Тема 4. Потребительские аспекты информационной безопасности.

Содержание:

1. Электронные деньги и банковские карты.
2. Сетевое мошенничество.
3. Онлайн-игры.
4. Спам.
5. Пользовательское соглашение.
6. Государственные услуги в интернете.

ПОТРЕБИТЕЛЬСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В данной теме будут рассмотрены аспекты получения и приобретения различных товаров и услуг в сети «Интернет».

ЭЛЕКТРОННЫЕ ДЕНЬГИ И БАНКОВСКИЕ КАРТЫ

В Интернете можно осуществлять покупки с банковских карт и с помощью электронных денег.

Электронные деньги - это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Обычно сервисы электронных денег предлагают клиентам анонимные и неанонимные аккаунты. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной. Зачастую анонимные аккаунты имеют существенные ограничения в свой работе.

Также следует различать электронные фиатные деньги, равные государственным валютам, и электронные нефиатные деньги, которые в свою очередь не равны государственным валютам.

В Интернете можно также расплачиваться банковскими картами, которые обычно разделяют на:

– ***Зарплатные карты.*** Их открывает банк по указанию предприятия, которое будет осуществлять выплату заработной платы, аванса, премий, отпускных, командировочных, социальных пособий, положенных работнику;

– ***Кредитные карты.*** Они имеют денежные средства, принадлежащие банку и предоставленные в качестве кредита. Эти деньги предоставляются на определенных условиях и на конкретный срок, в том числе в пределах выделенного лимита;

– ***Дебитовые карты.*** Они открываются для использования и расчетов собственными средствами. На них не установлено кредитного лимита, поскольку клиенту доступен баланс в размере внесенных им денег.

Банковские карты содержат следующую информацию на фронтальной стороне:

1) Уникальный номер карты, состоящий из 16 цифр;
2) Имя и фамилию владельца карты;
3) Срок действия карты в формате месяц/год;

На обратной стороне размещены контакты банка, который выдал карту, и в зависимости от вида карты специальные защитные элементы:

– Магнитная лента черного цвета хранит в зашифрованном виде ключ доступа к счету владельца карты;

– Посола подписи содержит подпись владельца карты;

– Защитная голограмма гарантирует подлинность банковской карты;

– Специальный код безопасности CVC2, который состоит из трех символов.

Многие банковские карты содержат специальный чип, а оплата по ним возможна только введения PIN-кода (пароля). Сейчас особой актуальностью пользуются карты с использованием технологии бесконтактной оплаты, позволяющие оплатить покупку без введения PIN-кода.

Важно помнить, что для покупок в Интернете зачастую достаточно знать только номер карты и срок ее действия, чем очень часто и пользуются злоумышленники.

Сервисы электронных денег и банки предоставляют возможность привязки к счету мобильного телефона, что позволяет не только восстановить доступ к счету или карте, а также подтверждать платежи (транзакции) с помощью одноразового пароля. Однако, необходимо в таком случае особенно помнить о безопасности устройства, а в случае его утери необходимости сообщить банку о его потере для блокировки счета.

Чтобы избежать проблем при использовании карт и электронных денег в сети рекомендуется:

– Для покупок в Интернете иметь специальную карту или специальный счет электронных денег, на которую можно переводить определенную сумму денег с основной карты или счет только для совершения конкретных транзакций;

– Использовать одноразовые пароли, которые приходят на номер телефона каждый раз перед оплатой, и в случае их отсутствия платеж не происходит;

– Не сообщать номер карты другим людям и хранить банковскую карту в надежном месте, в том числе нельзя держать пароли и коды рядом с картой. Никогда нельзя терять из виду карту, когда передаете ее кассиру или официанту;

– Подключить услугу SMS-уведомлений, чтобы получать сведения о всех совершаемых платежах с карты или счета;

– Регулярно просматривайте в интернет-банке или аккаунте историю выполненных операций и остаток на карте;

– Вводить номер карты и срок ее действия только на проверенных сайтах, которые необходимо самостоятельно изучить перед введением данных и соответствующие следующим требованиям:

– Аккредитованные сайты, на которых отображены логотипы Verified by Visa, MasterCard SecureCode и «МИР».

– Подтверждение платежа паролем должно осуществляться на странице банка или сервиса платежей;

– Использующие защищенный протокол https.

– Использовать специальные программы для интернет-платежей, разработанные производителями антивирусных программ.

Что делать, если:

1) Потеряна банковская карта. Сообщить по телефону в банк о произошедшем и попросить ее заблокировать. Банк предложит вместо данной

карты выпустить новую карту с новым номером. Пока не будет заблокирована банковская карта, любой, у кого она окажется в руках, сможет воспользоваться ей;

2) Пришло уведомление о платеже, который вы не совершали. Необходимо сообщить в банк или платежный сервис, направив заявление о чарджбеке (отмене операции), в котором максимально подробно описать произошедшее. Банк или платежный сервис рассмотрит обращение и вернет вам деньги в срок от 30 до 60 дней.

