УПРАВЛЕНИЕ «К» ПРЕДУПРЕЖДАЕТ: БУДЬТЕ ОСТОРОЖНЫ И ВНИМАТЕЛЬНЫ!

Сегодня в повседневной жизни используется множество разнообразных высокотехнологичных устройств – пластиковых карт, мобильных телефонов и компьютеров.

Постоянно появляются новые модели, программы и сервисы. Все это делает нашу жизнь удобнее, но требует определённых навыков и знаний.

Одновременно с развитием таких устройств появляются виды мошенничества, позволяющие обмануть и присвоить денежные средства граждан. Чтобы не поддаться на уловки злоумышленников, достаточно знать, как они действуют, и соблюдать правила пользования мобильными телефонами, пластиковыми картами и компьютерами.

Проанализировав все случаи такого мошенничества, специалисты Управления «К» МВД России подготовили для Вас понятную и полезную памятку. Предлагаем внимательно ознакомиться с содержанием этой брошюры и следовать нашим рекомендациям. Они защитят Вас от действий мошенников и сберегут Ваши средства.

Телефонное мошенничество

Телефонное мошенничество известно давно – оно возникло вскоре после массового распространения мобильных телефонов.

В настоящее время, когда широко используются мобильные телефоны, и личный номер может быть у всех, от десятилетнего ребёнка до восьмидесятилетнего пенсионера, случаи телефонного мошенничества растут с каждым годом.

Управление «К» МВД РФ напоминает, что 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.

Основные схемы телефонного мошенничества

Обман по телефону: случай с родственником
КАК ЭТО ОРГАНИЗОВАНО:

Вам звонят с незнакомого номера. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции за совершение того или иного преступления. Это может быть ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений.

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 10 до 500 тысяч рублей.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

В организации данной схемы может участвовать как один, так и несколько преступников. Звонящий может находиться как в исправительно-трудовом учреждении, так и на свободе. Набирая телефонные номера по возрастанию либо убыванию последней цифры, 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 или узнает адрес потерпевшего. 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.

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 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 набрать «02», узнать номер дежурной части данного отделения и поинтересоваться, действительно ли родственник или знакомый доставлен туда. Управление «К» МВД РФ обращает ваше внимание на то, что требование взятки является преступлением.

Выигрыш в лотерее

В связи с проведением всевозможных рекламных акций, лотерей и розыгрышей мошенники часто используют их для прикрытия своей деятельности и обмана людей.

КАК ЭТО ОРГАНИЗОВАНО:

На Ваш мобильный телефон поступает SMS-сообщение о выигрыше ценного приза. Это может быть телефон, ноутбук или даже автомобиль.

Чтобы получить приз, необходимо в ближайшее время перезвонить по указанному контактному номеру. Перезвонившему абоненту отвечает сотрудник «призового отдела» и подробно объясняет условия акции, грамотно убеждает в ее честности и сообщает Вам алгоритм дальнейших действий. Выигрыш приза выступает не только в роли приманки, но является поводом затребовать перечисления крупных денежных средств.

Для уточнения всех деталей Вас просят посетить определенный сайт и ознакомиться с условиями акции, а также позвонить по одному из указанных телефонных номеров.

Так, например, Вы можете получить 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.

Во время разговора мошенники сообщают о том, что надо выполнить необходимые формальности: получить восьмизначный код, дающий право на получение приза, уплатить госпошлину (вам могут предложить также оформить страховку и установить на выигранный автомобиль дополнительное оборудование и т.д). Для этого необходимо посредством платежных терминалов перечислить на счет Вашего мобильного телефона сумму, составляющую 1% от стоимости выигрыша, а затем под руководством «специалиста информационно-справочной службы» набрать определенную комбинацию цифр и символов якобы для проверки получения «кода регистрации». При этом Вас будут уверять, что денежные средства, потраченные Вами на прохождение стандартной процедуры регистрации, остаются на Вашем счете и могут быть использованы по Вашему усмотрению. Либо Вам могут предложить перечислить денежные средства на указанный злоумышленниками электронный кошелек.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

