РОЦИТ

Гид по финансовой грамотности

При поддержке

FinEx
ETF НА МОСКОВСКОЙ БИРЖЕ

При реализации проекта используются средства государственной поддержки, выделенные в качестве гранта в соответствии с распоряжением Президента Российской Федерации от 01.04.2015 №79-рп и на основании конкурса, проведенного Фондом ИСЭПИ

Дорогие друзья!

Цифровая среда, в которой мы все сейчас живем, уже давно стала «средой денег». Интернет- и мобильные сервисы помогают нам быстро решать задачи, связанные с оборотом денег – совершать платежи и делать покупки. Ежедневно миллионы Интернет-пользователей в России совершают множество финансовых операций именно через сервисы во Всемирной Паутине – и в личных целях, и в деловых. К их услугам – десятки тысяч Интернет-магазинов, банковских и платежных сервисов, платных онлайн-услуг.

В этом массиве предложений и функций неподготовленному человеку зачастую тяжело разобраться. Для того, чтобы понять, что именно может тот или иной сервис и как он работает, тоже требуются время и знания. При том в этой «мутной воде» успешно плавают мошенники всех сортов, жаждущие поживиться чужими деньгами – к которым они пытаются добраться благодаря цифровым возможностям. Тем не менее, преимущества цифровых сервисов стали настолько очевидны и настолько упрощают нашу жизнь, что отказываться от них и переходить снова «в оффлайн» уже нет желания – а иногда и возможности, если некую операцию нужно сделать дешево и быстро.

В этой брошюре мы постарались разобрать основные возможности, которые дает нам Интернет в плане совершения покупок, платежей и управления деньгами, и связанные с ними основные угрозы финансовой безопасности пользователей, а также дать простейшие советы по защите от наиболее типичных опасностей, подстерегающих пользователей в финансовом плане при использовании Интернета. Тематика брошюры затрагивает совершение обычных платежей, покупки в Интернет-магазинах, безопасность при использовании мобильных сервисов, семейную финансовую безопасность. Специальное внимание было уделено различным видам Интернет-мошенничеств и вымогательств, которые сопровождают нашу финансовую онлайн-жизнь.

Надеемся, что информация, собранная в этой брошюре, пополнит Ваши знания о цифровой безопасности и поможет Вам более уверенно пользоваться финансовыми сервисами в Интернете, а также позволит избежать различных угроз Вашим деньгам и оставить жуликов «с носом».

Содержание

Электронные деньги 4

Платежи в интернете 8

Интернет-магазины 16

Онлайн-аукционы и Интернет-доски объявлений о продаже товаров 24

Платим за опции и контент 26

Интернет-мошенничество 34

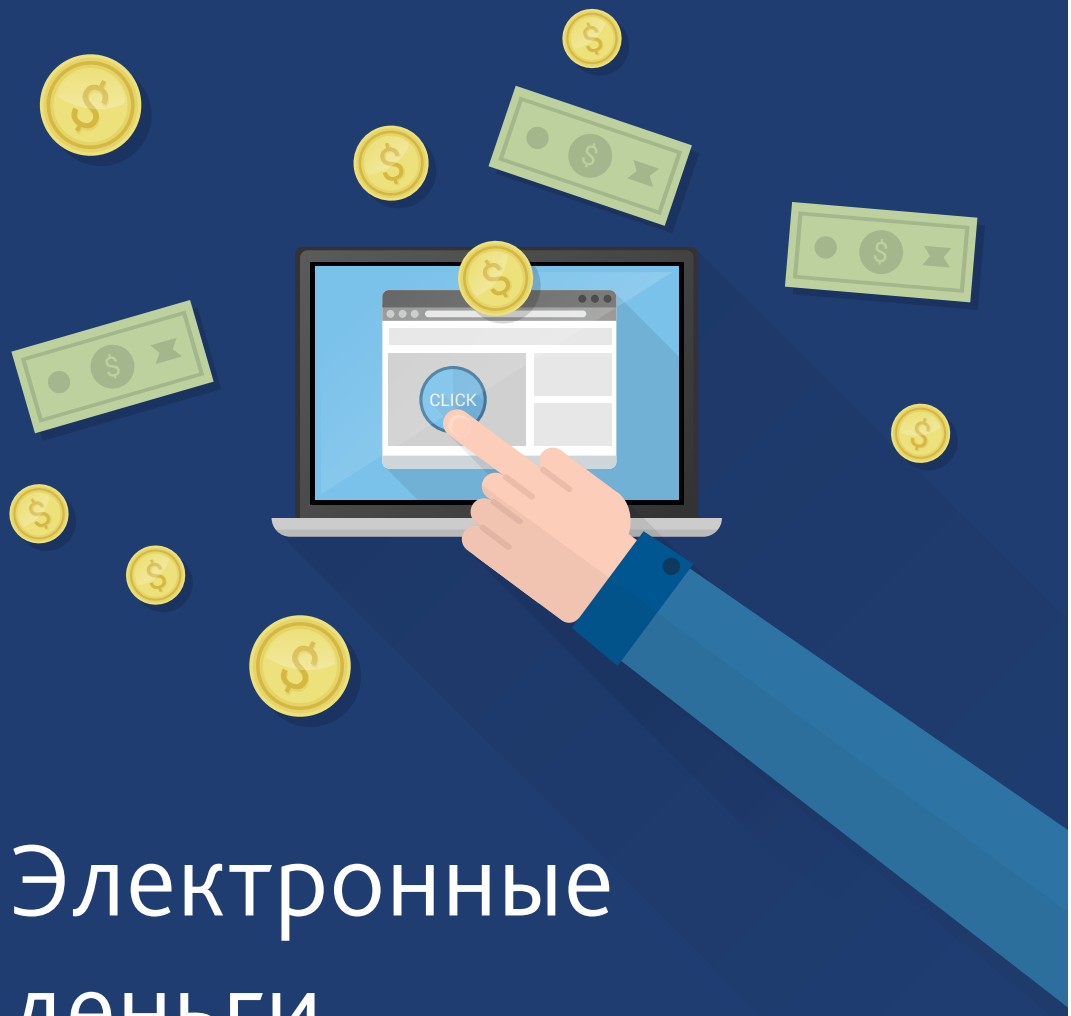
Электронное вымогательство 40

Мобильная безопасность 44

Безопасность персональных данных 50

Дети и деньги в Интернете 54

Инвестиции 58



Электронные деньги

Деньги… Кажется мы все знаем о деньгах… Как зарабатывать, где хранить, куда тратить…

А что такое ***«электронные деньги»****? Или точнее «деньги в интернете»? Чем они отличаются от привычных нам «бумажек» и «монеток»? Почему если они у Вас есть, то однажды их у Вас может не стать? И что делать, чтобы этого не произошло?*

А давайте попробуем разобраться вместе.

Так что же такое «электронные деньги»?

Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» так определяет понятие «электронные денежные средства - денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа. При этом не являются электронными денежными средствами денежные средства, полученные организациями, осуществляющими профессиональную деятельность на рынке ценных бумаг, клиринговую деятельность и (или) деятельность по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами и осуществляющими учет информации о размере предоставленных денежных средств без открытия банковского счета в соответствии с законодательством, регулирующим деятельность указанных организаций».

Вы что-нибудь поняли?.. Ну и ладно!

Для целей нашего буклета, давайте будем считать, что **«электронные деньги» - это денежные средства, переведенные на электронный носитель** (будь то банковская карта, электронный кошелек, электронная платежная система или что-то еще).

Для тех, кто хочет знать подробнее

Банковская карта (или банковская платёжная карта) – пластиковая карта, привязанная к одному или нескольким расчётным счетам в банке. Используется для оплаты товаров и услуг, в том числе через Интернет, а также снятия наличных в банкоматах и операционных кассах.

Конечно, на самом деле на карте нет никаких денег. Банковская карта только отражает состояние банковского счета, к которому она привязана. И в случае воровства денег с банковской карты, деньги утекают именно из банка, а значит банктоже (а не только Вы) несет ответственность за безопасность Ваших «электронных денег на банковской карте». Именно поэтому в соответствии с пунктом 15 статьи 9 Федерального закона «О национальной платежной системе» банк обязан возместить клиенту денежные средства, переведенные без его согласия, при условии, что клиент уведомил банк о том, что перевод сделан без его согласия. Такое уведомление должно быть направлено сразу после обнаружения факта утраты карты или её использования без согласия клиента, но не позднее дня, следующего за днем получения от оператора по переводу денежных средств уведомления о совершенной операции. При этом клиент не обязан доказывать, что потеря денежных средств произошла не по его вине, то есть банк обязан вернуть деньги в случае если «не докажет, что клиент нарушил порядок использования банковской карты, что повлекло совершение операции по переводу денег без согласия клиента».

Виртуальная банковская карта – банковская карта, предназначенная специально для совершения платежей в интернете. Может выпускаться в двух вариантах – в электронном виде и в виде пластиковой карты, не имеющей большинства атрибутов обычной банковской карты (чаще всего на такой карте указываются только номер карты, дата окончания её срока действия и код проверки подлинности карты CVC2/CVV2), что не позволяет использовать её для оплаты покупок в обычных оффлайн-магазинах, или снимать наличные в банкомате.

Электронный кошелек – чаще всего подразумевается устройство и программное обеспечение, позволяющее хранить, пополнять и перечислять электронные деньги. Самые известные электронные кошельки – Яндекс.Деньги, карта «Тройка» московского метро, электронный кошелек сервиса QIWI. Электронный кошелек позволяет легко

оплачивать некоторые услуги, оказываемые в электронном виде через интернет и не только (например, пополнив через интернет электронный кошелек карты «Тройка» вы можете оплатить поездку в московском метро без необходимости стоять в очереди в кассу). Электронные кошельки обычно не позволяют снять наличные напрямую, но дают возможность совершить перевод (через электронную платежную систему), например, на банковскую карту с которой уже можно будет получить деньги в банкомате.

Электронная платежная система – электронная система расчетов при покупке/продаже товаров и услуг через интернет. Самые известные электронные платежные системы – WebMoney и PayPal. Для совершения операций через такие платежные системы обе стороны сделки должны быть зарегистрированы в системе. Перевод денежных средств в электронной платежной системе осуществляется с электронного кошелька этой же системы, либо напрямую с банковской карты. Кроме того, при проведении трансграничного платежа (покупке в иностранном интернет-магазине) электронная платежная система может осуществлять автоматическую конвертацию валюты по своему курсу. Основная задача электронной платежной системы – предоставление гарантий безопасности перевода как покупателю, так и продавцу. Так например в системе PayPal в случае оплаты покупок, подлежащих доставке, деньги не поступают на счет продавца до тех пор, пока покупатель не подтвердит факт доставки, либо не истечет время открытия спора со стороны покупателя. В течение 180 дней с момента осуществления платежа покупатель имеет

возможность открыть спор в случае, если доставленный товар отличается от заказанного, либо доставка не осуществилась.

Мобильный и интернет-банк (интернет-банкинг) – сервис, предоставленный банком, для дистанционного банковского обслуживания клиента, позволяющий получить клиенту доступ к своим счетам и совершать операции с ними, предоставляющийся в любое время с любого устройства, имеющего доступ в интернет (в случае интернет-банкинга для выполнения операций используется специальный интернет-сайт, доступ к которому осуществляется посредством браузера (то есть отсутствует необходимость установки клиентской части программного обеспечения системы), в случае мобильного банка – мобильное приложение для смартфонов и планшетов). ■

Платежи в интернете

Зачем же еще нужны электронные деньги, если не для того, чтобы оплатить товар или услугу не выходя из дома?! Вспомним, как было раньше: чтобы оплатить счет за коммунальные услуги, мы брали бумажную квитанцию и шли в сберкассу, где стояли в очереди в маленькое окошечко операционистки; чтобы оплатить мобильный телефон, мы шли в офис мобильного оператора или покупали карту оплаты, с которой стирали защитный слой и вводили полученные циферки в соответствии с напечатанной инструкцией; чтобы купить билет на поезд, мы ехали на вокзал, где, отстояв очередь узнавали, что билетов на нужную дату уже нет…
А что сейчас?

