спросом. Aliexpress ещё в 2014 году стал самой популярной торговой площадкой России, а в 2015-м на отечественный рынок вышел JD.com. Цены в этих магазинах низкие, регулярно случаются распродажи, выбор огромный. Но есть и недостатки: иногда могут прислать вещь, которая не соответствует описанию или бракованная. А то и вовсе приезжает пустая коробка. Чтобы шопинг приносил радость, ***следуйте простым правилам.***

Внимательно читайте отзывы о продавце и товаре. Даже если приобретаете какую-то мелочь за 100 рублей, помните о том, что вы тратите на покупку не только деньги, но и время. Поэтому лучше уделить немного времени чтению отзывов, чем получить совсем не то, что вы покупали.

Большинство описаний товаров криво переведены с китайского, поэтому сразу определить, что такое «дамы натуральной вязки ёилет кролика кистями енот меховой» нелегко. Но кто-то наверняка уже рискнул заказать это чудо и написал об этом отзывы. Нередко там можно встретить фотографии, по которым есть шанс оценить реальный внешний вид и качество товара. Бывает, они ощутимо отличаются от витринных.

Сортируйте лоты по рейтингу, чтобы лучшие оказались в начале списка. Правда, это не даёт 100%-й гарантии, что товар будет хорош: недобросовестные продавцы иногда накручивают себе рейтинг.

Подумайте над вариантами поискового запроса. Чтобы найти вещь по самой выгодной цене, попробуйте ввести несколько разных запросов. Проявите фантазию! Цена на один и тот же лот в крупном магазине может значительно разниться от продавца к продавцу.

Будьте внимательны с размерами. Китайские размеры отличаются от российских, европейских и американских: они безбожно маломерят. Поэтому всегда изучайте размерные таблицы внизу страницы с описанием товара. Впрочем, они тоже могут подвести. Не поленитесь написать продавцу и попросить сделать замеры вещи.

Платите через PayPal. На Aliexpress нужно обязательно регистрироваться в их платёжной системе AliPay, а на JD можно оплачивать банковской картой, QIWI, «Яндекс.Деньгами» или PayPal. Лучше всего выбрать последний, у него есть программа защиты покупателей. В случае возникновения проблем вы сможете открыть диспут и вернуть деньги.

СОВЕТ! Не заказывайте во время праздников сани и купальник лучше готовить в межсезонье. Подарком на Новый год или День святого Валентина надо озаботиться уже в октябре. Во многих странах пик шопинговой активности из-за католического Рождества приходится на ноябрь и декабрь.

Помните об особенностях заказа в праздники. 11 ноября в Китае отмечают День холостяка, а в стране проходят распродажи. В последнюю пятницу ноября случается «чёрная пятница». Поэтому покупка, сделанная после 11 ноября, может приехать только в следующем году. В феврале вся страна уходит на двухнедельные каникулы в честь китайского Нового года.

Следите, чтобы товар отправили. Часто бывает, что вещи нет на складе, но продавец об этом умалчивает. Поэтому, если вы хотите получить свою посылку к определённому времени, обязательно проследите, чтобы её отправили в течение четырёх дней с момента оплаты заказа. Если этого не случилось, свяжитесь со службой поддержки и выясните причину задержки.

Обратите внимание на вес посылки, указанный в данных об отправке. Если он подозрительно маленький, а вы купили, например, смартфон, напишите продавцу и уточните, не перепутал ли он чего-нибудь. Бывали случаи, что покупателям гаджетов приходила пустая коробка с инструкцией.

Проверяйте посылки сразу. Проверяйте посылку, как только получите её: прямо на почте или при курьере. Если вам пришлют что-то не то или вещь окажется с браком, у вас будут свидетели. Товар могли повредить или потерять в пути. Зафиксируйте все проблемы и предъявите претензию магазину.