В первом случае оплачивая свой абонентский номер под руководством злоумышленника, Вы сами этого не подозревая, переводите деньги на его счет, во втором - Вы изначально переводите денежные средства в карман злоумышленника.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Управление «К» МВД РФ предупреждает: если Вы узнали о проведении лотереи только в момент «выигрыша», и при этом ранее не заполняли заявку на участие в ней и никак не подтверждали свое участие в розыгрыше, то, вероятнее всего, Вас пытаются обмануть. Популярные радиостанции, операторы сотовой связи, платежные системы не проводили, не проводят, и не будут проводить игр, в которых гражданам надо платить деньги за приз.

SMS-сообщения из банка

Сегодня трудно представить себе человека, не имеющего карты того или иного банка. На карты перечисляют заработную плату, социальные пособия, граждане охотно пользуются картами при оплате услуг, покупок, в путешествиях. И, к сожалению, этот факт также явился поводом к мошенническим действиям.

КАК ЭТО ОРГАНИЗОВАНО:

На Ваш мобильный телефон поступает SMS-сообщение о том, что Ваша банковская карта заблокирована либо приостановлена, либо о том, что Вами успешно осуществлен перевод, которого Вы на самом деле не делали. Для уточнения информации Вам предлагается перезвонить по указанному телефону службы безопасности.

В случае если Вы перезваниваете по указанному в сообщении телефонному номеру, мнимый сотрудник службы безопасности банка выяснит, в каком банке Вы оформили карту, Ваши данные, а затем предложит подойти к ближайшему банкомату и путем нехитрых манипуляций под его чутким руководством Вы сможете разблокировать Вашу карту путем набора комбинации цифр, который является не чем иным, как кодом мобильного перевода с Вашего счета на счет злоумышленника или его сообщников.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Управление «К» предупреждает: на Вашей банковской карте указан номер единой сервисной службы (в большинстве случаев он выглядит следующим образом 8-800-ххх-хх-хх), позвонив на который Вы можете узнать обо всех операциях, производимых с Вашей картой.

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 денежных средств с одного телефона на другой.

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. Кроме того, в этом случае также постарайтесь связаться с коллегами, друзьями или близкими для уточнения информации.

Платный код от оператора связи

КАК ЭТО ОРГАНИЗОВАНО:

Вам 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 ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Управление «К» МВД РФ советует Вам критически относиться к таким сообщениям и не спешить выполнять то, о чем просят. Зайдите на официальный сайт компании, предоставляющей Вам услуги связи, ознакомьтесь с размещаемой на нем информацией или перезвоните оператору связи, уточните ситуацию, возникшую с Вашим абонентским номером, затем сообщите о пришедшей на Ваш телефон информации.

Ошибочный перевод средств

КАК ЭТО ОРГАНИЗОВАНО:

Вам приходит SMS-сообщение о поступлении средств на счет, переведенных с помощью услуги «Мобильный перевод» либо с терминала оплаты услуг. Сразу после этого поступает звонок или SMS и Вам сообщают, что на Ваш счет ошибочно переведены деньги и просят вернуть их обратно тем же «Мобильным переводом».

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Управление «К» МВД РФ советует Вам не поддаваться на обман. Если Вас просят вернуть якобы ошибочно переведённую сумму, проверьте с какого номера пришло СМС-сообщение о пополнении счёта, а также состояние Вашего счета и историю его пополнения в «личном кабинете» на официальном сайте оператора связи или через сотрудника справочной службы. Не исключено, что к Вам обратился добропорядочный рассеянный гражданин, но вероятность общения с мошенником исключать нельзя.