Теперь мы можем оплатить коммунальные услуги, штрафы и налоги, купить билеты в кино и театр, на самолёт или поезд, перевести деньги родителям и многое другое, не слезая с любимого дивана и не снимая домашних тапочек. Да много чего можем – все зависит от того, есть ли соответствующая опция у получателя платежа, ибо механизм-то в общем один и тот же.

Не секрет, что именно оборот денег в Интернете является главной целью киберпреступников – свыше 80% преступлений, расследуемых полицейским управлением «К» (от слова «киберпреступления»), связаны как раз с нечестным уводом или отъемом денег при помощи цифровых технологий. Сформировался даже термин «экономические угрозы» - на практике они представляют собой совокупность программно-технических и контентных методов, направленных на хищение чужих денежных средств в Интернете. И речь здесь идет в общем-то не о взломе банковских компьютерных систем…

Где могут обмануть?

На фишинговом сайте (то есть сайте, сделанном специально для того, чтобы получить секретные данные Вашего банковского счета или карты)

Фишинговый поддельный сайт очень (ну очень-очень) похож на настоящий как дизайном, так и доменным именем (символами, которые вводятся в адресную строку браузера для попадания на нужную интернет-страницу). Отличить такой сайт от официального сайта банка или платежной системы «на глаз» очень сложно.

Здесь есть два варианта. Первый – когда пользователь изначально попадает на фишинговый сайт, являющийся точной копией оригинала. Второй вариант - фишер встраивает ссылку на свою страничку в подлинный сайт, и, кликая мышью на адрес платежной страницы, юзер на самом деле оказывается на ее имитаторе. При этом все остальные ссылки, кроме ключевой – настоящие. Далее в обоих случаях пользователь оставляет на сайте нужные для платежа данные – и расстается с деньгами навсегда.

С помощью фишинговых писем, направленных на электронную почту

Такие письма обычно маскируются под официальные сообщения от администрации банка, в которых сообщается, что получатель должен подтвердить све-

Довольно быстро после появления онлайн-мошенничества возникло словечко **«фишинг»** - сначала оно олицетворяло лишь один вид сетевого жульничества, затем стало синонимом Интернет-мошенничества вообще.

«Фишинг» - по-русски означает «рыбалка», в которой «рыбаки»-мошенники ловят невнимательного Интернет-пользователя. И главные объекты атаки таких «рыбаков» - внимательность и доверие юзеров.

Цель фишеров – получить доступ к тому месту, где в Интернете «чужие деньги лежат». Поэтому их интересует все, что позволит получить доступ к этим самым деньгам. Ключевое их отличие от хакеров, которые как раз взламывают банковские системы – в том, что они, подобно Остапу Бендеру, пользуются исключительно обманом доверия граждан. Таким образом они стремятся получить пароли, коды доступа, номера кредиток и прочую конфиденциальную информацию. В зависимости от ситуации, разными путями.

«Смычкой» фишеров и хакеров является использование **кейлоггера.** В данном случае злоумышленник при помощи программы, заранее «подсаженной» на компьютер жертвы, получает информацию даже о том, как именно жертва жмет на клавиши – отслеживаются порядок и интервал нажатия клавиш, после чего эта информация пересылается «хозяину». Кейлоггер относится скорее к разновидности **«трояна»**, поэтому его использование к собственно фишингу можно отнести с большой натяжкой – но тем не менее, поскольку речь идет о безопасности денег в цифровой среде, есть прямой резон о нем упомянуть. Технологической разновидностью фишинга в чем-то является и **кардинг** (снятие в мошеннических целях информации с кредитных карт посредством технических устройств), который давно выделился в самостоятельную проблему – однако кардинг представляет собой хотя и цифровую, но оффлайновую угрозу и касается работы с банкоматами.

дения о себе (или срочно сменить пароль), иначе его счет будет заблокирован, и приводится адрес подставного сайта, внешне очень похожего на официальный сайт банка. Среди данных, которые необходимо ввести, есть и те, которые нужны мошенникам. Следует всегда помнить: НИ ОДИН почтовый сервер и тем более ни одна кредитная организация НИКОГДА не запрашивает пароли своих клиентов – ни по почте, ни по Интернету.

1 - Фишинг (от английского «fishing» – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям, номерам и секретным кодам кредитной карты.

Обычно для определения адресатов фишер пользуется базой данных клиентов интересующего его банка. А вот если имитируется почтовая служба (кстати, один раз «изобразили» Mail.Ru), то точной разведкой пренебрегают – у таких сервисов слишком много клиентуры для того, чтобы клиент заподозрил фишинг. Конечно, в большинстве случаев пароли от почтового ящика денег не дают, но зато контроль над чужой почтой позволяет успешно спамить с этого ящика или читать приходящую туда конфиденциальную информацию (в том числе ведущую к деньгам).

В случае подмены платежных реквизитов получателя

К сожалению, далеко не все пользователи имеют терпение перепроверить кучу нулей в номерах счетов, ИНН или БИК, и ограничиваются только заголовком получателя платежа. Разновидностью такой схемы является подмена скачиваемых с сайта квитанций для оффлайнового платежа – если собственно платежная страница всегда защищена сильнее всего, то вот прочие текстовые страницы могут иметь к себе меньшее внимание работников кибербезопасности, и слегка поменять их содержимое зачастую оказывается легче.

Вы скачиваете подмененную квитанцию и, ничего не подозревая, идете с ней в банк, совершая перевод отнюдь не адресату – а мошеннику на его реквизиты. Надо сказать, что подобный способ обмана перекочевал и в оффлайн – в некоторых регионах России регистрировались случаи вброса в почтовые ящики фальшивых квитанций за коммунальные услуги, отличавшихся от оригинала только банковскими реквизитами.

На мошеннических сайтах продажи авиабилетов

Билеты на таких сайтах могут стоить значительно дешевле, чем на официальных сайтах известных авиакомпаний. После оплаты Вы даже можете получить на e-mail якобы электронный билет, а о том, что Вас обманули узнать уже в аэропорту.

В случае кражи или потери смартфона, а также заражения вирусом, ворующим деньги

Приложение «мобильный банк», установленное на смартфон, предоставляет слишком широкие возможности нечистым на руку гражданам.

В случае взлома электронной почты

Сервисы электронных платежей и электронные кошельки имеют опцию «восстановление пароля», которая работает через зарегистрированную электронную почту. Это значит, что в случае получения доступа к Вашей электронной почте, злоумышленник также получает доступ к связанному с ней электронному кошельку или платежной системе путем получения нового пароля.

Путем получения дубликата сим-карты

Внедрение услуги смс-оповещения от банков и некоторых интернет-сервисов заставило преступников искать новые способы доступа к деньгам интернет-пользователей. Получение дубликата сим-карты (например, с помощью сообщника в офисе мобильного оператора или фальшивой доверенности) позволяет перевести все операции с мобильным банком на смартфон мошенника или получить доступ к интернет-банкингу.

На что надо обратить внимание?

На строку ввода интернет-браузера

Сайты «приличных» электронных платежных систем всегда защищены сертификатами SSL. То есть адрес сайта, через который Вы хотите провести оплату, должен начинаться с «https://» и иметь пиктограмму в виде закрытого замка зе-

леного цвета, что означает что сайтом используется защищенный интернет-протокол, который не даст хакерам перехватить секретные данные вашего счета.

На любые отклонения от обычного поведения Вашего банка или платежной системы (например, запрос новых сведений, которые раньше не надо было вводить)

Если что-то идет не так как обычно, лучше отказаться от операции и перепроверить информацию у банка.

На доменное имя сайта

Если доменное имя отличается хотя бы на один символ от привычного Вам, лучше ввести имя сайта заново или вообще отказаться на некоторое время от использования интернет-сервиса в пользу альтернативного варианта.

Внимательно читайте текст электронных писем от банков и платежных систем, так как:

Электронные письма от известных компаний не должны содержать орфографических или грамматических ошибок.

Типичное фишинговое письмо начинается с обезличенного приветствия «Уважаемый пользователь» или обращения по адресу электронной почты. Ваш банк или платежная система обычно знает Ваше ФИО и в настоящем письме приветствует Вас, обращаясь по имени и фамилии (или имени и отчеству).

Чаще всего мошеннические электронные письма содержат призывы к безотлагательным действиям (используя такие слова как «немедленно», «безотлагательно» «последнее предупреждение»), пытаясь заставить Вас действовать быстро и необдуманно

На внезапный отказ в работе сим-карты (появление надписи «Вставьте sim-карту» или аналогичной)

Зайдите в ближайший офис Вашего мобильного оператора или позвоните ему с другого телефона и уточните в чем проблема, возможно, кто-то получил дубликат Вашей сим-карты – в этом случае срочно блокируйте её.

Что еще можно сделать?

При совершении Интернет-платежа необходимо тщательно проверить все платежные реквизиты.

Сравнить их с тем, что Вы видите на экране. Можно с другими страницами на том же сайте. Можно с данными других сайтов, относящихся к этой организации – их можно найти через поисковик. А если Вы оплачиваете штраф, пошлину или коммуналку тому же получателю уже не в первый раз, но сейчас хотите сделать это онлайн – просто возьмите старые квитанции и проверьте банковские реквизиты по ним. Потратив лишнюю минуту, Вы сэкономите приличное количество денег.

Фишерскую поделку реально выявить при помощи Интернет-браузера

При наведении мышью на кнопку сайта или ссылку в левом углу браузера обычно проявляется подлинный адрес веб-страницы. И в фишинговом случае вместо указанного на странице, скажем, pay.bank.com в углу проявится какой-то «левый» адрес, а то и вообще IP.

Не переходите по ссылке, указанной в письме

Лучше наберите адрес сайта в браузере сами или найдите через поисковую систему (например, «Яндекс» точно знает официальные адреса сайтов крупных банков и умеет предупреждать о подозрительных сайтах). Не стесняйтесь позвонить в банк по номеру телефона, указанному на Вашей карте (именно на карте, а не указанному в письме или сайте, открывшемуся по ссылке из письма, – там вполне может оказаться человек из команды мошенников) и все уточнить.

Не пренебрегайте возможностью услуги «смс-оповещение» от банка

Если деньги начнут внезапно утекать с Вашего счета, будет шанс успеть заблокировать карту.

Не вводите данные Вашей банковской карты или счета на неизвестных ресурсах, а также не оплачивайте авиабилеты «с карты на карту» или если получателем денежного перевода является физическое лицо

Солидный интернет-ресурс для проведения платежа переадресует Вас на сайт Вашего банка или выбранной платежной системы.

С помощью сервиса «http://www.tcinet.ru/whois/» можно узнать, как давно был создан сайт

Сайты мошенников – это интернет-страницы-«однодневки», созданные буквально вчера, и которые очень быстро закроются.

Установите лицензионный антивирус (не только на обычный компьютер, но и на смартфон)

Многие из них блокируют не только вирусные программы (что само по себе очень важно), но и ссылки на фишинговые сайты.

Покупая авиабилеты на незнакомом сайте, непременно посмотрите, что это за компания

Проверьте адрес сайта или телефон службы поддержки в поисковике, посмотрите, что пишут о нем пользователи.

Проверьте сайт продавца авиабилетов с помощью сервиса «настоящийбилет.рф»

Сервис создан специально для выявления мошенников, продающих несуществующие авиабилеты.

Если у вас к счету мобильного телефона привязана банковская карта, то в случае утраты мобильного телефона обязательно и срочно блокируйте не только сим-карту, но и банковскую карту

В крайнем случае позже ее можно будет разблокировать.

