Памятка «Основные виды мошенничества, совершаемых с использованием информационно-коммуникационных технологий».

Рекомендации по защите от действий мошенников.

Телефонное мошенничество

Чаще всего в сети телефонных мошенников попадаются пожилые или доверчивые люди. При этом каждый человек может стать жертвой мошенничества, если не будет следовать простым правилам безопасности.

Обман по телефону — требование выкупа.

Как это организовано: звонят с незнакомого номера. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции и обвинён в совершении того или иного преступления. Это может быть дородно-транспортное происшествие, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и даже убийство. Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном сообщает, что уже не раз помогал людям таким образом. Для решения вопроса необходима определенная сумма денег, которую следует привезти в оговоренное место или передать какому-либо человеку. Цена вопроса составляет от одной до тридцати тысяч долларов США.

На самом деле происходит следующее: в организации обмана по телефону с требованием выкупа участвуют несколько преступников. Звонящий может находиться как в исправительно-трудовом учреждении, так и на свободе. Набирая телефонные номера наугад, мошенник произносит заготовленную фразу, а далее действует по обстоятельствам. Нередко жертва сама случайно подсказывает имя того, о ком она волнуется. Если жертва преступления поддалась на обман и согласилась привезти указанную сумму, звонящий называет адрес, куда нужно приехать. Часто мошенники предлагают снять недостающую сумму в банке и сопровождают жертву лично. Мошенники стараются запугать жертву, не дать ей опомниться, поэтому ведут непрерывный разговор с ней вплоть до получения денег. После того как гражданин оставляет деньги в указанном месте или кому-то их передает, ему сообщают, где он может увидеть своего родственника или знакомого.

Как поступать в такой ситуации: первое и самое главное правило — прервать разговор и перезвонить тому, о ком идёт речь. Если телефон отключён, постарайтесь связаться с его коллегами, друзьями и родственниками для уточнения информации. Хотя беспокойство за родственника или близкого человека мешает мыслить здраво, следует понимать: если незнакомый человек звонит Вам и требует привезти на некий адрес денежную сумму — это мошенник. Если Вы получили звонок от якобы близкого родственника или знакомого с информацией о том, что он попал в неприятную ситуацию, в результате которой ему грозит возбуждение

уголовного дела, и если звонящий просит передать взятку якобы сотруднику правоохранительных органов, готовому урегулировать вопрос, следует задать уточняющие вопросы: «А как я выгляжу?» или «Когда и где мы виделись последний раз?», т.е. задавать вопросы, ответы на которые знаете только вы оба. Если вы разговариваете якобы с представителем правоохранительных органов, спросите, из какого он отделения полиции. После звонка следует обратиться в полицию, где поинтересоваться, действительно ли родственник или знакомый доставлен туда. Обращаем внимание на то, что требование взятки является преступлением.

SMS-просьба о помощи

SMS-сообщения позволяют упростить схему обмана по телефону. Такому варианту мошенничества особенно трудно противостоять пожилым или слишком юным владельцам телефонов. Дополнительную опасность представляют упростившиеся схемы перевода денег на счёт.

Как это организовано: абонент получает на мобильный телефон сообщение: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «друг» или другие.

Как поступать в такой ситуации: пожилым людям, детям и подросткам следует объяснить, что на SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники.

Как это организовано: приходит SMS с просьбой перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной — помощь другу, изменение тарифов связи, проблемы со связью или с Вашей банковской картой и так далее. После того как Вы перезваниваете, Вас долго держат на линии. Когда это надоедает, Вы отключаетесь — и оказывается, что с Вашего счёта списаны крупные суммы.

На самом деле происходит следующее: существуют сервисы с платным звонком. Чаще всего это развлекательные сервисы, в которых услуги оказываются по телефону, и дополнительно взимается плата за сам звонок. Реклама таких сервисов всегда информирует о том, что звонок платный. Мошенники регистрируют такой сервис и распространяют номер без предупреждения о снятии платы за звонок.

Как поступать в такой ситуации: не звонить по незнакомым номерам. Это единственный способ обезопасить себя от телефонных мошенников.

Телефонные вирусы

Очень часто используется форма мошенничества с использованием телефонных вирусов. На телефон абонента приходит сообщение следующего вида: «Вам пришло MMS-сообщение. Для получения пройдите по ссылке...». При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств с вашего счета.