Псевдоприложения для мобильных телефонов

КАК ЭТО ОРГАНИЗОВАНО:

На Интернет-ресурсах пользователям предлагаются различные услуги и сервисы, которые не всегда соответствуют заявленным: приложения для мобильных телефонов, не являющиеся таковыми например, программное обеспечение якобы для общения в сети Интернет через мобильные устройства, различные игровые приложения, вводящие пользователей в заблуждение, такие как «мобильный шпион», «конструктор диет», «GSM-локатор» и др. Для получения желаемого контента Вам предлагается отправить SMS-сообщение на указанный злоумышленниками короткий номер либо ввести свой номер мобильного телефона на сайте. При этом потенциальный потребитель далеко не всегда догадывается о реальной стоимости услуги.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

После того как Вы отправите SMS, с Вашего счета спишется значительная сумма, намного больше той, что была указана мошенниками, а интересующая Вас информация так и не поступит, либо не будет соответствовать заявленной. В случае если Вы ввели свой номер мобильного телефона в форму, предлагаемую на сайте, Вам может быть подключена услуга «подписка», что приводит к регулярному списанию денежных средств с Вашего счета.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Управление «К» МВД России предупреждает: прежде чем отправить SMS-сообщение на короткий номер или ввести свой абонентский номер на сайте, уточните стоимость услуги у своего мобильного оператора.

Телефонные вирусы

Данный вид правонарушений зачастую неотделим от предыдущего. На телефон абонента приходит сообщение следующего вида: *«Вам пришло MMS-сообщение. Для получения пройдите по ссылке...»* либо пользователь пытается закачать на свой мобильный телефон те или иные приложения.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

При переходе по указанной ссылке в телефон загружается приложение с вредоносной программой, с помощью которой происходит отправка SMS-сообщений на арендуемые злоумышленниками короткие номера, что приводит к списанию денежных средств с вашего счета. То же самое может произойти при скачивании приложений напрямую с сайта.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Управление «К» предупреждает: не переходите по сомнительным ссылкам, не загружайте и не открывайте файлы, установите блокировку отправки SMS-сообщений на «короткие номера», что позволит уберечься от нежелательных трат.

Блокировка компьютера Trojan. Winlock

КАК ЭТО ОРГАНИЗОВАНО:

Операционная система Вашего компьютера блокируется и на экране появляется сообщение следующего содержания: «Ваша операционная система заблокирована за нарушение правил пользования сети Интернет. Обнаружены следующие нарушения:…» и прилагается список якобы совершенных Вами нарушений вплоть до посещения сайтов, содержащих сцены насилия, зоофилии и детской порнографии. Блокировка предпринята с благими целями – недопущения распространения вышеназванного контента с Вашего ПК в сети Интернет. Для разблокировки операционной системы Вам предлагается пополнить номер того или иного абонента на сумму около 400 рублей через терминал оплаты и получить код для разблокировки, который будет указан на чеке.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Злоумышленники распространяют через сеть Интернет вирус, блокирующий операционную систему Вашего компьютера и вымогают денежные средства за ее разблокировку. Разумеется, получив требуемую сумму, они не разблокируют Ваш компьютер.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Управление «К» предупреждает: используйте и обновляйте надежное антивирусное программное обеспечение, не переводите денежные средства на незнакомые номера, в случае блокировки Вашего компьютера Вы можете узнать код разблокировки на сайтах известных производителей антивирусного ПО.

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:

Вам 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 ПОСТУПАТЬВ ТАКОЙ СИТУАЦИИ:

Управление «К» МВД РФ предупреждает: 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.

Владельцам пластиковых банковских карт

Как защититься от мошенников

В последнее время наблюдается рост числа случаев мошенничества с пластиковыми картами. Управление «К» МВД РФ рекомендует всем владельцам пластиковых карт следовать правилам безопасности.

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 ЗАЩИЩЁННЫМИ 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 ИСПРАВНЫМ

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.

Правила поведения в Интернете

Защита от вредоносных программ

Интернет называют «миром новых возможностей». Но тем, кто только пришёл в этот мир, следует вести себя осторожно и строго следовать правилам поведения в Сети. Как и в реальном мире, в Интернете действует множество мошенников и просто хулиганов, которые создают и запускают вредоносные программы. Управление «К» МВД РФ напоминает: для защиты пользователей от вредоносных программ разработано множество действенных контрмер. Надо лишь знать их и своевременно использовать.