Не используйте простые пароли (а тем более не надо использовать один и тот же пароль на разных интернет-ресурсах) и не ленитесь периодически их менять (особенно в случае появления подозрения, что текущий вариант пароля скомпрометирован)

Никто не любит сложных паролей из-за того, что их легко забыть, но если Вы хотите уменьшить вероятность взлома почты хакерами, это правило должно обязательно выполняться. ■

Интернет-магазины

Последнее время мы спешим все больше, а успеваем все меньше… С прогрессом ритм жизни жителя мегаполиса ускоряется. Нам уже некогда стоять у плиты и ходить по магазинам, и мы заказываем еду с доставкой на дом и покупаем товары в интернет-магазинах (в том числе и зарубежных). При этом цены в Интернет-магазинах, как правило, значительно ниже, чем в обычных – не только за счет налоговых особенностей, но и просто из-за уменьшения операционных расходов. Не нужен торговый зал, куча продавцов и кассовых аппаратов, даже доставку можно «аутсорсить».

Именно с Интернет-магазинами связано большинство «товарно-денежных» проблем, с которыми сталкиваются российские (и не только) пользователи Сети. Эти проблемы можно поделить на две части: **чистое мошенничество и проблемы с качеством товара.** В первом случае пользователь отправляет деньги и не получает товар вообще (или получает совершенно не то), во втором – заказчику приходит некачественный товар и он не знает, что с ним делать.

Покупка в интернет-магазине еще иногда походит на покупку кота в мешке – никогда не знаешь, совпадет ли то, что ты выбрал с тем, что тебе привезут. Ведь «производитель оставляет за собой право изменять конструкцию, технические характеристики, внешний вид, комплектацию товара, не ухудшающие его потребительских качеств, без предварительного уведомления потребителя», а «цвет товара может не совпадать с представленным на фото, в связи с индивидуальными настройками цветов монитора и его яркости»… Но это, конечно, не самое страшное. Хуже если Вы останетесь вообще без товара, заплатив при этом какие-то деньги, или вообще без денег…

Где могут обмануть?

Не доставить покупателю или доставить уже оплаченный товар, но заведомо худшего качества

Некоторые интернет-магазины принимают оплату товара онлайн – то есть Вы сначала оплачиваете выбранный товар с электронного кошелька (например, через «Яндекс.Деньги») или пластиковой карты, а уже после этого продавец высылает Вам товар.

Привезти «серый» или заведомо неисправный товар с последующим отказом его ремонтировать или принимать обратно в случае поломки

Зачастую передача товара, купленного в интернет-магазине, происходит наспех, у дверей офиса или подъезда, что ограничивает возможности покупателя в проверке покупки, в результате чего дефекты обнаруживаются уже после отъезда курьера.

Произвести незаконный сбор персональных данных

Некоторые онлайн-магазины требуют указать на сайте не только номер телефона «для связи», но и еще множество другой информации, абсолютно не пригодной

для целей покупки конкретного товара в конкретном магазине. Собранные данные могут использоваться для распространения спама или рекламных звонков.

На фишинговом сайте

Фишинговый сайт специально сделан для того, чтобы получить номера и пароли (коды) кредитных карточек или систем онлайновых платежей пользователя. Естественно никакого товара вам на таком сайте не поставят.

Заказ товара на зарубежной Интернет-площадке

Далеко не факт, что данная площадка имеет свое представительство в Российской Федерации, поэтому применить защищающие Вас нормы закона о защите прав потребителей здесь удастся в очень ограниченном объеме.

Любая уважающая себя торговая площадка в Интернете обеспечивает безопасность проводимых платежей – правда, здесь безальтернативным способом оплаты становится банковская карта (PayPal как средство проводки платежей также

«привязывает» банковскую карту). Присутствует базовая информация о доставке товара и, разумеется, о контактах; обычно дается информация о правилах возврата. Однако крупные площадки всегда предупреждают, что они не несут ответственности в связи с особенностями национального законодательства в каждой конкретной стране, поэтому уточнить все «национальные» вопросы лучше самому покупателю до заказа.

Заказ товаров, которые могут неожиданно оказаться «нелегальными» в России, хотя полностью легальны в стране, где находится зарубежный Интернет-магазин

В первую очередь это касается таких «модных фишек», как устройства с фото- и видеокамерами, а также диктофонами. Самый известный пример – Google Glass, очки со встроенной видеокамерой. В России они относятся к спецтехсредствам для негласного получения информации, а значит, могут использоваться только в оперативно-розыскной деятельности. Если раньше товар просто блокировался таможней и отправлялся назад (а Вы теряли деньги), то сейчас наши «доблестные» правоохранители могут устроить Вам «маски-шоу» прямо на почте, куда Вы, ничего не подозревая, придете за посылкой. Это же касается любых ручек и часов с встроенными камерами и диктофонами, которые Вы совершенно легально можете купить в Европе за скромную сумму. Но вот ввезти такое устройство в Россию – нет.

На что надо обратить внимание?

Отзывы покупателей о выбранном интернет-магазине

Покупайте на проверенных сайтах (по рекомендациям знакомых и друзей). Если выбираете товар в российском интернет-магазине, например через «Яндекс.Маркет», почитайте отзывы о продавце тех, кто уже совершал покупки. При покупке из-за рубежа обращайтесь к известным крупным интернет-магазинам («Amazon», «Ebay» и др.) – они дорожат своей репутацией и имеют свою систему безопасных покупок, позволяющую вернуть деньги.

Наличие защищенного SSL-сертификатом интернет-протокола в случае предоплаты товара

Как и сайты безопасных платежных систем, сайты интернет-магазинов должны быть защищены – это значит, что при проведении оплаты через интернет

строке ввода адрес сайта должен начинаться с «https://» и иметь пиктограмму в виде закрытого замка зеленого цвета.

Наличие чека

Требуйте у продавца кассовый чек – стопроцентной гарантии того, что в случае чего продавец заменит Вам негодный товар, нет, но без него Ваши шансы на замену или возврат денег резко сокращаются.

Количество и состав собираемых персональных данных

Бездумная раздача своих персональных данных может привести к неприятным последствиям, самым безобидным из которых может быть спам. Поэтому если заказываете товар с доставкой курьером, ограничьтесь указанием имени и номера мобильного телефона для связи. Если же заказать товар без указания дополнительной информации о себе невозможно, лучше выбрать другого продавца и написать жалобу в Роскомнадзор

Фотографии товара

«Ворованные» в другом магазине фото – явный признак проблемности. Бывает, конечно, что изображения товаров магазин ставит от официального производи-

теля или дилера, но обычно каждая площадка стремится продемонстрировать «индивидуальность» и лишний раз показать, что этот товар есть именно у них.

Слишком низкая цена

Если она значительно отличается от среднерыночной, то есть предлагаемой другими Интернет-магазинами. Именно этим приемом – очень низкой ценой – часто пользуются Интернет-мошенники, чтобы заставить людей отправить деньги именно им.

Что еще можно сделать?

Нужно внимательно почитать информацию, связанную с возвратом и обменом товаров, и сравнить ее с законом о защите прав потребителей

Магазины, которые предлагают «страховку от некачественного товара», имеет смысл обойти стороной – это значит, что даже если товар окажется некачественным, быстрой замены товара ожидать от магазина не придется. Точно так же лучше избежать покупок в тех магазинах, в которых информации о возврате или обмене практически нет или где есть абстрактная ссылка на закон без подробностей. Если же речь идет о пересылке товара из другого города, то вопрос организации возврата товара важно понимать тем более, так как возможность прямо сконтактироваться с продавцом здесь сведена к минимуму.

Не менее важно изучить еще два раздела: «Доставка и оплата» и «Контакты»

Помимо опций доставки, уважающий себя Интернет-магазин обязательно напишет, какие именно документы о покупке Вы получите – а это очень важно, если у Вас появятся претензии к товару. Из этого раздела Вы получите и сведения о том, кто на какой стадии отвечает за сохранность товара – это поможет избежать ситуации, когда магазин с курьерской компанией будут «кивать» друг на друга, пока Вы ждете разрешения своих претензий. Что же касается контактов, или раздела «О магазине» - то там, помимо рекламной информации, Вас в первую очередь должны будут заинтересовать чисто формальные сведения. Организационно-правовая форма, сведения о регистрации, всевозможные лицензии (если такие есть) и, разумеется, формы контактов. Минимум таких сведений должен навести на подозрения. Мно-

гие небольшие Интернет-магазины указывают для связи мобильный телефон и адрес электронной почты. Для «молодого» магазина это может быть нормально, но вот если магазин утверждает, что работает довольно давно – это может вызвать подозрение… Разумеется, наличие городского телефона и фактического адреса резко повышают «статус надежности» Интернет-магазина, но считать это стопроцентной защитой от мошенников нельзя – в конце концов, ничто не мешает им просто-напросто написать «липовый» адрес…

По возможности не производите предоплату покупок

Многие (а в Москве большинство) российские интернет-магазины позволяют оплатить товар курьеру после его доставки и проверки.

В случае если без предоплаты покупки не обойтись, используйте платежные системы, имеющие свою систему гарантий сделки или заведите себе отдельную пластиковую карту для оплаты покупок через интернет

Использование таких платежных сервисов (например, PayPal) обойдется дороже (за счет не очень выгодного курса обмена валюты или взимания некоторой комиссии), но позволит вернуть деньги в случае, если товар не доставлен или не того качества. В случае оплаты банковской картой, можно воспользоваться специально заведенной для таких случаев картой, на которую вы переводите достаточную сумму непосредственно перед покупкой, или виртуальной банковской картой.

Старайтесь тщательно проверить товар

Не поддавайтесь на разговоры курьера о том, что он спешит – в соответствие с Законом «О защите прав потребителей» у Вас есть право как минимум тщательно осмотреть своё приобретение и прилагающиеся документы, а при возможности и проверить работоспособность. В случае если Вы располагаете свободным временем, то лучше выбрать способ доставки «самовывоз» – при этом в пункте самовывоза обычно имеется возможность осмотреть и проверить работоспособность товара.

Самовывоз, как правило, позволяет покупателю сильно сэкономить на доставке – особенно если товар небольшого размера и покупатель имеет возможность за ним приехать. Некоторые магазины, впрочем, берут определенную плату и за самовывоз – хотя она будет значительно меньше, чем стоимость доставки. Самовывоз, как правило, производится со склада Интернет-магази-

на, где обычно располагается и сама контора, либо из пункта выдачи товаров данной торговой сети (в последнем случае это может значить, что продавцу придется привезти заказанный Вами товар в конкретный пункт). В любом случае Вы имеете возможность спокойно проверить товар на комплектность и качество, после чего спокойно заплатить деньги.

«Продвинутый» пользователь может проверить также дату регистрации домена и сопутствующие ему сведения из WHOIS (то есть реестра принадлежности доменных имен).

Разумеется, гораздо более надежными выглядят те магазины, которые зарегистрировали домен давно и на собственное юридическое лицо. Правда, здесь нужно учитывать, что довольно много магазинов создаются индивидуальными предпринимателями, и WHOIS опознает их как физических лиц (Private Person). Если же на сайте написано, что оператором магазина является юрлицо (скажем, некое ООО), а реестр доменов говорит о частном лице, это может вызывать некоторые «смутные сомнения»…

Обязательно изучите условия гарантийного обслуживания покупаемого Вами товара на территории России

Существует ли гарантийная мастерская, распространяется ли гарантия на нашу страну, какие документы Вам потребуются при возможном походе в мастерскую, есть ли, в конце концов, гарантия на обмен товара на территории нашей страны (это обычно касается электроники, хотя и здесь встречается крайне редко). Помните, что зарубежный Интернет-магазин торгует по законам своей страны.

Обязательно изучите таможенные нормы и правила относительно стоимости и веса товара для беспошлинного ввоза, а также о частоте покупок

Не исключено, что, если Вы в один месяц закажете кучу дорогостоящих товаров, то с них Вам предложат заплатить пошлину. При этом отправить товар назад может не получиться – магазин Вам деньги не вернет, так как за таможенные риски страны назначения он ответственности не несет.

