Руководство по безопасной работе в интернете

Автор: Дэвид Эмм, ведущий технический консультант "Лаборатории Касперского"

Почему мы подготовили это руководство?

В "Руководстве по безопасной работе в интернете" просто и понятно описывается потенциальный риск, связанный с работой в интернете, и объясняется, как защититься от интернет-угроз – как "традиционных" (спама и червей), так и более "современных" (фишинга и мошеннического ПО). Цель настоящего руководства – помочь читателю успешно противостоять кибератакам.

Подобные атаки становятся все более распространенными (за последний год число компьютерных угроз, циркулирующих в интернете, удвоилось). Их сложность также возросла: "традиционные" вирусы, черви и троянские программы сменились мошенническим ПО, т.е. программами, специально предназначенными для получения денег преступным путем.

Но несмотря на то, что интернет-атаки становятся все более значимой угрозой для домашних пользователей, простые меры предосторожности, описанные в настоящем

руководстве, помогут читателям в дальнейшем пользоваться интернетом продуктивно, с удовольствием и без негативных последствий.

В конце руководства приведен глоссарий, в котором объясняются технические термины, использованные в тексте.

В чем состоит риск?

К сожалению, при подключении компьютера к интернету он немедленно становится потенциальной мишенью для атак киберпреступников. Как незащищенный дом становится легкой добычей для взломщиков, так и незащищенный компьютер будто притягивает авторов вредоносных программ и интернет-мошенников.

От кибервандализма к мошенническому ПО

Еще несколько лет назад угроза для пользовательских компьютеров в основном исходила от кибервандалов, для которых программирование служило антисоциальным средством самовыражения. В то время программы редко создавались специально для причинения вреда, хотя запуск некоторых из них приводил к повреждению данных пользователя или выходу компьютера из строя (часто лишь в качестве побочного эффекта). При этом большую часть вредоносных программ в обращении составляли вирусы и черви.

Сегодня наиболее значительную угрозу представляет собой мошенническое ПО. Киберпреступники осознали, что в современном мире, который всегда находится "на связи", применение вредоносного кода позволяет заработать неплохие деньги. Мошенники используют вредоносные программы для кражи конфиденциальных данных пользователей (регистрационных имен, паролей, PIN-кодов и т.п.), чтобы затем с помощью этих данных получить незаконный доход. Большинство вредоносных программ, используемых с этой целью, составляют разного рода троянские программы, или троянцы. Одни из них регистрируют последовательность нажимаемых на клавиатуре клавиш, другие делают снимки экрана при посещении пользователем сайтов, предлагающих банковские услуги, третьи загружают на компьютер дополнительный вредоносный код, предоставляют хакеру удаленный доступ к компьютеру и т.д. Все эти программы объединяет то, что они позволяют злоумышленникам собирать конфиденциальную информацию и использовать ее для кражи денег у пользователей.

Все больше угроз

Киберугрозы не просто становятся более изощренными – их число также неуклонно растет. За прошлый год количество угроз, циркулирующих в интернете, удвоилось. По состоянию на июнь 2007 года антивирусные базы "Лаборатории Касперского" содержали более 340 000 записей, и каждый день к ним добавлялось более 450 новых угроз.

Если на компьютере появился вредоносный код

Как и любое другое программное обеспечение, вредоносные программы создаются с расчетом на определенное поведение и выполнение определенных функций. Таким образом, они имеют ограниченные возможности, поскольку делают только то, что запрограммировал вирусописатель.

В прошлом вирусы зачастую не несли никакой "полезной" нагрузки: единственной их целью было самораспространение. При этом в результате ошибок программирования некоторые из них совершали не предусмотренные авторами действия. Лишь немногие вирусы целенаправленно стирали файлы, перезаписывали участки диска "мусором" или вызывали медленное повреждение данных. И хотя вирусы вредили пользователям и приводили к потере данных, они, тем не менее, редко пытались собирать данные для будущего использования.

Современный вредоносный код, напротив, обычно создается не для повреждения данных на компьютере пользователя, а для их кражи. Именно поэтому многие троянские программы относят к категории шпионского ПО: они устанавливаются на компьютере скрыто, без ведома и согласия пользователя, и следят за его действиями изо дня в день. Они не привлекают к себе внимания и "заметают следы" с помощью специальных программ, которые называются руткитами. В результате увидеть их "невооруженным взглядом" трудно: с точки зрения рядового пользователя, его компьютер работает вполне нормально.

Хакерские атаки

Современные приложения чрезвычайно сложны; они компилируются из тысяч строк кода. Но создаются они людьми, а людям свойственно ошибаться. Поэтому нет ничего удивительного в том, что в программы закрадываются ошибки, что делает их уязвимыми для атаки. Хакерам эти лазейки позволяют проникнуть в систему, а вирусописатели используют ошибки в коде приложений, чтобы обеспечить автоматический запуск на компьютере вредоносных программ.

Термин "хакер" раньше использовался для обозначения высококвалифицированных программистов. Теперь так называют тех, кто использует уязвимости в программном обеспечении для внедрения в компьютерную систему. Это электронный эквивалент взлома помещения. Хакеры постоянно взламывают как отдельные компьютеры, так и крупные сети. Получив доступ к системе, они крадут конфиденциальные данные или устанавливают вредоносные программы. Они также используют взломанные компьютеры для рассылки спама или для атаки веб-сайтов путем перегрузки веб-серверов сетевым трафиком, что вызывает отказ в обслуживании (по-английски Denial of Service, или DoS) и делает сайты недоступными для пользователей. Подобный инцидент может нанести значительный урон бизнесу компании-владельца ресурса.