Важно помнить, что чем раньше удастся выявить проблему и начать предпринимать меры, то тем больше шансов уменьшить ущерб, который может быть нанесен вам, вашей семье и другим лицам.

ПОКУПКИ В СЕТИ

Сегодня в интернете можно купить буквально все и как в реальной жизни можно столкнуться с различными негативными последствиями.

Сайты предлагают различные товары и различные услуги, которые предоставляются как в реальной жизни, так и виртуально, например, можно купить смартфон или игровую валюту.

В основном вся работа с подобными сайтами заключается в следующем: оформление заказа, оплата заказа и доставка, которая может осуществляться путем добавления в личный кабинет, например, в игре или доставка на дом товара.

В первую очередь необходимо обратить внимание на устройство, с которого будут осуществляться платежи. Рекомендуется использовать только личное персональное устройство, например, домашний компьютер, смартфон или планшет, имеющий:

– Включенное антивирусное программное обеспечение;

– Актуальную версию операционной системы и браузера;

Не рекомендуется оплачивать, проверять баланс счета и проводить другие финансовые операции на компьютерах с общим доступом и устройствах, подключенных к публичным точкам доступа WiFI.

Сайты и сервисы для защиты своих клиентов при оплате онлайн используют протокол HTTPS, который можно увидеть в адресе платежной страницы в браузере, зачастую отмечаемый замком зеленого цвета. Только этот протокол обеспечивает безопасную передачу данных, поэтому рекомендуется оплачивать только на сайтах и сервисах, использующих данный протокол.

Закон Российской Федерации от 07.02.1992 № 2300-1 «О защите прав потребителей» устанавливает ряд обязательных требований к продавцам в интернете. При продаже товара дистанционным способом продавцом должна быть до продажи покупателю предоставлена следующая информация:

– об основных потребительских свойствах товара. Данная информация должна позволить потребителю определить, какой именно товар ему необходим;

– цену в рублях и условия приобретения товаров (работ, услуг), в том числе при оплате товаров (работ, услуг) через определенное время после их передачи (выполнения, оказания) потребителю, полную сумму, подлежащую выплате потребителем, и график погашения этой суммы;

– каков его состав, последствия его применения (употребления) и т.п. В случае если потребителю оказалось недостаточно представленной информации, то он вправе обратиться к продавцу с просьбой представить ему дополнительные сведения;

– об адресе (месте нахождения) продавца, при этом должен быть указан как адрес фактического места нахождения продавца, так и его юридический адрес, номер телефона, факс, электронный адрес. Наличие такой информации позволит потребителю в дальнейшем в случае необходимости быстро связаться с продавцом;

– о месте изготовления товара. Место изготовления товара – это не только страна-изготовитель, но также город, адрес (место нахождения) изготовителя. Такая информация должна быть доведена до потребителя доступным ему способом, например, закодированная информация в виде штрих-кода не может рассматриваться как факт представления информации о месте изготовления потребителю;

– о полном фирменном наименовании продавца (изготовителя). Такая информация фактически дополняет информацию о месте нахождения продавца (изготовителя) и также имеет своей целью обеспечить потребителю более быстрое обращение к продавцу (изготовителю) в случае возникновения такой необходимости;

– о условиях приобретения товара. Данная информация является одной из важнейших составляющих, однако продавцы нередко в целях привлечения большего числа покупателей указывают стоимость товара без учета налогов или без учета почтовой доставки. Сведения об этом приводятся, как правило, мелким шрифтом либо в менее заметных местах рекламного проспекта, каталога. Нередки случаи, когда на товар из каталога предоставляются значительные скидки, однако при этом где-нибудь в незаметном месте указывается, что рекламная кампания действует в течение ограниченного срока;

– о его доставке. Данный пункт может иметь важное значение, если продавец находится не в месте нахождения потребителя. В этом случае следует тщательно проверить условия доставки товара, входит ли условие о доставке товара в общую стоимость заказа или потребителю придется оплачивать доставку отдельно. При этом может также играть роль удаленность населенного пункта, в котором находится покупатель, от места нахождения продавца. В ряде случаев доставка товара является дополнительной услугой, и покупатель должен дополнительно сообщить о необходимости доставки продавцу. Если потребитель не сделает этого своевременно, то рискует взамен товара получить сообщение, что принадлежащий теперь покупателю товар он может получить в определенном (не всегда удобном для него) месте;

– о сроке службы, сроке годности и гарантийном сроке. Сведения, перечисленные в данном пункте, должны быть представлены потребителю до заключения договора купли-продажи. Таким образом, до приобретения товара потребитель должен узнать из информации, полученной от продавца, установлен ли на выбранный товар срок службы, срок годности или гарантийный срок, какова его продолжительность, где находятся сервисные центры;