В общем и целом, главное качество успешного онлайн-покупателя – внимательность. Изучите всю доступную информацию и обратите внимание на важные мелочи – это поможет избежать многих опасностей при совершении покупок в Интернете. ■

Онлайн-аукционы и Интернет-доски объявлений о продаже товаров

Очень во многом близки к Интернет-магазинам онлайн-аукционы и Интернет-доски объявлений о продаже товаров. Однако главное их отличие – в том, что на этих площадках производится «разовая» купля-продажа от частных продавцов, как на стихийной «толкучке». Правда, не секрет, что на многих крупных площадках подобного рода «работают» и полноценные Интернет-магазины, создавшие свое «представительство» на популярной площадке – такие продавцы, разумеется, придерживаются общих правил стандартных Интернет-магазинов. Но вот к частной купле-продаже такие правила обычно не применяются, и риски покупателя при покупке у «частника» значительно выше.

В принципе, все риски примерно совпадают с теми, что характерны для недобросовестных онлайн-магазинов. Хитрый продавец, разумеется, может умолчать о некоторых недостатках продаваемого товара, поместить его фотографии, не показывающие «проблемные» места, либо вообще поставить фотографию похожего товара. Доставка товара производится обычно либо почтой, либо при личной встрече – в обоих случаях ни о каких кассовых и товарных чеках, разумеется, речи не идет, и доказать факт покупки товара за определенную цену будет значительно сложнее – только при помощи самого объявления и переписки продавца с покупателем (впрочем, некоторые продавцы принимают оплату переводом на их банковскую карту). Самое же главное – обменять товар Вам, скорее всего, не удастся, так как у такого продавца замены просто может не быть. Поэтому ориентируйтесь на вариант возврата денег и поиска нового продавца с таким же товаром. ■

Платим за опции и контент…

Помните у Гермионы Грейнджер в волшебной сумке помещалось большое множество нужных вещей… А чем мы хуже? Вот у нас в сумках легко помещается целая библиотека книг, десяток CD-дисков популярных музыкантов и пара-тройка видеокассет с новинками кинопроката… В электронном виде, естественно. А все потому, что имея канал доступа в интернет с хорошей пропускной способностью, можно все это скачать на свой смартфон или планшет и спокойно забыть о походах в кинотеатр, на концерт или книжный магазин, ведь интернет позволяет приобретать не только материальные товары, но и ***контент***[2]*.*

2- Контент – обобщенное название всего того, что можно скачать (посмотреть, почитать, послушать и т.д.) в интернете (программы, тексты, фильмы и др.).

Неотъемлемая часть современного цифрового бизнеса – предоставление различных «дополнительных» услуг. Некоторые из них действительно облегчают жизнь (особенно для людей определенных профессий), некоторые служат чисто для развлечения. Поскольку в их создание и распространение вкладываются определенные деньги, то эти сервисы, как правило, платные – хотя обычно и недорогие. Отдельной строкой стоит **плата за доступ к контенту** – текстовому, звуковому, или видео, который распространяют на различных онлайн-площадках. Как правило, она связана с необходимостью отчислений авторам и правообладателям, то есть с тем самым «копирайтом».

Основная финансовая проблема, которая возникает у людей, регулярно пользующихся такими платными «примочками» - в какой-то момент с их мобильных счетов **начинает уходить гораздо больше денег, чем они ожидали**. В некоторых случаях причина этому – просто неумение отслеживать все свои мобильные и контентные расходы, но очень часто перерасход средств так просто не объяснить… И тут уже вопросы возникают к тем, кто эти платные услуги предоставляет – потому что в таких случаях проблема обычно с их стороны.

Дело в том, что вся информация об условиях предоставления услуги до пользователя часто не доходит. К примеру, пользователь может видеть рекламный слоган на пол-экрана, а вот ссылку на полные условия предоставления услуги придется поискать. И если она найдется где-то в медвежьем углу сайта мелким шрифтом, то пользователь получит кучу текста мелким шрифтом, который он на экране смартфона просто не разберет. Поэтому юзер ориентируется на главное условие из рекламного слогана, оставаясь неосведомленным о других, столь же важных для него, условиях. Например, об отключении услуги или о характере взимания платы за нее. В результате легко может оказаться, что пользователь кликает по рекламе «Получите доступ к фильму за 20 рублей», думая, что он платит 20 рублей за этот фильм – а на самом деле он соглашается на списание с него двадцати рублей в день независимо от того, заходил ли он в последующие дни на этот сайт или нет. В месяц это уже 600 рублей получается…

Еще один характерный пример – **изменение стоимости мобильной услуги.** Например, в рекламных целях абонентам мобильной сети предлагается некий сервис «за бесплатно». А через какой-то период он становится платным. Причем пользователю «напоминалка» об этом либо не прилетает вообще, либо может прийти обычная СМС, совершенно не говорящая, как и где именно можно отключить данную услугу. «Хорошим тоном» считается прислать прямую ссылку для отключения услуги – в ином случае юзер будет метаться по сайту мобильного оператора, пытаясь найти место, где он сможет управлять своими подписками. И, с учетом теперешнего **уровня цифро-**

вой грамотности населения, далеко не каждый это место найдет. И тогда с пользователя опять же будут списываться дополнительные деньги за услугу, от которой он на данных условиях вообще-то собирался отказаться.

Важно!

Принимая решение качать фильм или книгу через торрент-трекер или файлообменник надо помнить, что в Российской Федерации (а равно и в других цивилизованных странах мира) авторское право защищено законом. Это значит, что если данный контент размещен незаконно, а Вы его скачиваете – Вы обкрадываете любимого автора. А еще это значит, что незаконное размещение (а кое-где и скачивание) электронной версии фильма, книги, музыки и другого контента с нарушением чужих авторских прав наказывается по закону реальным штрафом или даже сроком заключения.

И это не говоря об обычных мобильных и Интернет-мошенниках, которые либо вообще не дадут пользователю запрошенной услуги, либо получат данные о его электронном кошельке (а то и банковской карте) и сметут оттуда все без остатка. Или, как вариант, попросят оплатить услугу отправкой СМС на короткий номер, «скромно» умолчав о настоящей цене – которая будет составлять несколько сотен рублей… Впрочем, об этом – в других разделах.

На массовость проблемы обратили внимание общественные организации по защите Интернет-пользователей, которые затем поставили ее на вид индустрии и законодателям. В результате наметились позитивные подвижки навстречу интересам юзеров. К примеру, сотовые операторы облегчили доступ пользователей к управлению их подписками на контент и прочие дополнительные сервисы. Благодаря этому пользователю стало проще видеть, какие конкретно дополнительные опции и «фишки» у него подключены, кто является провайдером данной услуги, и самое главное – сколько денег реально списывается за эту услугу. Там же пользователь сможет ненужную ему услугу отключить – после чего деньги за эту услугу списываться перестанут.

Бесплатный контент

Существует достаточно много сервисов, распространяющих контент по бесплатной или «условно бесплатной» (предполагающей возможность бесплатного потребления контента при условии просмотра рекламы) модели. Особой популярностью в этом ряду пользуются **«торренты»**[3] и **«файлообменники».**

3 - Торрент – система передачи файлов (файлового обмена между пользователями) с использованием специального программного обеспечения. Особенность этой системы в том, что файлы передаются частями с компьютеров пользователей уже скачавших файл, при этом скорость закачки напрямую зависит от количества таких компьютеров. После закачки всех частей файла торрент-программа (торрент-трекер) собирает его в одно целое.

Атрибутом защищаемого авторским правом контента (будь то текст, картинка или что-то еще) является з**нак копирайта** – латинская буква С в окружности – © или полукруглых скобках – (С), вместе с именем правообладателя и годом публикации.

Знак копирайта (С) оповещает пользователя о том, что права правообладателя данного контента защищены законодательством об авторском праве. А это значит, что Вы не можете использовать контент по своему усмотрению без разрешения правообладателя. Так, например, большинство СМИ разрешают перепечатку своих авторских текстов при условии указания ссылки на первоисточник, а вот профессиональные фотографы, заработок которых напрямую зависит от числа копий сделанных ими фотографий, запрещают любое бесплатное использование своих авторских произведений.

Таким образом, наличие знака © однозначно говорит о том, что на использование контента наложены какие-то ограничения. Вместе с тем, отсутствие знака копирайта не говорит о том, что данный контент можно свободно использовать.

Но существует еще контент, защищаемый «свободной лицензией» (free license) – это такой лицензионный договор, условия которого содержат разрешения пользователю от правообладателя на конкретный перечень способов использования его произведения. Например свободная лицензия на программное обеспечение (так называемое СПО – свободное программное обеспечение) или свободная лицензия на произведения культуры «Creative Commons» (CC). Свободные лицензии также могут налагать некоторые ограничения на использование контента – например, запрет использования произведения в коммерческих целях.

Где могут обмануть?

При распространении пиратской копии

Если сомневаетесь в «чистоте» авторских прав скачиваемого файла лучше поискать другие, легальные способы получить нужную информацию. Например, воспользоваться сайтом «онлайн-кинотеатр», где недорого (а может и бесплатно, но при наличии рекламы) можно посмотреть приглянувшийся фильм.

Спрятав вирус внутри архива скачиваемого файла

Такой способ «внедрения» вируса на Ваш компьютер встречается достаточно часто. Особенно внутри самораспаковывающихся архивов.

4 - Файлообменник – это сервис, на котором пользователь может разместить свой файл (или несколько файлов) в интернете, а взамен получить ссылку (гиперссылку), по которой этот файл будет круглосуточно доступен всем, кому она будет известна.

При отправке смс с «секретным» кодом доступа

При попытке найти в интернете бесплатный контент в виде фильма или программного обеспечения пользователи периодически натыкаются на сайты, предлагающие ввести номер мобильного телефона. Выглядит это примерно так: «Напишите номер своего мобильного, Вам придет смс с кодом (или ссылкой), подтвердите ее получение ответной смс-кой (или нажмите на ссылку) и будет Вам счастье в виде фильма». Объясняется это защитой от «ботов», но на самом деле вполне возможно, что Вас подпишут на платную рассылку или спишут Н-ную сумму со счета телефона, а нужного файла Вы так и не увидите.

На что надо обратить внимание?

На формат скачиваемого файла

Если скачиваемый файл является архивом (или самораспаковывающимся архивом) – лучше поискать другой способ получения нужного контента.

На наличие знака копирайта

Использование контента, защищенного авторским правом, что явно указано наличием знака копирайта, возможно только в пределах обозначенных автором. Если же автор не указал конкретных условий использования своего творения, то использовать его можно только для личных нужд и не в коем случае не для получения коммерческой выгоды.

На качество фильма

Определить авторские права контента, размещенного в сети, простому интернет-пользователю чаще всего не под силу. Но, например, в случае скачивания фильма плохое качество явно говорит о его пиратском происхождении.

Что еще можно сделать?

Не вводить номер мобильного телефона на сомнительных сайтах

Часто тут же мошенники размещают сообщение якобы от лица другого пользователя, который утверждает, что прошел все требуемые процедуры и уже скачал файл, и ничего страшного не случится, если вы сделаете то же самое. Не верьте!

Не отправляйте ответных смс и не активируйте пришедшие ссылки

Некоторые популярные сайты («Одноклассники», «ВКонтакте») для дополнительной защиты просят указать номер мобильного телефона, на который потом присылают код, который надо ввести НА САМОМ САЙТЕ, но ни в коем случае не отправить ответной смс-кой.

Проверьте скачанный файл антивирусом

Современные антивирусы проверяют скачиваемые файлы на наличие в них вредоносных закладок. Не пренебрегайте такой возможностью.

Платный контент

Современные гаджеты позволяют приобретать различные мобильные сервисы – приложения, игры, музыку и т.д. Оплата при этом происходит либо через специальный аккаунт путем списания денег с подключенной к нему банковской карты (обычно при этом не требуется дополнительного ввода данных Вашей карты, а только лишь подтверждение оплаты путем введения пароля), либо с банковской карты напрямую.