Другой вид мошенничества выглядит так. При заказе какой-либо услуги через якобы мобильного оператора или при скачивании мобильного контента

абоненту приходит предупреждение вида: «Вы собираетесь отправить сообщение на короткий номер ..., для подтверждения операции, отправьте сообщение с цифрой 1, для отмены с цифрой 0». При отправке подтверждения, со счета абонента списываются денежные средства. Мошенники используют специальные программы, которые позволяют автоматически генерировать тысячи таких сообщений. Сразу после перевода денег на фальшивый счёт они снимаются с телефона. Не следует звонить по номеру, с которого отправлен SMS — вполне возможно, что в этом случае с Вашего телефона будет автоматически снята крупная сумма.

Выигрыш в лотерее

В связи с проведением всевозможных рекламных акций, лотерей и розыгрышей, особенно с участием радиостанций, мошенники часто используют их для прикрытия своей деятельности и обмана людей. «Вы победили, сообщите код карты экспресс-оплаты». Карточки экспресс-оплаты упростили процедуру зачисления денежных средств на счёт, но одновременно и открыли новые возможности для мошенников.

Как это организовано: на мобильный телефон звонит якобы ведущий популярной радиостанции и поздравляет с крупным выигрышем в лотерее, организованной радиостанцией и оператором мобильной связи. Это может быть телефон, ноутбук или даже автомобиль. Чтобы получить приз, необходимо в течение минуты дозвониться на радиостанцию. Перезвонившему абоненту отвечает сотрудник «призового отдела» и подробно объясняет условия игры:

- просит представиться и назвать год рождения;
- грамотно убеждает в честности акции (никаких взносов, переигровок и т.д.);
- спрашивает, может ли абонент перевести на свой номер денежные средства с карты экспресс-оплаты на определенную сумму (от 300 долларов и выше);
- объясняет, что в течение часа необходимо подготовить карты экспресс-оплаты любого номинала на указанную сумму и еще раз перезвонить для регистрации и присвоения персонального номера победителя, сообщает номер, куда надо перезвонить;
- поясняет порядок последующих действий для получения приза: с 10.00 до 20.00 такого-то числа абоненту необходимо с паспортом, мобильным телефоном и присвоенным персональным номером прибыть по указанному адресу для оформления радостного события. Если по каким-то причинам абонент не сможет в течение часа купить экспресс-карту, то все равно должен позвонить для согласования дальнейших действий.

Затем мошенник объясняет порядок активации карт: стереть защитный слой; позвонить в призовой отдел; при переключении на оператора — сообщить свои коды. Якобы оператор их активирует на номер абонента, а призовой отдел контролирует правильность его действий, после чего

присваивает ему персональный номер, с которым «победитель» должен ехать за призом. Но если Вы предложите самостоятельно активировать карты на свой номер и приехать с доказательными документами из сотовой компании, то это объявят нарушением правил рекламой акции.

Другие варианты мошенничества

Вам может поступить звонок от якобы представителя вашей сотовой компании, который предложит пополнить счет карточкой экспресс-оплаты. Но прежде чем совершить оплату, Вы должны будете сообщить оператору личный ПИН-код, перезвонив на определенный номер.

На самом деле происходит следующее: задача мошенников — вынудить Вас купить карты экспресс-оплаты на крупную сумму и сообщить личный код с этих карт. Это позволит злоумышленникам присвоить средства с этих карт. Приз и «победа» — приманка, призванная усыпить ваше внимание и бдительность.

Как поступать в данной ситуации: активировать карточки экспресс-оплаты следует исключительно через специальный короткий номер, указанный на карточке, а личный код никому никогда не сообщается. Всё это указано на карте экспресс-оплаты — и в первую очередь надо следовать этим правилам. Если Вам поступило предложение от радиостанции активировать карточки экспресс-оплаты — не верьте. Радиостанции никогда не требуют активировать карточки экспресс-оплаты при проведении лотереи. «Вы выиграли машину, нужны деньги для её оформления». Выигрыш приза может стать не только приманкой, но и поводом затребовать перечисления крупных денежных средств для оформления нужных документов.