– о порядке оплаты товара. Продавцом должна быть определена прежде всего форма оплаты: денежный перевод, наличные денежные средства в кассу и т.д. При этом продавец вправе самостоятельно выбрать наиболее приемлемую для него форму оплаты товара или предоставить ее выбор на усмотрение потребителя. Кроме того, должно быть определено, необходима ли предоплата или можно оплатить товар по факту его получения. Если речь идет о предоплате, то продавец вправе предусмотреть как полную, так и частичную предоплату. Подробная информация об этом также должна быть предоставлена покупателю;

– о сроке, в течение которого действует предложение о заключении договора. Если продавец не представил покупателю информацию о сроке действия его предложения, то считается, что оно действует неопределенный срок, при этом именно на тех условиях, которые стали покупателю известны из рекламного проспекта, каталога и т.п.

Вся вышеизложенная информация должна быть также предоставлена покупателю в момент доставки товара в письменной форме, а также предоставлены в письменной форме сведения о порядке и сроках возврата товара.

При выборе сайта или сервиса, на котором планируется что-либо приобрести, также рекомендуется:

– Сравнивать цены в различных сайтах и сервисах;

– Ознакомиться с отзывами покупателей данного сайта или сервиса;

– Избегать предоплаты;

– Уточнить возможность подать жалобу или/и отменить заказ;

– Проверять реквизиты, название сайта или сервиса и информацию продавце (как о физическом или юридическом лице);

– Проверить историю сайта или магазина, в частности через поисковые системы либо по дате регистрации домена.

Если сайт или сервис не соответствует вышеуказанным требованиям, то лучше исключить возможность покупки на нем.

Особенно рекомендуется обратить внимание и избегать сайты и сервисы:

– продающие технику, на которой отсутствует русификация. Это является одним из признаков контрабандного товара либо оборудование уже на заводе не планировалось поставлять в Россию;

– использующие для приема платежей электронные кошельки, поскольку такие сервисы предоставляют возможность принимать платежи сразу после регистрации, указав только электронную почту. E-mail нельзя отследить, что сказывается на отсутствие возможности установить личность продавца;

– которые не имеют пунктов самовывоза или своих офисов.

До покупки необходимо ознакомиться с правилами сайта или сервиса и условиями покупки. Зачастую пользователи не знают о таком праве сайтов как распространять информацию о покупках своих клиентов публично, а многие сервисы предоставляют пробный бесплатный период, по окончании которого включается подписка на платные услуги с автоматическим продлением, от которой сложно отказаться.

Во время покупки или для ее подтверждения администраторы или модераторы сайта или сервиса не могут требовать полные данные счета, пароли и пин-коды для подтверждения платежа. Если кто-то запрашивает подобные данные, то, скорее всего, это мошенники.

После покупки все сайты и сервисы обязаны предоставить пользователю электронный чек, который можно как скачать, так и отправить на адрес электронной почты или смс-сообщением покупателю. В чеке обязательно публикуется следующая информация:

1) наименование документа;

2) порядковый номер за смену;

3) дата, время и место (адрес) осуществления расчета, а также адрес сайта;

4) наименование продавца: наименование организация или фамилия, имя, отчество (при наличии) индивидуального предпринимателя;

5) идентификационный номер налогоплательщика продавца;

6) применяемая при расчете система налогообложения продавца;

7) наименование товаров, работ, услуг, цена за единицу с учетом скидок и наценок;

8) форма расчета (в безналичном порядке) и сумма оплаты в безналичном порядке;

9) адрес сайта уполномоченного органа в сети "Интернет", на котором может быть осуществлена проверка покупки;

10) абонентский номер либо адрес электронной почты покупателя;

11) адрес электронной почты отправителя кассового чека;

12) QR-код.

Согласно закону у покупателя имеется возможность отказаться от товара в любое время до его передачи, а после передачи товара – в течение 7 дней. В случае если продавцом в момент доставки товара не была предоставлена информация в письменной форме о порядке и сроках возврата товара надлежащего качества, то потребитель имеет право отказаться от товара в течение трех месяцев с момента передачи товара.

В этой связи особо важным обстоятельством при покупках в сети является сохранение чеков, отчетов об оплате и доставке товаров, которые получает покупатель после покупки.

В зависимости от наличия недостатков в приобретенном товаре можно выделить две возможных ситуации, в которых процесс возврата товара будет отличаться:

– возврат товара, в котором нет недостатков, т.е. товара надлежащего качества;

– в товаре обнаружены недостатки, т.е. передан товар ненадлежащего качества.