Где могут обмануть?

При подписке с ежемесячной/ежегодной оплатой

Некоторые производители платного контента с целью заработать как можно больше идут на хитрость подключая пользователю так называемую «подписку» на свой контент, в результате чего деньги снимаются не единоразово, а с определенной периодичностью.

На стоимости смс

Смс сейчас позволяет сделать много – например, разместить объявление в электронном СМИ или оставить комментарий на форуме радиослушателей. Но вот цена такой смс будет сильно отличаться от стоимости смс-ки Вашего тарифного плана и не в Вашу пользу.

При описании контента

Некоторые производители приписывают своим продуктам несуществующие достоинства, обоснованно полагая, что реклама – двигатель торговли.

На что надо обратить внимание?

На особые условия

Обязательно прочитайте все имеющиеся сноски и «звездочки» - возможно именно там «собака зарыта», т.е. спрятаны главные расходы.

На дополнительную информацию от Вашего мобильного оператора

В соответствии с действующим законодательством при оплате цифрового контента путем отправки смс, оператор связи обязан предупредить Вас о реальной сумме, которая спишется с Вашего телефона, и попросить Вас подтвердить свой платеж. В случае если показанная сумма окажется выше той на которую Вы рассчитывали, Вы можете отказаться от приобретения.

На условия использования цифрового контента

В некоторых случаях приобретенным контентом можно воспользоваться только один раз, а в других – множество раз в течение определенного времени, а в третьем – может оказаться, что Вы оплатили только демо-версию. В любом случае, прежде чем оплатить продукт, ознакомьтесь, что же именно Вы покупаете.

На отзывы пользователей

При покупке, например, мобильного приложения не забудьте почитать отзывы покупателей уже скачавших его себе на смартфон или планшет. Естественно, что при совокупной оценке 2 по пятибалльной шкале и отрицательных отзывах приобретать приложение стоит, только если Вам совершенно не жалко своих денег.

Что еще можно сделать?

При покупке платного контента придерживайтесь правил, указанных в разделе «интернет-магазины»

Покупка цифрового контента отличается от покупки обычного товара только тем, что Вы его не сможете «подержать в руках». В остальном правила оплаты товара через Интернет применимы и здесь.

Отменить покупку в случае покупки «ненужного» мобильного приложения или не соответствующего описанию

При такой покупке через аккаунт магазина цифрового контента мобильной операционной системы можно нажать «отменить покупку» и деньги будут возвращены на вашу карту. Также можно вернуть покупку в интернет-магазин программного обеспечения, например SoftKey, указав например, что приобретенное ПО не подошло для Вашей операционной системы (правила возврата конкретного интернет-магазина необходимо уточнить у продавца), при этом деньги вернутся на сайт, а ПО деактивируется.

Основные рекомендации пользователям:

- **Внимательно читать ВСЕ условия,** на которых предоставляется услуга. Прежде чем подключиться к услуге, нужно найти раздел, где изложены полные условия ее предоставления – и особенно тщательно изучить там, на какой период предоставляется сервис и сколько денег за какой период Вам предстоит за него заплатить. Если Вы не нашли такой раздел – лучше откажитесь от такой подписки, в конечном счете это обойдется дешевле;

- **Обращать внимание на «напоминалки»,** приходящие Вам относительно условий предоставления услуги. Сейчас Интернет-индустрия начинает переходить на принцип «информированного добровольного согласия» пользователя, как в медицине – то есть, если Вы никак не выразили желания получать услугу на новых условиях, услуга сама собой отключится. Однако многие еще работают «по старинке», поэтому – если Вы получили СМС-напоминание об изменении условий оказания услуги и новые условия вас не устраивают – откажитесь от этой услуги. Для этого зайдите в свой Личный кабинет и найдите управление Вашими подписками. Либо позвоните в Вашу сотовую компанию и попросите это сделать оператора – а если он почему-то не может это сделать сам, то пусть он Вам даст подробную инструкцию, как «отключиться» самостоятельно;

- **Не пользуйтесь малоизвестными сервисами,** предоставляющими доступ к контенту. Крупный и серьезный сервис уважает свою репутацию и потому более клиентоориентирован – там легче понять, сколько и за что конкретно Вы платите. К тому же, меньше вероятность вместо вожделенного доступа к новому фильму попасть на сайт Интернет-мошенников. ■

Интернет-мошенничество

Мошеннических сайтов и инициатив в Интернете хватает. Два ключевых свойства Всемирной Паутины – **трансграничность и относительная анонимность** *– переплелись со стремлением людей быстро и без усилий улучшить свое финансовое положение. В результате жулики снимают со своей «целевой аудитории» сливки, измеряемые в миллионах долларов, а число обманутых пользователей продолжает расти.*

Где могут обмануть?

Речь здесь идет о **сайтах и письмах, обещающих «приумножить Ваши вложения»**. Обещание быстрого дохода при минимальном участии вкладчика выглядит всегда заманчиво, но очень редко гарантирует финансовую безопасность…

Финансовые пирамиды

Те, кто постарше, наверняка помнят яркие телерекламы и бренды двадцатилетней давности – «Нефть-Алмаз-Инвест», «Русский Дом Селенга», который «желает вам счастья»… И, конечно же, знаменитое «Я не халявщик, я – партнер» с твердым заверением: «Мы сделаем Ваш ваучер золотым! МММ-Инвест!». Чем обернулись все эти красивые рекламы для обычных людей, решивших поправить свои дела через вложения в «инвестиционные фонды», в России тоже помнят до сих пор – толпы обманутых «не-халявщиков-партнеров», пытающихся вернуть враз исчезнувшие куда-то деньги, были показаны по телеканалам всего мира, а бренд «МММ» стал чуть ли не символом финансовой пирамиды для российского рынка и общества.

Законодатели, разумеется, выводы из той эпохи «первоначального накопления капитала» сделали – деятельность финансовых пирамид в России была запрещена. Однако с развитием в нашей стране Интернета мы получили их «второе пришествие», наряду с обычными мошенническими сайтами.

Что такое «финансовая пирамида»?

Это схема, при которой доход предыдущим вкладчикам обеспечивается исключительно за счет притока новых средств от последующих вкладчиков. Рано или поздно «пирамиде» наступает конец, когда количество новых вкладчиков начинает иссякать. Поскольку вложенные деньги сами по себе не «работают» и не приумножаются, системе взять деньги для выплаты дивидендов (или даже самого вложенного капитала) становится просто негде – и «пирамида» банкротится, а последние вкладчики остаются «при своих интересах». Это в лучшем случае, потому что обычно пирамида делает все, чтобы даже более ранние вкладчики не «выходили из игры» - и, таким образом, при банкротстве схемы они также остаются ни с чем. Организаторы пирамиды, разумеется, не забывают про себя любимых и потому оказываются чуть ли не единственными выигравшими в этой «игре».

В Интернете финансовые пирамиды маскируются примерно так же, как и их оффлайновые предшественники в начале 90-х – под некие **«инвестиционные фонды»** или, чаще, под **«игру на бирже»**. Последнее, по мнению мошенников, очень привлекательно для современной целевой аудитории, потому что в доходы от вложений в промышленность или сельское хозяйство не верят даже пенсионеры. **Торговля акциями** же – для большинства обычных граждан что-то малопонятное, об этом они знают только одно: где-то далеко люди в мгновенном режиме продают и покупают акции через компьютеры, делая на этом деньги. Именно такой механизм и пытаются предложить в Интернете жулики.

На что надо обратить внимание?

Выглядит такой сайт весьма серьезно. Строгий деловой стиль, убедительный язык, даже четко изложенные схемы «работы денег» без Вашего участия - и, разумеется, безусловные заверения, что **Вы в любой момент можете «вывести свои деньги».**

Вот на этом-то последнем и возникает проблема. На сайте, в Вашем «личном кабинете», Вы будете видеть, как очень быстро растет сумма на Вашем аккаунте. **Только вот когда Вы захотите эту сумму оттуда снять, Вам будут чинить различные преграды.** Разумеется, надуманные. От технических сложностей снятия денег до ссылок на различные правила и условия, которые не позволяют вывести деньги из «игры». Если же клиент оказывается настойчив, с ним просто перестают общаться – телефонные звонки остаются без ответа, электронные письма уходят «в пустоту».

С точки зрения возможности остаться без вложенных денег «пирамида» имеет мало отличий от обычного мошеннического сайта – тем более что для Интернет-варианта в любом случае характерна практическая **невозможность забрать свою прибыль.** Именно это и должно в первую очередь насторожить очередного желающего быстро обзавестись новыми деньгами. Еще больше должно насторожить **отсутствие четких оффлайновых координат** в виде офиса, номера лицензии, городского телефона. Обычно подобные сайты в качестве координат указывают в лучшем случае мобильный номер, а зачастую – вообще только адрес электронной почты. Серьезные финансовые конторы, разумеется, так не работают. От совсем уж липовой конторы может частично защитить **самостоятельная проверка лицензии и данных из ЕГРЮЛ через Интернет** – развитие электронных госуслуг сделало это быстрым и легким делом, однако

«фирмы-однодневки» еще никто не отменял – то есть данный способ защиты не стопроцентный. Бывает и так, что мошенники «косят» под иностранную фирму, и этим объясняют отсутствие российских контактов.

Что можно сделать?

Не гнаться за длинным рублем

А если уж жажда обогащения вот-вот готова пересилить здравый смысл, то **обязательно проверить, как выбранная Вами финансовая контора выглядит в оффлайне.** Нелишним будет даже нанести туда визит.

Как и в любых других финансовых делах, внимательнейшим образом читать условия договора – и не «входить в игру», если что-то покажется хоть немного подозрительным.

Особенно если подозрение возникнет насчет условий вывода денег.

«Нигерийские письма»

Название этот вид мошенничества получил по тексту одной из первых подобных рассылок – от имени якобы вдовы свергнутого нигерийского диктатора. Суть подобных писем, приходящих обычно по электронной почте, в том, что к адресату якобы обращается некий потенциально богатый персонаж (или его адвокат). Личность персонажа, как и сценарий, зависит исключительно от фантазии отправителя: например, это может быть сбежавший от госпереворота диктатор далекой страны или чиновник свергнутого режима (чаще – его «вдова» или «дети»), как разновидность - попавший под некие «санкции» бизнесмен. И этому персонажу якобы нужна чья-то помощь, чтобы вывести из-под блокировки большие деньги. Вам за помощь, соответственно, предлагается процент, который составит весьма приличную сумму. От Вас же требуется небольшой – по сравнению с обещанной суммой – перевод на какую-нибудь цель: взятка, переоформление счета и так далее. Разумеется, после получения Вашего перевода «вдова диктатора» исчезает в неизвестном направлении, а Вы остаетесь с несбывшейся надеждой разбогатеть «на халяву».

Если мошенничество уже произошло – обратиться в полицию

Однако это уже будет «махание кулаками после драки» - так как лучше все меры предосторожности принимать заранее…

«Нигерийские письма»

Говоря о контентных мошенниках, нельзя не вспомнить про **«нигерийские письма»** - собирательное название довольно специфичного вида Интернет-мошенничества, который эксплуатирует **стремление людей к неожиданной «халяве».**

Сообразив, что юзеры уже не очень «горят желанием» отсылать живые деньги, мошенники сменили тактику. В некоторых случаях они просят с жертвы не деньги, а персональные данные – для того, чтобы с их использованием беспроблемно добраться до тех самых денег. Мошенники полагают, что пользователь, увидев, что в письме от него не требуют денег, больше поверит в озвученную ему «сказку» и окажется более сговорчивым. Соответственно, фабула повествования тоже поменялась. Например, с Вами может связаться «адвокат», представляющий интересы якобы умершего не так давно Вашего однофамильца. Который будто бы завещал конкретно Вам определенную сумму денег. Впрочем, поскольку получатели обычно неплохо знают свою генеалогию и никак не могут понять, откуда у них взялся «родственник» на другом конце света, история в очередной раз изменилась – теперь обычно деньги бывают «завещаны» первому попавшемуся человеку с такой же фамилией. Или чуть иначе – скончался некий филантроп, который решил облагодетельствовать первого попавшегося с определенными критериями (фамилия, имя, возраст), под которые Вы, разумеется, «подходите». Далее наглый мошенник просит сразу денег, а более хитрый – подробные данные о Вас.