Как это организовано: на мобильный телефон — как правило, в ночное время — приходит SMS-сообщение, в котором говорится о том, что в результате проведенной лотереи Вы выиграли автомобиль. Чаще всего это Audi A6, но упоминаются и другие известные иностранные модели и марки. Для уточнения всех деталей Вас просят посетить определенный сайт и ознакомиться с условиями акции либо позвонить по одному из указанных телефонных номеров. Во время разговора мошенники сообщают о том, что надо выполнить необходимые формальности: уплатить госпошлину и оформить необходимые документы. Для этого необходимо перечислить на счет своего мобильного телефона 30 тысяч рублей, а затем набрать определенную комбинацию цифр и символов якобы для проверки поступления денег на счет и получения «кода регистрации».

На самом деле происходит следующее: комбинация цифр и символов, которую Вы набираете, на самом деле является кодом, благодаря которому злоумышленники получают доступ к перечисленным средствам. Как только код набран, счет обнуляется, а мошенники исчезают в неизвестном направлении.

Как поступать в такой ситуации: если Вы узнали о проведении лотереи только в момент «выигрыша», и при этом ранее Вы не заполняли заявку на

участие в ней и никак не подтверждали свое участие в розыгрыше, то, вероятнее всего, Вас пытаются обмануть. Оформление документов и участие в таких лотереях никогда не проводится только по телефону и Интернету.

Простой код от оператора связи

Как это организовано: поступает звонок либо приходит SMS-сообщение якобы от сотрудника службы технической поддержки Вашего оператора мобильной связи. Обоснования этого звонка или SMS могут быть самыми разными:

- предложение подключить новую эксклюзивную услугу;
- для перерегистрации во избежание отключения связи из-за технического сбоя;
- для улучшения качества связи;
- для защиты от СПАМ-рассылки;
- предложение принять участие в акции от вашего сотового оператора.
- вам предлагается набрать под диктовку код или сообщение SMS, которое подключит новую услугу, улучшит качество связи и т.п.
- На самом деле происходит следующее: код, который Вам предложат отправить, является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников. Как только вы его наберёте, Ваш счёт будет опустошён. Никакая услуга не будет подключена.

Как поступать в такой ситуации: любая упрощённая процедура изменения тарифных планов выглядит подозрительно. Не ленитесь перезванивать своему мобильному оператору для уточнения условий. SMS-сообщения могут быть самыми разными. Советуем критически относиться к таким сообщениям и не спешить выполнить то, о чем просят. Лучше позвоните оператору связи, узнайте, какая сумма спишется с вашего счета при отправке SMS или звонке на указанный номер, затем сообщите о пришедшей на Ваш телефон информации. Оператор определит того, кто отправляет эти SMS и заблокирует его аккаунт.

Штрафные санкции и угроза отключения номера

Как это организовано: злоумышленник представляется сотрудником службы технической поддержки оператора мобильной связи и сообщает, что произошло нарушение условий договора:

- абонент сменил тарифный план, не оповестив оператора;
- не внес своевременно оплату;
- воспользовался услугами роуминга без предупреждения и так далее.

Чтобы предотвратить отключение номера, Вам предлагается:

- купить карты экспресс-оплаты и сообщить их коды;
- перевести на свой номер сумму штрафа и набрать код;
- перевести средства на указанный номер.

После этого Вы якобы сможете доказать свою невиновность и при этом сохраните свой номер.

На самом деле происходит следующее: пользуясь тем, что телефон Вам нужен постоянно потеря номера может стать для Вас критической, мошенник запугивает Вас. В результате он получает возможность присвоить себе Ваши средства — с карт экспресс-оплаты либо напрямую со счёта телефона.

Как поступать в указанной ситуации: перезванивать своему мобильному оператору для уточнения условий. Помните, что у Вас, как у потребителя услуг связи, есть права, которые защищаются законом. Никакой оператор связи не может требовать выплачивать ему штрафы до тех пор, пока Ваша вина не будет доказана.

Ошибочный перевод средств

Как это организовано: приходит SMS-сообщение о поступлении средств на счет, переведенных с помощью услуги «Мобильный перевод» либо с терминала оплат услуг. Сразу после этого поступает звонок, и Вам сообщают, что на Ваш счет ошибочно переведены деньги и просят вернуть их обратно тем же «Мобильным переводом» либо перевести на «правильный» номер. Вы переводите, после чего такая же сумма списывается с Вашего счёта.