Потребитель вправе отказаться от товара, в котором не было обнаружено недостатков, в течение 7 дней с момента получения товара. При этом причины возврата законом не устанавливаются, то есть они могут быть любыми. Важно запомнить, что возврат товара надлежащего качества возможен в случаях, если сохранены его товарный вид, потребительские свойства и документ, подтверждающий факт и условия покупки товара у продавца. В случае если по каким-либо причинам документ, подтверждающий факт покупки товара, у потребителя отсутствует, это не лишает его возможности ссылаться на другие доказательства приобретения товара (свидетельские показания, распечатки с интернет-сайтов и др.).

Также необходимо помнить, что не все товары можно вернуть как товар надлежащего качества – нельзя отказаться от товара, имеющего индивидуально-определенные свойства. Это означает, что данный товар был сделан индивидуально для потребителя, и только он может его использовать. Например, изготовление обуви по меркам, которые предоставлены индивидуально, конкретным потребителем. Продавец возвращает покупателю денежную сумму, уплаченную за товар, за исключением расходов продавца на доставку от покупателя возвращенного товара. Возврат денежных средств осуществляется в течение 10 дней с момента предъявления такого требования.

В случае если потребителю был передан товар ненадлежащего качества, т.е. в нем имеются какие-либо недостатки. Потребитель имеет право на предъявление следующих требований:

– безвозмездное устранение недостатков;

– соразмерное уменьшение покупной цены;

– замена на товар аналогичной марки либо на товар другой марки с соответствующим перерасчетом покупной цены;

– отказ от исполнения договора и возврат денежных средств, уплаченных за товар.

СЕТЕВОЕ МОШЕННИЧЕСТВО

С развитием сети интернет его стали осваивать и мошенники.

Злоумышленники могут использовать различные методы социальной инженерии (угрозы, шантаж, игру на чувствах жертвы — например, жадности или сочувствии), чтобы выманить деньги и получить личные и конфиденциальные данные: к таким данным относятся логины и пароли от различных сервисов, в том числе банковских, номера и пин-коды банковских карт и другие персональные данные.

Сетевое мошенничество имеет множество методов.

Фишинг (англ. phishing, от fishing — рыбная ловля, выуживание) предполагает за счет использования различных методов заманивания пользователя на поддельный сайт, например, через ссылку в письме, баннер или ссылку в тексте.

Иногда вредоносная ссылка маскируется под правильную ссылку – так злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение с помощью опечатки в адресе сайта, или сайты, копирующие интерфейс известных ресурсов.

Примеры: http://www.sberbank.ru/ и http://www.sbenbank.ru/ либо www.yandex.ru и www.yadndex.ru .

На подобных сайтах пользователю предлагается ввести логин и пароль или данные счета, после чего зачастую происходит перенаправление на реальный сайт, но данные уже попадают в руки мошенников.

Вишинг является разновидностью фишинга, в которой используется телефон. Мошенник может позвонить и представиться сотрудником банка или платежного сервиса и попросить продиктовать какие-либо платежные данные, например, пароль или код, пришедший на телефон. Его цель – выманить платежные данные, с помощью которых можно украсть деньги с карты или кошелька. Часто дополнительно присылается СМС со ссылкой, которая ведет на фишинговый сайт.

Фарминг или скрытое перенаправление является также разновидностью фишинга, но направляет пользователя вирус или взломанная программа на поддельный сайт, являющийся полной копией официального ресурса.

Сетевое мошенничество имеет также множество видов, в частности:

– Липовые акции и фальшивые выигрыши в лотереи. Пользователь может получить сообщение (по телефону, почте или SMS), что выиграл некий приз, а для его получения необходимо «уплатить налог», «оплатить доставку» или просто пополнить какой-то счет. Признаки фальшивой лотереи: пользователь никогда не принимал участие в лотерее; пользователь никогда не оставлял своих

личных данных на этом ресурсе; почтовый адрес отправителя – общедоступный почтовый сервис, например, gmail.com, mail.ru, yandex.ru;

– Просьба «друзей» сообщить пароль, когда знакомый в социальной сети сообщает о потере телефона, просит напомнить ваш номер, вам приходит SMS с неким кодом, а тот же друг в социальной сети сообщает, что заказывает товар или регистрируется на сайте и случайно указал ваш телефон вместо своего. Он просит сообщить пришедший код. Таким образом, ваш номер будет подключен к платной подписке и с вас начнут списывать деньги;

– Ложная блокировка аккаунта в социальной сети: на баннере подробно расписан вариант «спасения» от блокирования страницы в социальный сети, который включает отправку SMS на «короткий» номер или введение кода подтверждения. В первом случае происходит разовое списание денег, а во втором оформляется ежедневная подписка на какую-либо платную услугу;

– Рекламные сообщения и баннеры о необходимости обновления браузера имеют риск подписаться на платную загрузку или получить вирус с архивом платной программы;

– Бесплатное скачивание файлов и просмотр каких-либо файлов с подпиской по номеру телефона, после чего включится подписка и с указанного номера могут начать списываться деньги;