Относительно недавний тренд в **«нигерийских письмах»** - использование «брендов» государственных и правоохранительных органов. Например, в Латвии ряд адресатов получили письма якобы от американского ФБР. Которое будто бы раскрыло преступление злобных Интернет-жуликов, коварно покушавшихся на Ваши деньги в Интернете. Поэтому по той или иной причине (они могут разниться – чаще всего фигурировал возврат на Ваш счет якобы уже своровванных и перехваченных средств) от Вас требуется тот или иной объем персональных данных, иногда вплоть до номера счета. Подписано это электронное письмо ни много ни мало, а директором ФБР. Разумеется, то, что это полнейшая липа (вплоть до того, что жулики часто не знают настоящую фамилию директора ФБР США), лишний раз говорить не надо – и так ясно.

Самый главный совет по безопасности в связи с подобными письмами прост:

Нужно помнить, что ничейного богатства в Интернете не бывает, и возможности легко обогатиться подобным образом просто нет. Поэтому не надо гнаться за длинным рублем, долларом или евро и рассчитывать на собственную «синицу в руках». Иначе не только «журавль» не достанется, но и «синица» исчезнет – то есть Вы стопроцентно не разбогатеете, а вот часть своих нынешних денег потеряете гарантированно. ■

Электронное вымогательство

Да-да, в Интернете бывают не только мошенники, но и самые натуральные вымогатели. Которые не пытаются увести Ваши деньги обманом или хитростью, а нагло требуют перечислить Вам некую сумму – потому что «иначе будет хуже». Впрочем, мошенниками они тоже являются – так как после того, как получат от жертвы выкуп, обещанного все же не делают.

Где могут обмануть?

При установке «локера»

Разумеется, требование денег основано не на пустом месте. Сначала вымогатель **«заражает» или берет под контроль Ваше устройство** – будь то компьютер, ноутбук или смартфон. И вот за то, **чтобы** устройство вновь **разблокировалось** или вернулось под Ваше полное управление, он и **требует деньги.**

Программка, блокирующая удаленное устройство, называется **«локер».** Для пользователя результат ее работы выглядит примерно следующим образом. На экране появляется сообщение с примерно следующим текстом: «Внимание! Ваш компьютер заблокирован! Для разблокировки Вам следует перечислить такую-то сумму на такой-то электронный кошелек в течение такого-то времени! Иначе все Ваши данные с компьютера будут стерты! То же самое случится, если Вы начнете разблокировать компьютер самостоятельно!»

Впрочем, могут быть и варианты. Например, некоторые жулики пытаются **поставить пользователя в стыдную ситуацию** – то есть сделать так, чтобы ему было стыдно обращаться за помощью. При этом они могут «прикрываться» именем государственных структур. Например, на экране может появиться надпись от имени полиции, извещающая, что с Вашего компьютера якобы смотрели детскую порнографию, и потому Вам срочно нужно уплатить «штраф» - иначе Вас якобы посадят. Расчет здесь делается на то, что с такой надписью жертва в полицию не пойдет – а ну как та решит, что человек действительно смотрел детскую порнографию? Хотя, конечно, в России просмотр детской порнографии на данный момент не криминализован, но все равно могут посмотреть косо.

Надо сказать, что **иногда «локер» на самом деле ничего не «запирает»** и является всего лишь **всплывающим окном,** то есть жулик давит чисто психологически. Разобраться с такой проблемой проще простого – **кликнуть по окну или перезагрузить компьютер** (хотя жулики и стращают этого не делать).

Однако, к сожалению, гораздо чаще устройство блокируется по-настоящему. Далеко не факт, что через некоторое время оно запустит «программу стирания дисков», но то, что на устройстве больше работать нельзя – это есть.




Базовую защиту от «локеров» обеспечит **постоянно обновляемый антивирус.** Однако не надо думать, что антивирус – это панацея от всех компьютерных и мобильных бед. Многие действия, приводящие к заражению цифровых устройств, запускаются самим пользователем – и здесь нелишне помнить основные правила программно-технической безопасности. В частности, не открывать незнакомые файлы, слушаться рекомендаций антивируса (как бы ни хотелось добраться до вожделенного контента, который «злобный» антивирус не дает открыть) и сначала думать, а потом кликать. Те же рекомендации справедливы для любых программно-технических попыток добраться до Ваших паролей и денег на компьютерах и смартфонах, включая использование «троянских» программ.

Что можно сделать?

Платить вымогателям явно не следует.

Для них каждый лишний выход с Вами на связь – это **риск разоблачения**. Поэтому очень часто они получают с пользователя запрошенные деньги и…

оставляют его «при своих интересах». То есть с по-прежнему заблокированным устройством. Поэтому **лучше сразу обратиться к компьютерному мастеру.**

Не забудьте поставить антивирус на Ваше мобильное устройство!

Количество вредоносных программ для мобильных операционных систем растет в той мере, в которой мы все чаще совершаем финансовые действия с мобильных устройств. Поэтому, чтобы защититься от программно-технического вторжения в Ваш карман (в прямом и переносном смысле), нужно обязательно потратиться на антивирусную программу и регулярно ее обновлять. Это очень сильно повысит шансы Вашего кошелька – и цифрового, и обычного – на безопасность.

Если Вы все же стали объектом вымогательства, необходимо обратиться с заявлением в правоохранительные органы, так как деяния такого рода подпадают под признаки состава преступления, предусмотренного ст. 163 Уголовного кодекса Российской Федерации. ■

Мобильная безопасность

Мобильными телефонами сейчас в России пользуются практически все. Если взять количество действующих **мобильных номеров,** *то окажется, что на одного «экономически-активного» человека приходится примерно по два номера. В последние годы слово* **«мобильный телефон»** *становится синонимом слова* **«смартфон»** *- смартфоны становятся дешевле, и теперь их покупка не составляет проблемы даже для ограниченного бюджета. А значит, все больше и больше людей получают возможность выходить в Интернет из любого места, где есть сигнал – с улицы, из поезда или вообще из леса.*

Разумеется, преступники не могли оставить всеобщую «мобилизацию» населения без своего внимания. В результате общество сейчас сталкивается с двумя блоками «мобильных» проблем:

- **Проблемы, характерные для использования любого мобильного телефона;**
- **Проблемы, связанные с мобильным Интернетом.**

Где могут обмануть?

СМС-рассылки

Простейшие схемы «мобильной разводки» работают «наудачу». Преступники **массово рассылают СМС** типа «Маша, это я, Вася. Я попал в беду. Помоги мне, надо срочно 1000 рублей!». Разумеется, текст не строго такой, его исполнение зависит лишь от фантазии жуликов. Это может быть необходимость взятки инспектору ГИБДД, отсутствие денег на поезд в другом городе, «украденный кошелек» или… все, что угодно. Обычно жулики просят перевести им **деньги с Вашего мобильного счета**, хотя особо наглые могут попросить и **данные Вашей банковской карты.**

Смысл «разводки» в том, что жертва – если, конечно, ее зовут Маша - начинает гадать, что это за Вася такой. Скорее всего, почти у каждой Маши найдется относительно хороший знакомый по имени Вася. Маша мгновенно отождествляет Васю из СМС со своим знакомым из реала и тут же переводит ему запрошенную сумму. Не особо «заморачиваясь» тем, что СМС пришла совершенно не с Васиного номера – хотя на этот случай жулик подготовит «правдоподобное» объяснение: новый номер, старый не работает, номер друга… При этом Маша, видя свое имя в СМС, ни секунды не сомневается, что сообщение адресовано именно ей – а как же иначе, если написано «Маша» и пришло именно на ее номер? Значит, ей… Впрочем, имени получателя в просьбе может и не быть вообще – такое тоже бывает сплошь и рядом.

На самом деле такие рассылки жулики обычно делают «на кого Бог пошлет». **Из тысячи разосланных СМС примерно 50-60 по законам статистики попадут к людям с тем именем, которое мошенники используют в своей рассылке.** Из этих 50-60 некоторое число все-таки «купится» на столь настойчивую просьбу – все зависит от уровня цифровой грамотности получателей. Дополнительный расчет жулики делают и на небольшие суммы, которые обычно просят мошенники (1000 рублей – для такого способа многовато, обычно просят рублей по 200-300)

– дескать, даже при наличии некоторых подозрений жертва не будет особенно бояться расстаться с такой суммой. В итоге же – поскольку обманутая жертва далеко не одна - у мошенников образуется весьма немаленький капитал…

Вам может позвонить «взволнованный голос»

Он сообщит примерно то же – «голос» якобы попал в сложную жизненную ситуацию и потому вынужден просить помощи у других людей. Помощи, разумеется, денежной. Как вариант – позвонить на ту же тему от имени Вашего знакомого или родственника.

Разновидность «взволнованных голосов» - **вымогатели с программно-техническим инструментарием.** Вам точно так же может позвонить или написать случайный человек, и под неким предлогом попросить Вас ввести, допустим, логин и пароль от некоего Google-аккаунта. Вы введете – и злоумышленник, получив таким образом доступ к Вашему смартфону, тут же заблокирует Ваш телефон и потребует денег «за разблокировку». Причем во многих случаях, даже получив от Вас деньги, никто разблокировать телефон не будет. Отсюда рекомендация: посылайте с подобными просьбами «куда следует» (в службу поддержки или в полицию), если это не стопроцентно идентифицированный Вами близкий родственник. Подробнее об этом виде угрозы уже упоминалось в разделе «Электронное вымогательство».

СМС или звонок с информацией, что Вы получаете некий сногсшибательный бонус

Пожизненную подписку на некий сервис, новую онлайн-игру – опять же все зависит от фантазии жуликов, а с этим у них обычно полный порядок. Если жулик именно звонит, то он представится менеджером Вашего сотового оператора или какой-нибудь компании-партнера (банка, дистрибьютора игр и так далее). Далее Вам предложат совершить некие действия – которые на самом деле и интересуют злоумышленников. К примеру, Вам могут попросить отправить некий код на «короткий номер» - а СМС окажется стоимостью рублей в триста или больше. Короткий номер приобрести довольно легко, так что четырехзначный номер для отправки СМС – отнюдь не гарантия надежности «контрагента». Впрочем, жулики могут и прямо попросить Вас оплатить некую сумму за обещанный «бонус», а то и попросить Ваши персональные данные или данные банковской карты.

Вам может позвонить уже отнюдь не «взволнованный», а «очень строгий» голос

Он тоже представится работником сотовой компании или некоего сервиса, к которому Вы якобы подключились, и строго поведает Вам, что у Вас есть некий долг за услуги – который Вам надо срочно погасить. Для этого Вы будете должны опять же перевести куда-то некую сумму, иначе будут те или иные санкции вплоть до суда или запрета на выезд за границу. Бывают, конечно, случаи, когда мошенники представляются сотрудниками банков или коллекторами, но эта схема работает редко – человек обычно в курсе своих финансовых отношений с банками.

«Ошибочный перевод»

Схема довольно проста – Вам «прилетает» сообщение о пополнении Вашего баланса на некую сумму. Вскоре Вам напишет или позвонит некий человек, который скажет, что он ошибся при переводе денежных средств – набрал не ту цифру, и платеж якобы улетел на Ваш номер. А потому он просит вернуть ошибочно переведенную сумму, но не на тот номер, на который он якобы хотел перевести деньги, а на его собственный – причем не на тот, с которого Вам якобы поступил перевод.