Требуйте замену или возврат. Если товар приехал не полностью, не соответствует описанию или был испорчен, смело пишите продавцу, выбрав под товаром опцию «Открыть спор». Выберите причину и не забудьте приложить фото дефекта. Обычно торговцы заботятся о рейтинге и идут навстречу покупателю, предлагая выслать новую вещь или вернуть деньги. Если не удалось договориться с продавцом напрямую, обратитесь в службу поддержки торговой площадки.

9. БАНКОВСКИЕ КАРТЫ ДЛЯ ПОКУПОК В ИНТЕРНЕТЕ

Узнаем, какими способами можно оплачивать покупки в интернете и как правильно выбрать карту для онлайн-шопинга.

Какую карту выбрать. Для полной уверенности, что карту примут в любом интернет-магазине, ***лучше всего выбрать Visa или MasterCard*** – это самые распространённые международные платёжные системы. Обязательно ***обратите внимание на категорию карты,*** поскольку некоторые зарубежные торговые площадки не работают с самыми базовыми (Visa Electron, MasterCard Maestro и Electronic). А вот в каком банке вы её откроете, особой роли не играет.

Не забудьте узнать, как быстро пополнять карту и можно ли застраховать лежащие на ней средства.

Отдельная карта. Заядлым онлайн-покупателям советуем завести отдельную карту для шопинга в Сети. Попросите свой банк выпустить дополнительную дебетовую карту, на которую будете переводить нужную сумму непосредственно перед покупкой. Так, если её данные будут похищены, ваши основные сбережения не пострадают.

Лучше вообще не хранить крупные суммы денег на карте, которой пользуетесь ежедневно. Получили зарплату? Переведите её на счёт, к которому не привязано вообще никаких карт, а уже с него закидывайте мелкие суммы на основную.

Также стоит подумать о выпуске виртуальной карты. Оформить её можно онлайн.

Виртуальная банковская карта выдаётся специально для покупок и платежей онлайн. Часто она даже не имеет материального носителя: банк сообщает вам только номер, срок действия и код проверки подлинности карты (CVC2/CVV2). Бывает в пластике, но оплачивать покупки офлайн и снимать наличные с её помощью нельзя.

Электронная платёжная система или кошелёк. Некоторые зарубежные продавцы принимают деньги только через электронные платёжные системы (самые известные – WebMoney и PayPal). Это удобно: вы можете переводить деньги с привязанной к кошельку банковской карты, но продавец не увидит её реквизиты. Не забывайте, что, когда вы оплачиваете товар в зарубежном

магазине рублёвой картой, платёжная система автоматически конвертирует сумму в валюту продавца по собственному курсу.

ВАЖНО! Электронная платёжная система гарантирует безопасность сделки для обеих сторон. PayPal, например, возвращает деньги, если покупку не доставили или товар не соответствует описанию.

Техника безопасности

Покупайте только на сайтах с отличной репутацией. Чем дольше существует магазин и чем больше о нём положительных отзывов, тем лучше.

Вводите конфиденциальные данные только на защищённых страницах. Адрес сайта должен начинаться с «https://», рядом с которым нарисован закрытый замок зелёного цвета. Это значит, что данные передаются в зашифрованном виде и надёжно защищены.

Подключите СМС-оповещения. Большинство банков поддерживают технологию верификации 3D-Secure. При совершении операции вам приходит сообщение с кодом подтверждения транзакции, который нужно ввести в специальном окошке на платёжной странице. Поэтому важно сообщать в банк, если у вас украли телефон или вы сменили номер.

ВАЖНО! Если у вас украли деньги с карточки, сразу же позвоните в банк, чтобы сообщить об этом и заблокировать карту.

По закону (№ 161-ФЗ, статья 9) обратиться с заявлением о несанкционированном списании нужно сразу же, как только это произошло, максимум на следующий день после получения уведомления о совершённой операции. Если опоздаете, банк не будет нести никакой ответственности за ваши пропавшие средства.

10. СПИСОК ЛИТЕРАТУРЫ

Учебные материалы Региональной общественной организации «Центр интернет-технологий» (РОЦИТ), 1996–2019.