– Пользователю предлагается бесплатный антивирус, под видом которого на устройство попадет вредоносная программа, либо создается иллюзия, что компьютер уже заражен и для уничтожения угрозы нужно воспользоваться специальным антивирусом, который, опять же, окажется вирусом. Примером является появление надписи на экране компьютера о блокировке операционной системы, устранить которую можно только при отправке SMS с кодом, пришедшим на телефон при подтверждении, – после чего запускается сам вирус;

– Предложения очень выгодных покупок, реклама больших скидок или анонс распродаж, которые размещаются на сайтах, в социальных сетях и присылаются смс или на электронную почту. Такие предложения обычно предполагают перевод денег на банковскую карту, электронный кошелек или мобильный номер. В настоящее время стала актуальна следующая разновидность данной угрозы – пользователям рассылаются на оплату мобильного телефона, домашнего интернета, ЖКХ и т.д. Зачастую мошенники направляют поддельные квитанции раньше официальной даты оплаты, чтобы успеть собрать свои платежи;

– Мошенник может попросить денег в долг под видом знакомого, например, через взломанный аккаунт в социальных сетях. При этом перевести деньги он может попросить любым удобным способом – на электронный кошелек, банковскую карту, через интернет-банк.

Фишинговые сообщения могут содержать:

– сведения, вызывающие тревогу, или угрозы, например, закрытие ваших банковских счетов;

– обещания большой денежной выгоды с минимальными усилиями или вовсе без них;

– сведения о сделках, которые слишком хороши для того, чтобы быть правдой;

– запросы о пожертвованиях от лица благотворительных организаций после сообщений в новостях о стихийных бедствиях;

– и другую информацию.

Отдельным подвидом необходимо рассматривать мобильное мошенничество, которое в частности предполагает получение смс-сообщений с незнакомых номеров, которые могут содержать:

– ссылки на фишинговые или зараженные ресурсы;
– информацию о выигрышах, которых не существует;
– ложные просьбы о помощи;
– о переводе денег на сотовый, прямые просьбы о переводе денег;
– SMS из несуществующего банка;
– просьбы перезвонить на платный номер;
– требования выкупа;
– просьбы отправить СМС, которые активируют платные услуги;
– и другую информацию.

Мобильное мошенничество также часто встречается в формах:

– Wangiri («Очень дорогой звонок») – когда человек звонит с неизвестного номера, но, как только человек берет трубку, звонок внезапно обрывается. Вы перезваниваете на неизвестный номер и попадаете на автоинформатор, задача которого – как можно дольше удержать абонента на линии, пока со счета списываются деньги;

– Требования выкупа – когда кто-то звонит вам с неизвестного номера, но, как только вы берете трубку, звонок внезапно обрывается. Вы перезваниваете на неизвестный номер и попадаете на автоинформатор, задача которого – как можно дольше удержать абонента на линии, пока со счета списываются деньги. Когда вам позвонили или прислали SMS с неизвестного номера с просьбой о помощи близкому человеку: не впадайте в панику, не торопитесь переводить деньги. Перезвоните родным и узнайте, все ли у них в порядке. Уточните, где находятся близкие.

Мобильное мошенничество имеет примеры смежных технологий: пользователю может прийти SMS от банка или платежного сервиса с паролем для совершения платежа, а сразу после этого может позвонить человек, который скажет, что ввел этот номер мобильного телефона по ошибке и попросит сообщить код из SMS, которое только что пришло пользователю. На самом деле код из SMS — это пароль не к счету незнакомца, а к счету пользователя, с помощью которого злоумышленник может поменять настройки кошелька или интернет-банка, украсть деньги и т.д.

Особо актуальной проблемой в сфере сетевого мошенничества стало стремление злоумышленников получить доступ к аккаунтам жертвы, например, в социальных сетях, почтовых и других сервисах. Украденные аккаунты они используют, например, для распространения спам-писем и вирусов. Мошенники могут получить доступ к учётной записи жертвы следующими способами:

– Заставить жертву ввести свои данные на поддельном сайте;
– Подобрать пароль жертвы, если он не является сложным;
– Восстановить пароль жертвы с использованием “секретного вопроса” или введенного ящика электронной почты;
– Перехватить пароль жертвы при передаче по незащищенным каналам связи.

Какие меры помогут бороться с мошенничеством в сети?

– Внимательно проверять доменное имя сайта и особенно доменные имена сайтов, на которых вводятся учетные данные.

– Использовать проверенные и безопасные веб-сайты, в том числе интернет-магазинов и поисковых систем. Использовать закладки в браузере часто посещаемых сайтов.

– При переходе по ссылке из сомнительных источников, в частности e-mail, форумы, сообщения в социальных сетях и всплывающие окна, вы рискуете попасть на «фишинговый сайт».