Чаще всего сообщение о пополнении Вашего баланса является «липой», и никто на самом деле Вам никаких денег не переводил. А само сообщение пришло с постороннего номера – либо вообще с обычного, либо с короткого (который может быть «замаскирован» под название Вашего сотового оператора). Поэтому Вы, пойдя на поводу у мошенника, просто переводите ему свои деньги. Однако под влиянием роста цифровой грамотности абонентов мошенники тоже адаптируют свои схемы. Теперь они знают, что грамотный пользователь обязательно проверит свой настоящий баланс и историю переводов – к примеру, через свой «Личный кабинет» на сайте сотового оператора, благо смартфоны сейчас далеко не редкость. И придумали, как усыпить бдительность грамотных абонентов…

По новой схеме Вам придет уже не поддельное, а самое настоящее сообщение о переводе денег на Ваш мобильный. Вы проверите баланс, «Личный кабинет» - и действительно увидите совершенный перевод. По логике мошенника, Вы успокаиваетесь и возвращаете «ошибочно» переведенные деньги на указанный

мошенником номер. Однако все не так просто – получив от Вас перевод, мошенник тут же мчится в ближайший офис сотового оператора и подает заявление на возврат своего платежа. Сотовый оператор удовлетворяет просьбу, снимая эти деньги с Вашего аккаунта. Ведь он не знает, что Вы уже вернули эти деньги «в добровольном порядке»! В итоге, Вы «возвращаете» деньги дважды. Доказать же что-то в офисе сотового оператора при разборе дела вряд ли получится, так как Вы наверняка «вернете» деньги не на тот номер, с которого Вам был перевод. Поэтому лучший способ защиты – порекомендовать «ошибившемуся» самому обратиться в офис сотовой компании с заявлением на возврат ошибочного платежа. Для честного человека это никакой проблемы не составит, да и мошенник – если это все же он - останется «при своих».

Что можно сделать?

Если Вам «прилетело» подобное сообщение – не торопитесь делать все, что от Вас просят.

Для начала переберите в уме всех потенциальных знакомых с похожим именем. Затем ОБЯЗАТЕЛЬНО перезвоните им – но по тому номеру, который у Вас давно записан в телефонной книжке! И поинтересуйтесь, что у друга (подруги) за проблема и что происходит. Если друг не отвечает – не беда, можно поискать его в соцсетях, позвонить его близким или просто подождать. Но до прояснения ситуации **НИ В КОЕМ СЛУЧАЕ не переводить деньги!** 300 рублей, как известно, «не спасут гигантов мысли», а вот Ваш кошелек – вполне.

В случае звонка неизвестного попробуйте завязать разговор.

Если Вас мучает совесть, что рассказ неизвестного может быть и правдой – Выясните, какая именно проблема случилась, и поймите, как можно ее решить без перевода денег. Скажем, звонком родственникам. Предложите такой выход «взволнованному голосу». Если же он будет настаивать на деньгах, спросите просто: «Вам нужны деньги или помощь?»

Позвоните Вашему сотовому оператору по координатам, указанным на его официальном сайте, и поинтересуйтесь, что происходит.

Если у Вас действительно есть какой-то долг, то Вам о нем, разумеется, сообщат достоверную информацию – и решать возникшую проблему Вам следует именно

по достоверным координатам. Однако, скорее всего, никакого долга на самом деле нет, и Вас просто пытался атаковать очередной мошенник.

Сейчас существуют Интернет-справочники коротких номеров, которые Вам точно скажут, сколько в реальности будет стоит отправляемая на конкретный короткий номер СМС.

Если же Вам «позвонил менеджер сотовой компании», то лучше всего взять и позвонить в Вашу сотовую компанию по ее общеизвестному номеру.

И поинтересоваться у настоящего менеджера, есть ли в реальности обещанная Вам акция, спецпредложение или бонус. Если обещанное Вам – правда, то настоящий менеджер без проблем подключит Вам интересующую Вас опцию. ■

Безопасность персональных данных

Наши **персональные данные** *– это ключ ко многим нашим тайнам. Особенно в цифровом мире, с его мгновенностью, трансграничностью и относительной анонимностью. Именно поэтому защите персональных данных уделяется такое внимание в законодательстве многих стран, в том числе и в России.*

Персональные данные – это почти все, что может помочь нас идентифицировать. Это не только паспортные данные, но и то, что считается тайной личной жизни. Как известно, в «бесконтактном» цифровом мире нас идентифицируют именно по таким данным – так как в 99 процентах случаев «на другом конце провода» нас не видят. Поэтому знание некоторых элементов наших персональных данных может «открыть двери» злоумышленникам очень далеко – вплоть до наших банковских счетов.

С некоторыми примерами, «как это бывает», наши сограждане познакомились еще до того, как они вошли в нашу жизнь. Например, с **удаленной банковской идентификацией**. Ключевым ее элементом является кодовое слово, причем большинство пользователей выбирает его как ответ на весьма стандартный список вопросов, предлагаемый банком. Например, кличка собаки или название первой машины – а лет 30-40 назад вариант кодового слова был практически безальтернативен и представлял собой девичью фамилию матери клиента.

Где могут обмануть?

Размещение данных в социальных сетях

В условиях Web 2.0 добраться до такой информации злоумышленникам стало неизмеримо проще, чем это было 20-30 лет назад. Ведь сейчас **почти всю информацию о себе мы выкладываем в общий доступ в тех же социальных сетях.** Повальной модой стало выкладывание фотографий – как актуальных, так и исторических, с родителями, друзьями и подругами, домашними животными, детьми, с отдыха и работы, из ресторанов и с пляжей… При этом, **чтобы фотографии «говорили», мы, разумеется, их подписываем.** Скажем, фотография с любимым котом – «С Барсиком на диване».

А теперь представим себе злоумышленника, который пытается добраться до Вашего аккаунта на том или ином Интернет-сервисе. И, допустим, он доходит до той стадии, когда ему требуется ответить на «контрольный вопрос». Скажем, при «восстановлении пароля». Старательный Интернет-сервис спрашивает: «Кличка Вашей собаки?» Думаете, злоумышленник встает в тупик или начинает бессмысленно подбирать пароли? Да ничего подобного! Он идет на Вашу страницу в социальную сеть. И тщательно просматривает

всю Вашу публичную информацию. Среди которой ему на глаза попадается фотография Вас с собакой и с подписью для друзей: «С Тузиком на природе». Собственно, все – в этот момент **Вы сами открыли злоумышленнику доступ к своему аккаунту.** Вооруженный Вашей же информацией, он уверенно вводит ответ «Тузик» - и система его опознает как Вас, позволяя сменить пароль или прямо попасть в «аккаунт, где деньги лежат».

По сути, при помощи социальных сетей, а также блогов весьма легко составить Вашу полную анкету – не только узнать о дате Вашего рождения, но и узнать, где Вы живете и с какого периода, сколько людей проживает вместе с Вами (и даже когда они бывают дома), где Вы работаете и сколько времени проводите на работе, на чем Вы ездите на работу и в магазин. **Чекины** в различных местах вообще позволяют точным образом установить **Ваше местонахождение** без всяких радиомаячков. Все эти сведения интересны не только друзьям, но и злоумышленникам – особенно если они решат выдать себя за Вас при попытке добраться до Ваших денег. Или если они выбирают себе жертву для кражи, ограбления, автоподставы, а то и похищения ребенка.

Что можно сделать?

Меньше конкретных данных о своей жизни

Не публикуйте информацию, по которой можно определить Ваш домашний адрес и время, когда там никого не бывает;

Не размещайте в общем доступе посты о дорогостоящих покупках или сделках, в результате которых можно сделать вывод о наличии у Вас крупной суммы денег или ценностей, которые можно перепродать;

Не описывайте свой постоянный маршрут, пролегающий между домом и работой – нападения с целью ограбления не всегда бывают случайными;

Если очень хочется поделиться радостью от начинающегося отпуска, добавьте к сообщению приписку о включенной охранной сигнализации (даже если это не правда) – это наверняка отпугнет «продвинутых» любителей легкой наживы.

Доступ к своей странице в соцсети нужно ограничить

Его необходимо открыть только друзьям. Не «для друзей друзей», а именно «для друзей». При таком уровне приватности можно позволить себе выложить в Интернет несколько больше. Если же Вам нужен именно публичный аккаунт – то не нужно выкладывать туда элементы личной жизни. Никакие. И даже если Вы описываете там какие-то личностные элементы, относящиеся к Вашей публичной теме, тщательно подумайте – а не открываете ли Вы таким образом дорогу злоумышленнику. Разумеется, то же самое относится и к блогосфере, и к Твиттеру. Чекины же лучше не делать – безопаснее будет.

Лучше всего использовать псевдоним использовать в Интернете псевдоним

А объем персональной информации свести к минимуму – скажем, к контактам для связи. Никто не может гарантировать, что добросовестно введенные Вами персональные данные не будут использоваться против Вас. Их могут банально украсть вместе с десятками тысяч других. А может быть и ситуация, когда их будет «абьюзить» сам сервис – слать, например, тонны рекламы. Даже госорганы склонны использовать персональные данные граждан не для того, для чего эти данные изначально собирались – не говоря уже о том, с какой скоростью всякие базы данных «утекают» из своих законных хранилищ и затем начинают продаваться в Интернете или на радиорынках… ■

Дети и деньги в Интернете

Любые денежные отношения в Интернете в общем-то бесконтактны и в чем-то более анонимны. То есть при совершении некоторых действий – в Интернет-магазине или даже в Интернет-банке – **пользователя идентифицируют исключительно по тем данным, которые он ввел во время логина** *(входа в сервис). С одной стороны, это вроде бы менее анонимно, чем на улице – ибо мы все же «представились» сервису. Но с другой стороны, на «другом конце провода» наше лицо не видят. Раз человек ввел соответствующие пароли и коды подтверждения – значит, это он и есть. А, как мы знаем, в реальности это может быть отнюдь и не так…*

О том, что нужно прятать свои пароли, номера банковских карт и тому подобные сведения от посторонних, сейчас знают почти все Интернет-пользователи. Однако внутри семьи подобных тайн зачастую не бывает. И в результате все чаще бывают случаи, когда **«не посторонний» оказывается «посторонним».**

В первую очередь речь идет о детях. В отличие от взрослого, ребенок – даже подросткового возраста – слабее понимает ценность денег. Для несовершеннолетних деньги – это всего лишь нечто, что необходимо ввести, отдать, передать в обмен на некий товар или услугу. Казалось бы, «финансовую грамотность» должны поднимать различные компьютерные игры с «экономической составляющей» - где нужно приобретать что-то за игровые кредиты… Оказалось наоборот - **«игровое» отношение к кредитам в компьютере начинает переходить на настоящие деньги**, и приобретение товаров или услуг через Интернет начинает восприниматься детьми как разновидность игры.

А если ребенок, обиженный отказом родителей приобрести ему некую игрушку, вдруг решит купить ее самостоятельно, через Интернет?

Это отнюдь не фантастика. Еще пять лет назад в Англии трехлетний ребенок воспользовался аккаунтом дедушки и забрел на Интернет-аукцион. Как работает аукцион, маленький «вундеркинд» уже понимал, а вот что такое деньги – еще нет. В результате он, увидев очень детальную картинку экскаватора, от имени дедушки купил… настоящий экскаватор, приняв его за игрушку. Примерно в то же время еще один «юный гений» очень захотел игровую приставку и купил ее на онлайн-аукционе за огромную сумму, которой бы хватило на сотню таких приставок по магазинным ценам. Опять же, разумеется, из-под аккаунта взрослого. На этом фоне попытки американских подростков купить алкоголь через Интернет по папиной кредитке уже не кажутся чем-то сногсшибательным.

В связи с этим главное правило семейной финансовой безопасности должно быть таким:
ВСЕ, что ведет к деньгам и покупкам в Интернете, должно быть недоступно для детей.