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. Компьютерные вирусы существуют давно. В последнее же время, когда компьютеры стали объединять в компьютерные сети, подключать к Интернету, в дополнение к традиционным компьютерным вирусам появились вредоносные программы нового типа: сетевые черви и троянские программы.

Сетевые черви – это вредоносные программы, которые размножаются, но не являются частью других файлов, представляя собой самостоятельные файлы. Сетевые черви могут распространяться по локальным 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.

ТАКТИКА БОРЬБЫ С ВРЕДОНОСНЫМИ ПРОГРАММАМИ

Вредоносные программы срабатывают при запуске на Вашем компьютере. Тактика борьбы с ними достаточно проста: не допускать, чтобы вредоносные программы попадали на Ваш компьютер; если они к Вам все-таки попали, ни в коем случае не запускать их; если они все же запустились, то принять меры, чтобы, по возможности, они не причинили ущерба.

КАК УБЕРЕЧЬСЯ ОТ ПОЛУЧЕНИЯ 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. Это очень опасно, поэтому, прежде всего, необходимо предпринять меры к его поиску и удалению, а также постараться 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 программы-архиватора. Польза получится двойная, поскольку размер файла-архива получается гораздо меньше размера исходного 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 ВЫПОЛНЕНИЕВРЕДОНОСНЫХ 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. Учитывая сказанное, необходимо взять за правило: не открывать сообщение, особенно если оно пришло от неизвестного отправителя. Текст можно прочитать в режиме быстрого просмотра списка сообщений, при отображении его в основном диалоговом окне, а не открывать каждое сообщение в отдельном диалоговом окне. Управление «К» МВД РФ рекомендует 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 – ЭТО ВАЖНО

Обращайте внимание на расширение файла. 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 видео файлы. 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 информацию с компьютера без вашего ведома, она тут же будет обнаружена и ее действия вы сможете заблокировать. 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.

БУДЬТЕ БДИТЕЛЬНЫ!

Управление «К» МВД РФ рекомендует больше внимания обращать на то, что происходит на вашем компьютере во время сеанса связи с Интернетом. Если Вы заметите, что в то время, когда Вы не выполняете никаких действий с компьютером, не происходит обновление антивирусного программного обеспечения и компонентов операционной системы, а индикатор активности передачи данных по сети говорит об обратном, немедленно отключите соединение с сетью и проверьте компьютер антивирусными программами. Индикатором активности работы с сетью может служить внешний модем (лампочки мигают), значок двух соединенных компьютеров, появляющийся при установлении связи внизу на

панели задач (мигает), работающие сторонние процессы, определяемые в диалоговом окне панели задач, установленной на компьютере операционной системы.

Безопасное использование телеконференций и ICQ

Самым густонаселенным вирусами местом в Интернете, по мнению специалистов-антивирусников, остается, так называемая, сеть Usenet, включающая в себя разнообразные группы новостей (телеконференций). Другими словами, конференции Usenet – это очень ненадежный источник получения файлов, поэтому относиться к таким источникам нужно более чем осторожно. Старайтесь пользоваться конференциями Usenet по их прямому назначению: для поддержания дискуссий, обмена мнениями, информацией, но не в качестве источника бесплатных программ. Форма взаимодействия в новостях – это все тот же обмен почтовыми сообщениями, поэтому при работе с конференциями Usenet используйте те же рекомендации, что и при работе с электронной почтой.

Другой неприятностью при работе с новостями (и другими подобными сервисами) может стать огласка вашего электронного почтового адреса, который впоследствии может быть использован для спам рассылок или рассылок сообщений с вирусами. Когда вы помещаете сообщение в конференциях Usenet, в нем содержится ваш обратный адрес. Это потенциально опасно, поскольку существуют специальные программы, которые способны автоматически сканировать подобные объявления, выуживая из них почтовые адреса. Однако такие программные автоматы легко обмануть. Измените свой обратный адрес, включив в него некоторую выделяющуюся часть, например, *I.Ivanov-DEL-@provider.ru*: обычные пользователи поймут, каков Ваш настоящий адрес, а программы будут использовать обманку «вслепую».