– Помнить, что платежные сервисы и банки никогда не рассылают сообщения о блокировке счета по электронной почте, а также никогда не просят сообщать – ни по почте, ни по телефону – пароль, пин-код или код из SMS. Нельзя переходить по ссылкам из таких писем и вводить свои пароли на посторонних сайтах, даже если они очень похожи на сайт банка или платежного сервиса.

– Не указывать свой мобильный номер на незнакомых сайтах.

– Не переходить по ссылкам в сообщениях электронной почты и сообщениях из социальной сети.

– Не размещать личную информацию в интернете. Даже маленькие кусочки личных данных могут быть использованы в преступных целях.

– Никому не сообщать не сообщать пароли, пин-коды и коды из SMS, которые приходят на мобильный номер от банков, платежных сервисов, мобильных операторов и других организаций.

– Не поддаваться на провокации злоумышленников, например, с требованием перевести деньги или отправить SMS, чтобы снять блокировку компьютера.

– Не открывать файлы и другие вложения в письмах, даже если они пришли от друзей и знакомых. Необходимо уточнить у них, отправляли ли они эти файлы.

– Не доверять объявлениям о подозрительно дешевых товарах, акциях и распродажах на малознакомых сайтах. Перед покупкой необходимо прочитать отзывы в интернете о сайте или частном продавце, а в случае их отсутствия отказаться от покупки.

– Проверять реквизиты, указанные в платеже перед оплатой. Если они не совпадают с заявленными ранее, то отказаться от покупки.

– Настроить онлайн-платежи на заранее проверенные реквизиты (авто-платежи).

– В случае просьб от друзей и знакомых о деньгах необходимо лично перезвонить и уточнить необходимость в помощи, а в случае отсутствия возможности позвонить, задать какой-либо проверочный вопрос, ответ на который может знать только данный человек.

Что делать если уже возникли проблемы?

– Если СМС-подписка была оформлена, то необходимо обратиться по телефону в службу поддержки оператора и попросить отключить её.

– Если аккаунт был взломан, то необходимо заблокировать аккаунт, сообщить администрации сайта о взломе, поменять пароль к сайту, а также предупредить всех своих знакомых о том, что произошел взлом и, возможно, от вашего имени будет рассылаться спам и ссылки на фишинговые сайты.

– Если деньги или другие важные данные вашей банковой карты были предоставлены неизвестным лицам, то необходимо как можно быстрее обратиться в банк для блокировки карты и возврата средств.

ОНЛАЙН-ИГРЫ

Современные онлайн-игры - это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт.

Игры разделяют на следующие категории:

– Платные – доступ к самой игре осуществляется после оплаты единожды либо согласно лимиту (день, неделя, месяц и т.д), а сама игра не содержит платных дополнительных услуг и предложений;

– Бесплатные – доступ к игре предоставляется бесплатно, а сама игра не содержит платных дополнительных услуг и предложений;

– Условно-бесплатные: доступ к игре предоставляется бесплатно, однако игра содержит платные дополнительные услуги и предложения (например, улучшить ваш персонаж или получить какие-либо игровые привилегии) за счет внесения реальных денег.

При этом важно понимать цель игр платных и условно-бесплатных – получение прибыли. Однако полученные средства разработчиками игр также идут на поддержание и развитие игры, а также на совершенствование системы безопасности: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов. Кроме этого, на полученные средства нанимаются разработчики и специалисты, осуществляющие в частности поддержку пользователей.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности своего игрового аккаунта:

- Если другой игрок создает неприятности, оскорбляет и нарушает своим поведением правила игры, заблокируй его в списке игроков и сообщи в администрацию о поведении данного игрока, в том числе со скринами. Такое действие позволяет администрации игр находить подобных игроков и исключить их из игры, что обычно предусмотрено правилами каждой игры для развития самой игры – ведь никто не будет играть в игру, когда в ней имеются такие игроки;
- Не рекомендуется указывать личную информацию о себе в аккаунте и распространять ее среди других игроков, поскольку она может привести к различным негативным последствиям в реальной жизни;
- Необходимо соблюдать правила игры и уважать других игроков, в частности создавать неприятности и оскорблять их;
- Во время игры не стоит отключать антивирус, поскольку во время игры компьютер, смартфон или планшет может быть заражен;
- Необходимо всегда контролировать потраченное в игре время и деньги, поскольку это позволяет оценить свои действия корректно;
- Нельзя приобретать дополнения к играм, оплачивать подписки и внутриигровые предметы на сторонних ресурсах, поскольку часто

злоумышленники получают ваши деньги и доступ к карточкам оплаты и электронным кошелькам.

СПАМ

Согласно статье 18 Федерального закона от 13.03.2006 N 38-ФЗ "О рекламе" распространение рекламы допускается только при условии предварительного согласия абонента или адресата на получение рекламы.