На самом деле происходит следующее: чтобы во второй раз списать сумму с Вашего счёта, злоумышленник использует чек, выданный при переводе денег. Он обращается к оператору с заявлением об ошибочном внесении средств и просьбой перевести их на свой номер. То есть первый раз Вы переводите деньги по его просьбе, а во второй раз он получает их по правилам возврата средств.

Как поступить в такой ситуации: не поддаваться на обман. Если Вас просят перевести якобы ошибочно переведённую сумму, напомните, что для этого используется чек. Отговорка, что «чек потерян» скорее всего свидетельствует о том, что с Вами общается мошенник.

Доступ к SMS и звонкам

Многие люди хотя бы раз в жизни испытывали любопытство по отношению к частной жизни своих родственников и знакомых. Мобильная связь, фиксируя SMS и звонки, даёт ложное ощущение, что каждый может стать шпионом. И мошенники пользуются этим.

Как это организовано: в интернете или прессе публикуется объявление, в котором Вам предлагается изучить содержание SMS-сообщений и список входящих и исходящих звонков интересующего Вас абонента. Для этого необходимо отправить сообщение стоимостью от 10 до 30 руб. на указанный короткий номер и вписать в предлагаемую форму номер телефона абонента.

На самом деле происходит следующее: после того как Вы отправите SMS, с Вашего счета спишется сумма намного больше той, что была указана мошенниками — до 500 рублей. Разумеется, интересующая Вас информация так и не поступает. При этом большинство пострадавших не обращаются в

полицию, не желая признаваться в желании шпионить за другими людьми. В результате мошенники остаются безнаказанными.

Как поступать в такой ситуации: предложение о предоставлении данной услуги является мошенничеством, так как такая услуга может оказываться исключительно операторами сотовой связи и в установленном законом порядке!

Мошенничества с банковскими картами

Банковская карта — это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

Как это организовано: приходит сообщение о том, что Ваша банковская карта заблокирована. Предлагается бесплатно позвонить на определенный номер для получения подробной информации. Когда Вы звоните по указанному телефону, Вам сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации.

На самом деле происходит следующее: чтобы ограбить Вас, злоумышленникам нужен лишь номер Вашей карты и ПИН-код. Как только Вы их сообщите, деньги будут сняты с Вашего счета.

Как поступать в такой ситуации: не торопитесь сообщать реквизиты вашей карты! Ни одна организация, включая банк, не вправе требовать Ваш ПИН-код! Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка. Скорее всего, Вам ответят, что никаких сбоев на сервере не происходило, а Ваша карта продолжает обслуживаться банком.

Правила безопасности владельцам пластиковых карт, для сохранения финансовых средств

Пин-код — ключ к вашим деньгам. Никогда и никому не сообщайте ПИН-код Вашей карты. Лучше всего его запомнить. Относитесь к ПИН-коду как к ключу от сейфа с вашими средствами. Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё — в этом случае Вы даже не успеете обезопасить свой счёт, заблокировав карту после кражи или утери.

Ваша карта только Ваша. Не позволяйте никому использовать Вашу пластиковую карту — это всё равно что отдать свой кошелёк, не пересчитывая сумму в нём.

Ни у кого нет права требовать Ваш пин-код. Если Вам позвонили из какой-либо организации, или Вы получили письмо по электронной почте (в том числе из банка) с просьбой сообщить реквизиты карты и ПИН-код под различными предлогами, не спешите её выполнять. Позвоните в указанную организацию и сообщите о данном факте. Не переходите по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники. Помните:

хранение реквизитов и ПИН-кода в тайне — это Ваша ответственность и обязанность.

Немедленно блокируйте карту при ее утере. Если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка. Для этого держите телефон банка в записной книжке или в списке контактов Вашего мобильного телефона.

Пользуйтесь защищенными банкоматами. При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д. Граждане, пользующиеся банкоматами без видеонаблюдения, могут подвергнуться нападениям злоумышленников.