Безопасное использование пейджеров ICQ

Пейджеры ICQ также являются сервисами повышенной опасности. Дело в том, что, кроме просто обмена сообщениями, они дают возможность обмениваться файлами, которые могут оказаться вредоносными программами. Правила работы с файлами такие же, что и при приеме файлов-вложений по электронной почте: никогда не открывайте присланные файлы, предварительно не проверив их антивирусной программой. Не поддавайтесь желанию немедленно посмотреть фотографии собеседника. Сначала проверьте, не является ли присланный файл подделкой под файл-изображение, старайтесь не разглашать информацию о себе.

Защита IP-адреса компьютера

Другая потенциальная опасность ICQ – возможность определения IP-адреса Вашего компьютера, который может быть использован для воздействия извне. Работая в ICQ, обязательно установите флажок, запрещающий показывать IP-адрес.

ОБЩИЕ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОЙ РАБОТЫ В ИНТЕРНЕТЕ

1. АНТИВИРУСНЫЕ ПРОГРАММЫ – ВАШИ ПЕРВЫЕ ЗАЩИТНИКИ

Установите антивирусное программное обеспечение с самыми последними обновлениями антивирусной базы. Регулярно обновляйте антивирусные программы либо разрешайте автоматическое обновление при запросе программы. Повышайте свою компьютерную грамотность, используйте программное обеспечение с открытым кодом, участвуйте в его совершенствовании.

2. ОБНОВЛЕНИЯ – ЭТО ПОЛЕЗНО И БЕЗОПАСНО

Отслеживайте появление новых версий операционных систем и своевременно устанавливайте обновления к ним, устраняющие обнаруженные ошибки. По возможности отказывайтесь от использования старых операционных программ в пользу более современных. Регулярно обновляйте пользовательское программное обеспечение для работы в сети, такое как интернет-браузер, почтовые программы, устанавливая самые последние обновления. Помните, что обновления операционных систем разрабатываются с учётом новых вирусов.

3. НАСТРОЙТЕ СВОЙ КОМПЬЮТЕР ПРОТИВ ВРЕДОНОСНЫХ ПРОГРАММ

Настройте операционную систему на своём компьютере так, чтобы обеспечивались основные правила безопасности при работе в сети. Не забудьте подкорректировать настройки почты, браузера и клиентов других используемых сервисов, чтобы уменьшить риск воздействия вредоносных программ и подверженность сетевым атакам.

4. ПРОВЕРЯЙТЕ НОВЫЕ ФАЙЛЫ

Никогда не устанавливайте и не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников: скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях. Подозрительные файлы лучше немедленно удалять. Проверяйте все новые файлы, сохраняемые на компьютере. Периодически проверяйте на наличие угроз компьютер полностью.

5. БУДЬТЕ БДИТЕЛЬНЫ И ОСТОРОЖНЫ

По возможности, не сохраняйте в системе пароли (для установки соединений с Интернетом, для электронной почты и др.) и периодически меняйте их. При получении извещений о недоставке почтовых сообщений обращайте внимание на причину и, в случае автоматического оповещения о возможной отправке вируса, немедленно проверяйте компьютер антивирусной программой.

6. РЕЗЕРВНОЕ КОПИРОВАНИЕ – ГАРАНТИЯ БЕЗОПАСНОСТИ

Регулярно выполняйте резервное копирование важной информации. Подготовьте и храните в доступном месте системный загрузочный диск. В случае подозрения на заражение компьютера вредоносной программой загрузите систему с диска и проверьте антивирусной программой.

Помните:
если Вы или Ваши близкие
стали жертвами мошенников
или Вы подозреваете,
что в отношении Вас планируются
противоправные действия –
незамедлительно обратитесь
в ближайший отдел полиции
либо напишите заявление
на официальном сайте МВД России
www.mvd.ru