В свою очередь юридически спам можно определить как рекламу, распространяемую без предварительного согласия абонента или адресата.

Важно, что допускается реклама при условии предварительного согласия абонента, причем согласие должно быть не устным, а в спорных ситуациях, касающихся рассылок, распространитель обязан доказать наличие такого согласия.

Также согласно закону распространитель такой рекламы обязан немедленно прекратить распространение данной рекламы в адрес лица, обратившегося к нему с таким требованием.

Для этого необходимо:

– В электронном сообщении найти кнопку «Отказаться от рассылки», пройдя по которой подтвердить отказ от получения рекламных сообщений;

– По телефону или электронной почте организации или лицу, направившему сообщение СМС или в мессенджере, сообщить о необходимости исключить из рекламной рассылки.

Также сервисы электронной почты и мессенджеры позволяют отметить сообщение или адресата как спам или распространитель спама соответственно. Для этого необходимо выделить нужное письмо и нажать кнопку «Это спам», после чего письмо или сообщение будет перемещено в папку Спам или удалено. При этом администрация сервиса сможет отследить отправителя спама и заблокировать распространение данной информации или отправителя для других пользователей.

В соответствии с ч. ч. 1 и 7 ст. 38 Закона N 38-ФЗ "О рекламе" рассылка физическими и юридическими влечет административный штраф.

Для привлечения к ответственности распространителя спама получателю спама необходимо обратиться с ФАС России, сообщив о получении спама, указав на отсутствие согласия на получение таких рассылок, и приложив сообщение, его фотографию или скриншот, содержавший рекламу.

Однако каждый пользователь Интернет-сети обязан соблюдать определенные правила безопасности. Пункт 28 Правил оказания телематических услуг связи, утвержденных постановлением Правительства Российской Федерации от 10 сентября 2007 г. № 575, обязывает абонента (пользователя сети): …б) использовать для получения телематических услуг связи пользовательское (оконечное) оборудование и программное обеспечение, которое соответствует установленным требованиям; 33 …д) предпринимать меры по защите абонентского терминала от воздействия вредоносного программного обеспечения; е) препятствовать распространению спама и вредоносного программного обеспечения с его абонентского терминала.

ПОЛЬЗОВАТЕЛЬСКОЕ СОГЛАШЕНИЕ

Отношения пользователей и различных сайтов и сервисов носят правовой характер и имеют форму Пользовательского соглашения.

Так данное Пользовательское соглашение является публичной офертой или договором присоединения:

– Реклама и иные предложения, адресованные неопределенному кругу лиц, рассматриваются как приглашение делать оферты. Содержащее все существенные условия договора предложение, из которого усматривается воля лица, делающего предложение, заключить договор на указанных в предложении условиях с любым, кто отзовется, признается офертой (публичная оферта).

– Договором присоединения признается договор, условия которого определены одной из сторон в формулярах или иных стандартных формах и могли быть приняты другой стороной не иначе как путем присоединения к предложенному договору в целом. Присоединившаяся к договору сторона вправе потребовать расторжения или изменения договора, если договор присоединения хотя и не противоречит закону и иным правовым актам, но лишает эту сторону прав, обычно предоставляемых по договорам такого вида, исключает или ограничивает ответственность другой стороны за нарушение обязательств либо содержит другие явно обременительные для присоединившейся стороны условия, которые она, исходя из своих разумно понимаемых интересов, не приняла бы при наличии у нее возможности участвовать в определении условий договора.

Перед регистрацией или использованием пользователь должен подтвердить свое согласие с условиями «Пользовательского соглашения», а в случае несогласия с ними не имеет права пользоваться сайтом. Именно поэтому регистрация пользователя означает полное и безоговорочное принятие пользователем пользовательского соглашения.

Кроме этого, зачастую администрация сайтов и сервисов оставляет за собой право изменить Пользовательское соглашение в одностороннем порядке без какого-либо специального уведомления, публикуя Пользовательское соглашение в открытом доступе, поэтому рекомендуется регулярно проверять условия Пользовательского соглашения на предмет их изменения и/или дополнения.

При этом продолжение использования сайтом или сервисов пользователем после внесения изменений и/или дополнений в Пользовательское соглашение означает принятие и согласие пользователя с такими изменениями и/или дополнениями.

В Пользовательском соглашении отражены различные аспекты работы сайтов или сервисов, которые включают такие вопросы как порядок регистрации и использования, права и ответственность администрации сайта или сервиса, права и ответственность пользователя, перечень возможностей использования и правил их использования пользователем сайта или сервиса и другие аспекты.

Особую актуальность Пользовательское соглашение приобретает в условиях возможности передачи персональных данных пользователей другим организациям и лицам для коммерческих целей и ответственность пользователя за размещение или предоставление доступа к материалам, нарушающим интеллектуальные права.