Опасайтесь посторонних. Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей. Если это невозможно, снимите деньги с карты позже либо воспользуйтесь другим банкоматом. Набирая ПИН-код, прикрывайте клавиатуру рукой. Реквизиты и любая прочая информация о том, сколько средств Вы сняли и какие цифры вводили в банкомат, могут быть использованы мошенниками.

Банкомат должен быть «чистым». Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нём телефону.

Банкомат должен быть полностью исправленным. В случае некорректной работы банкомата — если он долгое время находится в режиме ожидания или самопроизвольно перезагружается — откажитесь от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.

Советуйтесь только с банком. Никогда не прибегайте к помощи либо советам третьих лиц при проведении операций с банковской картой в банкоматах. Свяжитесь с Вашим банком — он обязан предоставить консультационные услуги по работе с картой.

Не доверяйте карту официантам и продавцам. В торговых точках, ресторанах и кафе все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.

Основные правила поведения в интернете.

Защита от вредоносных программ (виды вредоносных программ). Вредоносные программы — любое программное обеспечение, которое предназначено для скрытного (не санкционированного) доступа к персональному компьютеру с целью хищения конфиденциальных данных, а также для нанесения любого вида ущерба, связанного с его использованием. Все вредоносные программы нередко называют одним общим словом

«вирусы». На самом деле вредоносные программы можно разделить на три группы: компьютерные вирусы; сетевые черви; троянские программы.

Компьютерные вирусы — это программы, которые умеют размножаться и внедрять свои копии в другие программы, т. е. заражать уже существующие файлы. Обычно это исполняемые файлы (*.exe, *.com) или файлы, содержащие макропроцедуры (*.doc, *.xls), которые в результате заражения становятся вредоносными.

Сетевые черви — это вредоносные программы, которые размножаются, но не являются частью других файлов, представляя собой самостоятельные файлы. Сетевые черви могут распространяться по локальны сетям и Интернету (например, через электронную почту). Особенность червей — чрезвычайно быстрое «размножение». Червь без Вашего ведома может, например, отправить «червивые» сообщения всем респондентам, адреса которых имеются в адресной книге Вашей почтовой программы. Помимо загрузки сети в результате лавинообразного распространения, сетевые черви способны выполнять опасные действия.

Троянские программы не размножаются и не рассылаются сами, они ничего не уничтожают на вашем компьютере, однако последствия от их деятельности могут оказаться самыми неприятными и ощутимыми. Задача троянской программы — обеспечить злоумышленнику доступ к Вашему компьютеру и возможность управления им. Все это происходит очень незаметно, без эффектных проявлений. Просто однажды Ваша частная переписка может быть опубликована в Интернете, важная бизнес-информация продана конкурентам, а баланс лицевого счета у интернет-провайдера или в электронных платежных системах неожиданно окажется нулевым или отрицательным.

Безопасное использование электронной почты. Являясь удобным видом связи, как личной, так и деловой, электронная почта остаётся одним из самых популярных способов распространения вредоносных программ в Интернете. Обычное сообщение электронной почты — это просто текст, сам по себе он не может быть опасен. Но к сообщению можно прикрепить файл, называемый файлом вложения или файлом присоединения, который вполне может оказаться вредоносной программой или зараженным вирусом файлом.

Как уберечься от вредоносных программ. Если Вы получили сообщение с вирусом, значит, Вы уже невольно выполнили первый шаг на пути к заражению Вашего компьютера, поскольку опасный файл сохранился на жестком диске. Пока это не фатально, но очень опасно, поэтому, прежде всего, необходимо предпринять меры к тому, чтобы этого не происходило впредь. У многих операторов связи имеются на почтовых серверах фильтры, отсекающие подозрительные послания. Однако, несмотря на очевидную эффективность общесистемного фильтра, для обеспечения безопасности его все-таки недостаточно, поскольку он рассчитан на обезвреживание уже известных вирусов, тогда как новые вирусы могут беспрепятственно попадать в почтовый ящик. Поэтому пользователю необходимо принять дополнительные меры безопасности. Самый действенный способ оградить от