Разумеется, обычные деньги родители – как правило – от детей прячут. А вот кредитные карты – зачастую нет. Поэтому ребенок может легко «подсмотреть» все необходимые данные карты и воспользоваться ими для Интернет-покупок. Скажем, «прокачать» своего героя в онлайн-игре, или купить все ту же игрушку в онлайн-магазине. Поскольку верификация платежа по СМС имеет место далеко не всегда (а в некоторых

случаях ребенок позаботится о том, чтобы увидеть код подтверждения на родительском мобильном), о покупке Вы узнаете только из СМС-ки о списании средств.

Еще более важно это правило для аккаунтов в Интернет-банках, Интернет-магазинах, онлайн-аукционах и прочих сервисах. Некоторые создают специальные онлайн-кошельки, в том числе привязанные к конкретным сервисам. В отличие от банковских карт, никакое уведомление о транзакции на мобильный телефон по ним не приходит. А вот доступ к личным кабинетам, как правило, довольно прост – за исключением разве что некоторых банков, которые уже начали верифицировать клиента по СМС уже при входе. **Если родители используют один и тот же пароль для всех (или большинства) своих онлайн-сервисов, то «домашний шпион» попадет в этот сервис довольно легко** – достаточно будет тем или иным образом узнать пароль дома. Из родительских разговоров, например, или просто стоя за плечом у папы-мамы. Не говоря уже о том, если пароль родители куда-то записали. Если же родители для разных сайтов используют разные пароли, то – с учетом того количества онлайн-сервисов, которые нас сейчас окружают – все эти пароли родители стопроцентно где-то запишут. Именно это «где-то» ребенок легко может найти. А уж **сохранять пароли на сайте – верх небезопасности**, здесь ребенку и делать-то ничего будет не надо: вошел и кликнул мышью.

Поэтому основное правило домашней Интернет-безопасности заключается в том, что…

ВСЕ пароли должны быть «под замком»

Если Вы записываете для памяти свои логины и пароли (хотя специалисты по инфобезопасности этого не рекомендуют, но реальность есть реальность), то они должны быть **стопроцентно вне досягаемости ребенка** и храниться там же, где наиболее важные документы и деньги. И, разумеется, ни в коем случае нельзя сохранять введенные пароли в браузере. Лучше потратить некоторое время на ввод сложного пароля, чем в один «прекрасный» день неприятно удивиться…

Это правило действует и для тех сайтов, в Ваших «личных кабинетах» на которых «живых» денег нет. Например, для Интернет-аукционов, про которые уже столько говорилось. Дело в том, что клик **«Покупка» на таких сайтах – это юридически обязывающее действие для кликнувшего**. Как только человек подтвердил покупку, он обязался приобрести товар или услугу по указанной цене. **Нарушение** этого правила **грозит санкциями** – от серьезной потери рейтинга до блокировки аккаунта и финансовых штрафов за отказ от сделки. Многое здесь зависит от контрагента – он может пойти навстречу, узнав, что «покупку» в реальности совершил ребенок, а может и не пойти – допустим, просто Вам не поверив («придумали, дескать, историю про ребенка,

а на деле просто передумали и теперь на жалость давят»). Но здесь Вы теоретически можете отделаться относительно «малой» кровью, если заказ еще не был оплачен (если был – то все хуже). Еще более неприятной ситуация может получиться, если речь идет об Интернет-магазине – здесь вступает в действие **закон о защите прав потребителей**. И по его положениям некоторые товары просто невозможно вернуть, а еще больше товаров не подлежат возврату в исправном состоянии. Хорошо, если Ваше чадо выбрало доставку и оплату на месте – есть шанс попытаться отменить сделку, а вот если оплата уже прошла – могут возникнуть сложности с возвратом товара.

Разумеется, ребенок вполне может совершать собственные действия через Интернет, предусматривающие небольшие денежные расчеты. Скажем, оплачивать доступ к видеоклипам или аудиофайлам.

Что можно сделать?

Лучше создать специальный аккаунт, доступ к которому будете иметь как Вы, так и ребенок.

И пополнять этот аккаунт следует со строгой периодичностью и на небольшие суммы – чтобы ребенок мог удовлетворять свои базовые потребности через онлайн и при этом не имел соблазнов «купить слона» в буквальном смысле.

Ни в коем случае не следует «привязывать» к детскому аккаунту собственные банковские карты и тем более настраивать какие-либо «автоплатежи»

Иначе Вы рискуете тем, что при быстром «обнулении» баланса стараниями ребенка банк будет исправно «поставлять» чаду все новые и новые порции Ваших денег, которые он будет упоенно тратить все быстрее и быстрее.

Прежде чем заводить такой аккаунт, чадо следует сначала обучить базовым правилам цифровой безопасности

Это нужно для того, чтобы ребенок не стал жертвой мошенников и тратил деньги только на действительно нужные ему вещи.

Что же касается денежных аккаунтов для детей в онлайн-играх – то данный вопрос обычно относится на усмотрение родителей: кто-то «подбрасывает» на счет немного денег, кто-то – нет, опасаясь лавинообразного расхода денег «на прокачки» персонажей. Решать, разумеется, только Вам. ■

Инвестиции

Интернет сегодня пестрит объявлениями о выгодных современных способах инвестирования.

Банковские вклады в последнее время перестали быть хорошим вариантом для формирования капитала. Они разве что позволяют сохранить деньги, сберечь их от кражи, но не получить реальный доход, так как депозитные ставки не компенсируют даже инфляции, то есть, по сути, стали отрицательными в реальном выражении. И, конечно, в такой ситуации на первый план выходят более выгодные биржевые инвестиционные инструменты и альтернативные варианты заработка.

Возможные риски

Потребителю финансовых услуг, не являющемуся профессионалом в инвестировании, нужно уметь разделять то, что действительно является современным инструментом, и то, что является мошенничеством (скажем, различные варианты финансовых пирамид), а также инвестиции, потенциально, может быть, и сулящие высокий доход, но сопровождающиеся высокими рисками.

К последним, к примеру, можно отнести рынок Форекс, слабо регулируемый законодательством и основанный на валютных спекуляциях. Чисто теоретически на Форексе можно заработать, только вот большинство непрофессиональных игроков теряют там свои деньги из-за работы с заемными средствами (с “финансовым рычагом”). Если вы решите обратиться к Форекс-брокеру, риски высоки: многие компании на этом рынке нацелены на то, чтобы «выжать» из клиента как можно больше денег и перейти к следующему, но не на то, чтобы принести клиенту реальную доходность.

Или еще один пример высокорисковых инвестиций - инвестиции в нынче модные микрофинансовые организации (МФО). Они обещают своим инвесторам как минимум 24% годовых (на длинных сроках инвестирования даже выше), однако сама суть микрофинансового бизнеса предполагает высокие риски невозврата капитала. МФО вкладывают деньги инвесторов в кредитование высоко-рискованных категорий заемщиков, которым банки, как правило, в ссуде уже отказали. При этом инвестировать в МФО предлагается довольно высокую сумму - от 1.5 млн рублей. «Порог входа» на рынок микрофинансового бизнеса высокий, и также высока вероятность потерять свои вложения.

Онлайн-работа на Бирже

По оценкам экспертов, в текущей экономической ситуации гораздо разумнее и правильнее инвестировать накопления в инструменты, торгующиеся на Московской Бирже. В отличие от того же Форекса, работа этот сегмент финансового рынка регулируется законодательством и регулятором (Центральным Банком), а значит инвестиции в биржевые инструменты по определению уже более надежны.

Тем более, что законодательство сегодня идет по пути упрощения работы частных лиц на фондовой площадке. Так, россияне смогут получить удаленный доступ к биржевым

инструментам. Дело в том, что уже совсем скоро большинство российских брокеров получат возможность заключать договоры дистанционно, без личной явки клиентов. Для этого брокеры должны быть подключены Минкомсвязью к Единой системе идентификации и аутентификации (ЕСИА). По данным НАУФОР и Московской Биржи, с 15 октября к ЕСИА уже подключились первые семь компаний. Остальные – в процессе.

ЕСИА — это система, созданная «Ростелекомом» для портала госуслуг, через который россияне не первый год успешно оплачивают штрафы, налоги, оформляют документы, а также получают другие категории госуслуг. На сегодняшний день на портале зарегистрировано более 17 млн пользователей. При этом, система поддерживает различные методы аутентификации: можно ввести пароль или электронную подпись. Также возможна двухфакторная аутентификация - по постоянному паролю и одноразовому паролю, высылаемому в виде СМС-сообщения.

В связи с тем, что идентификация россиян на госуслугах происходит при регистрации, для тех, кто уже есть в ЕСИА, будет проводится упрощенная идентификация брокером. Кроме того, через онлайн-счет они будут переводить средства с банковского счета, то есть еще будут идентифицированы банком.

По оценкам экспертов, уже до конца года будет открыто 10-20 тыс брокерских счетов дистанционно. Подобная процедура будет особенно востребована жителями мегаполисов, нацеленных на экономию времени.

Безопасные инвестиции

Безопасные инвестиции - это инвестиции в надежные активы, причем, инвестиции диверсифицированные (по инструментам, активам, валютам, странам) и сбалансированные.

Обеим этим характеристикам удовлетворяет такой финансовый инструмент как биржевой индексный фонд (ETF), который представляет собой диверсифицированный европейский фонд, акции которого свободно торгуются на Московской Бирже. Во-первых, этот инструмент очень ликвидный - продать и купить его легко в любой момент времени через брокера, комиссии минимальны. Во-вторых, ETF - диверсифицированный инструмент. Структура ETF повторяет структуру выбранного базового индекса (списка акций с определенными весами). Это позволяет инвестору получить гарантии того, что фонд не проиграет соответствующему индексу с поправкой на комиссии. По

статистике, 80–90% активно управляемых взаимных фондов (если вы, скажем, решите инвестировать в ПИФы) не дотягивают до индексов по доходности, таким образом, индексные фонды максимально защищают инвестора от ошибок управляющих, обеспечивая автоматическую диверсификацию за счет вложения в широкие индексы. Таким образом, данный инструмент подходит как для профессиональных инвесторов и трейдеров, так и для начинающих.

На Московской Бирже представлена линейка из 11 ETF:

- • ETF акций – фонды, основанные на страновых индексах наиболее крупных и интересных экономик – США, Германии, Великобритании, Китая, Японии, Австралии;

- Фонды корпоративных еврооблигаций российских эмитентов;
  Золотой ETF;

- Максимально надежный фонд денежного рынка США (FXMM).

Сформировать портфель из ETF можно на Московской Бирже, обратившись к брокеру, а перед этим можно воспользоваться робо-эдвайзером «Финансовый автопилот», который позволит собрать инвестиционный портфель, «заточенный» под ваш риск-профиль (ваше отношения к рискам), ваши ожидания по доходности и ваши цели. «Финансовый автопилот» не просто предложит вам наиболее подходящие фонды, но сформирует из ряда инструментов сбалансированный портфель и распишет подробно его структуру и доходности. Очень удобно, наглядно и просто. ■

БЕЗОПАСНЫЙ ИНТЕРНЕТ

КРАТКИЙ КУРС

РОЦИТ

Ознакомиться с материалом можно на сайте

www.mindex.rocit.ru

РОЦИТ

Горячая линия Рунета

Вы столкнулись с информацией, которая нарушает ваши права и ограничивает вашу свободу

Вы пострадали от некачественного предоставления услуг в сети Интернет

Вы стали жертвой противоправного контента, который нарушает законодательство Российской Федерации

hotline.rocit.ru

Что делать?

Сформировать заявление на сайте Горячей линии Рунета, с прикреплением всех необходимых удостоверяющих материалов и документов.

Чего ждать?

Горячая линия — это сервис защиты и поддержки пользователей Рунета. Мы оказываем информационно-консультационную поддержку и помогаем строить и контролировать диалог между пользователем, столкнувшимся с угрозой в Сети, организациями и государственными органами, которые помогут с решением проблемного вопроса.

Горячая линия

Региональный Общественный Центр Интернет-Технологий, 2015 г.