ГОСУДАРСТВЕННЫЕ УСЛУГИ В ИНТЕРНЕТЕ

Государственные услуги – это услуги, которые нам оказывают органы власти и государственные организации для решения различных жизненных задач. Например, первой государственной услугой в жизни каждого гражданина является получение свидетельства о рождении.

Когда гражданину исполняется 14 лет, ему предоставляется право получать государственные услуги самостоятельно, например, получение паспорта, запись на прием к врачу, поиск работы или получение результатов экзаменов.

Получить государственные услуги можно тремя способами: через Интернет, через многофункциональные центры (МФЦ) и в традиционном порядке, посетив государственное учреждение.

Получение государственной услуги через Интернет – один из самых простых, удобных и современных способов, поскольку:

– Электронные государственные услуги экономят время: некоторые предоставляются дистанционно и результат можно получить также дистанционно, а другие в назначенное время без очереди;

– Возможность проверки статуса заявления;

– Портал государственных услуг функционирует 24 часа в сутки 7 дней в неделю в праздники или выходные дни, что позволяет подать заявление в любое время.

Государственные услуги предоставляются на сайте gosuslugi.ru

В настоящее время получить государственные услуги можно по различным вопросам, в том числе:

– Получение паспорта гражданина РФ и заграничного паспорта;

– Получение страхового свидетельства обязательного пенсионного страхования (СНИЛС);

– Запись на прием к врачу;

– Результаты государственной итоговой аттестации (ГИА);

– Результаты вступительных испытаний и о зачислении в образовательные учреждения;

– Получить направление на временное трудоустройство;

– Записаться на профессиональную ориентацию;

– Получение справок для получения государственной социальной стипендии;

– И многие другие.

Заявление на предоставление услуги в электронной форме подается онлайн с помощью компьютера, планшета или мобильного телефона, а документы при необходимости прикрепляются в виде скана или фотографии. Прежде чем подать заявление, пользователь может ознакомиться со всей нужной информацией о предоставлении услуги и ответственных организациях онлайн.

Для получения государственной услуги в сети необходимо в первую очередь зарегистрироваться в ЕСИА – Единой системе идентификации и аутентификации.

ЕСИА представляет собой логин и пароль от всех государственных порталов и сайтов. С его помощью можно подавать электронные заявления, оплачивать счета и штрафы и многое другое. Например, в некоторых регионах России узнать оценки в электронном дневнике родители могут с помощью ЕСИА, а учетная запись ЕСИА дает возможность пользоваться бесплатным беспроводным интернетом в метро Петербурга и Москвы.

Зарегистрироваться в ЕСИА могут граждане, достигшие возраста 14 лет и имеющие паспорт. Дети до 14 не могут иметь свою собственную учетную запись.

Для получения ЕСИА необходимо:

– Заполнить контактные данные на форме регистрации ЕСИА https://esia.gosuslugi.ru/registration .

– Далее в созданном личном кабинете нужно ввести данные паспорта и номер СНИЛС (он указан на страховом свидетельстве в виде зеленой пластиковой карты);

– После этого в личный кабинет придет уведомление, что данные документов успешно прошли проверку;

– Для завершения процесса регистрации нужно подтвердить свою личность. Для этого нужно прийти с паспортом и СНИЛС в любой МФЦ.

Также возможно получить ЕСИА можно сразу в ближайшем отделении МФЦ.

После регистрации в этой системе будет открыт полный доступ к государственным сайтам и порталам, а для получения непосредственно государственных услуг необходимо:

– Найти и ознакомься с описанием услуги. Для этого необходимо выбрать в каталоге на главной странице портала интересующую услугу или найти ее с помощью строки поиска, перейдя к странице с ее описанием. После необходимо изучить информацию на странице, в частности сведения о праве на получение услуги, какие документы необходимы для ее получения, и другую важную информацию. Часто услуга предоставляется разным категориям заявителей: физическим лицам, юридическим лицам и индивидуальным предпринимателям.

– Нажать на кнопку «Получить услугу». После получения информации об услуге можно перейти к ее получению. Чтобы заполнить электронное заявление, необходимо нажать на кнопку «Получить услугу».

– Заполнить электронное заявление. Внесение необходимой информации в поля формы электронного заявления. На любом шаге заполнения заявления возможно создать его черновик, нажав кнопку «Сохранить», и вернуться к подаче заявления в удобное время.

– Прикрепление необходимых документов. На этом шаге потребуется прикрепить документы, необходимые для получения услуги. Возможно прикрепить скан или фотографию документа.

– Отправить электронное заявление. После заполнения всех полей формы заявления необходимо нажать на кнопку «Отправить».

– Отслеживание хода оказания услуги. В личном кабинете или по электронной почте можно отслеживать ход оказания услуги.

– Получение результата. По некоторым услугам получить результат услуги можно онлайн. Но иногда для получения готового документа, например, паспорта, требуется личное обращение в орган власти.