вредоносных программ свой почтовый ящик –запретить прием сообщений, содержащих исполняемые вложения. Если абонент включает подобный фильтр, то все сообщения, содержащие исполняемые файлы, будут автоматически удаляться непосредственно на почтовом сервере. Несмотря на кажущуюся радикальность подобной меры, она очень эффективна и в большинстве случаев не приводит к неудобствам или ограничениям возможностей пользователей. Во-первых, как правило, по электронной почте чаще всего рассылают документы и изображения, но не программы. Во-вторых, в случае необходимости получения программы по почте, можно договориться с отправителем, чтобы он предварительно упаковал ее с помощью какого-либо архиватора, например, Winzip или WinRar. Польза получится двойная, поскольку размер полученного файла-архива должен быть гораздо меньше размера и сходного файла. Имеется ещё один способ не сохранять подозрительные сообщения на своем компьютере. Надо сначала просматривать только заголовки сообщений и удалять ненужные письма непосредственно на сервере, не скачивая их на свой компьютер.

Как запретить выполнение вредоносных программ. Бывают обстоятельства, при которых невозможно организовать работу так, чтобы не получать сообщения с исполняемыми файлами. В этом случае есть вероятность получить сообщения с вредоносными программами. Значит, необходимо принять меры, чтобы вредоносные программы ни в коем случае не были запущены на выполнение. Чтобы запустить файл вложения на выполнение, следует открыть сообщение в отдельном окне, дважды щелкнув по строке сообщения в списке (сообщение с вложением помечено скрепкой) и открыть файл-вложение, дважды щелкнув по имени файла в заголовке сообщения (поле «Присоединить»).

Учитывая сказанное, необходимо взять за правило:

- не открывать сообщение (дважды щелкнув мышкой), особенно если оно пришло от неизвестного отправителя. Текст можно прочитать в режиме быстрого просмотра: когда при одиночном щелчке мышкой на сообщении в списке текст сообщения отображается не в отдельном, а в основном окне программы.
- немедленно удалять все подозрительные сообщения. Никогда не открывайте сразу присланные файлы-вложения, в том числе полученные от друзей, коллег или от имени известных фирм. Принимайте во внимание, что сообщения от якобы знакомых лиц могут оказаться рассылками, отправленными сетевыми червями. Также имейте в виду, что без вашего ведома ни одна уважаемая организация не будет рассылать файлы, даже если это важные данные, такие, как обновления системы или очередная защита от вирусов.

Расширение файла. Обращайте внимание на расширение файла. Особую опасность могут представлять файлы со следующими расширениями: *.ade, *.adp, *.bas, *.bat, *.chm, *.cmd, *.com, *.cpl, *.crt, *.eml, *.exe, *.hlp, *.hta, *.inf, *.ins, *.isp, *.jse, *.lnk, *.mdb, *.mde, *.msc, *.msi, *.msp, *.mst, *.pcd, *.pif, *.reg, *.scr, *.sct, *.shs, *.url, *.vbs,*.vbe, *.wsf, *.wsh, *.wsc. Вредоносные

файлы часто маскируются под обычные графические, аудио- и видеофайлы. Для того, чтобы видеть настоящее расширение файла, обязательно включите в системе режим отображения расширений файлов.

Как правильно удалять сообщение из почтовой программы. Будьте очень осторожны при получении сообщений с файлами-вложениями. Подозрительные сообщения лучше немедленно удалять. Чтобы удалить сообщение в почтовой программе полностью: удалите сообщение из папки «Входящие»; удалите сообщение из папки «Удаленные»; выполните над папками операцию «Сжать» (Файл/Папка/Сжать все папки).

Защита электронной почты. К сожалению, нельзя исключать случаи, когда присылаемые файлы все-таки будут запущены. Однако и в этих случаях можно принять контрмеры. В первую очередь, следите, чтобы у вас были установлены самые последние обновления программ. Нелишним будет установить персональный межсетевой экран (firewall). В нём следует указать исчерпывающий список программ и доступных им портов и сервисов. Как только какая-либо незнакомая программа попытается отправить почту, она тут же будет обнаружена, и зараза не распространится с Вашего компьютера дальше. Кроме того, отслеживать и блокировать опасные действия, которые могут выполнять вредоносные программы (обращение к файлам, загрузочной области диска, системному реестру и т. п.), способны специальные программы-сторожа, обычно входящие в состав антивирусных пакетов. Они автоматически запускаются на выполнение при загрузке операционной системы и незаметно прослеживают действия программ.