Конечно, киберпреступники стремятся использовать свое время и затраченные усилия с максимальной отдачей, поэтому они, как правило, атакуют наиболее популярные системы. Этим, в частности, объясняется большое внимание, уделяемое ими Microsoft® Windows® – операционной системе, установленной на подавляющем большинстве персональных компьютеров.

Как защитить компьютер от вредоносного кода и хакерских атак?

Вы сможете защитить свой компьютер от вредоносного кода и хакерских атак, если будете следовать приведенным ниже несложным правилам:

- Установите на своем компьютере решение для защиты от информационных угроз.
- Чтобы обеспечить всестороннюю защиту компьютера, в состав решения должны входить следующие компоненты:
    - Антивирус

    - Защита от шпионских программ
    - Защита от фишинга
    - Персональный сетевой экран (файервол)
    - Защита от вторжений в систему
    - Анти-спам
    - Технологии проактивной защиты от новых, неизвестных угроз
- Регулярно (не реже раза в день) устанавливайте обновления программ, обеспечивающих безопасность вашего компьютера.
- В дополнение к постоянной защите компьютера не реже раза в неделю проводите проверку (сканирование) системы.
- Всегда устанавливайте обновления операционной системы и прикладных программ, предназначенные для устранения пробелов в их безопасности. Если вы пользуетесь Microsoft® Windows®, вам не нужно вручную загружать обновления каждый месяц, достаточно установить режим автоматических обновлений – Пуск | Панель управления | Центр обеспечения безопасности Windows® (Start | Control Panel | Security Center).
- Если вы пользуетесь программным пакетом Microsoft® Office, не забывайте регулярно устанавливать его обновления.
- Если вы получили по электронной почте сообщение с вложенным файлом (документ Word, таблица Excel, исполняемый файл с расширением .EXE и т.д.), не открывайте вложение, если отправитель письма вам неизвестен. Не открывайте вложение, если вы не ожидали получить подобное сообщение. НИ ПРИ КАКИХ УСЛОВИЯХ не открывайте вложения, присланные в нежелательных сообщениях (спаме).
- Используйте на своем компьютере учетную запись с правами администратора только в тех случаях, когда вам надо установить программы или изменить настройки системы. Для повседневного использования создайте отдельную учетную запись с ограниченными правами пользователя (для этого нужно зайти в раздел "Учетные записи пользователей" Панели управления). Это важно потому, что при атаке вредоносный код получает тот же уровень прав, с которым вы вошли в систему. Если вы зарегистрировались в системе с правами администратора, то такой же уровень прав будет и у вируса, червя или троянской программы, и вредоносное ПО получит доступ к ключевым данным, хранящимся в системе.
- Регулярно сохраняйте резервные копии своих данных на компакт-диске (CD), DVD-диске или внешнем USB-накопителе. В случае повреждения или шифрования вредоносной программой данных на жестком диске вы сможете восстановить их из резервной копии. Помните также, что, как и у любой другой домашней техники, срок службы у вашего компьютера ограничен.

Что такое фишинг (phishing)?

Фишинг – это особый вид компьютерного мошенничества, связанный с кражей личных данных и финансовых реквизитов пользователей.

Фишинг-атаки организуются следующим образом: киберпреступники создают подложный сайт, который выглядит в точности так же, как сайт банка или сайт, производящий финансовые расчеты через интернет. Затем мошенники пытаются обманным путем добиться, чтобы пользователь посетил фальшивый сайт и ввел на нем свои конфиденциальные данные – например, регистрационное имя, пароль или PIN-код. Обычно для этого используется массовая рассылка электронных сообщений, которые выглядят так, как будто они отправлены банком или иным реально существующим финансовым учреждением, но при этом содержат ссылку на подложный сайт. Конечно,

многие из получателей подобных писем не являются клиентами соответствующего банка или платежной системы. Но мошенники получат прибыль даже в том случае, если лишь немногие получатели сообщения "попадутся на удочку" и оставят на фальшивом сайте свои данные.

Пройдя по ссылке, вы попадаете на поддельный сайт, где вам предлагается ввести ваши учетные данные. Часто в фишинг-сообщениях используются те же логотипы и оформление, что и в письмах настоящего банка, а также ссылки, похожие на реальный адрес банка в интернете. Кроме того, сообщение может содержать ваше имя, как будто оно действительно адресовано вам лично. В письмах мошенников обычно приводится правдоподобная причина, требующая ввода вами на сайте "банка" своих данных. Например, ваш банк якобы проводит выборочную проверку безопасности учетных записей или изменил свою компьютерную инфраструктуру, в связи с чем всем клиентам необходимо заново ввести свои личные данные.

Введенные вами на подложном сайте данные затем переправляются организаторам мошеннической схемы. Получив ваши реквизиты, преступники используют их для снятия средств с вашего счета. Чтобы не привлекать внимания жертв, преступники зачастую снимают небольшие суммы. Однако, если обманутых пользователей много, мошенники получают весьма значительную прибыль.

Как защититься от фишинговых атак?

Соблюдение перечисленных ниже правил (а также советов по защите компьютера от вредоносных программ и хакерских атак, изложенных выше) позволит вам успешно противостоять фишинговым атакам:

- Относитесь с опаской к сообщениям, в которых вас просят указать ваши личные данные. Вероятность того, что ваш банк может запросить подобные данные по электронной почте, чрезвычайно мала. Если вы получили электронное письмо, якобы отправленное банком, перезвоните в банк и уточните, действительно ли вам посылали сообщение.
- Не проходите по ссылкам в электронных письмах в формате HTML: киберпреступники могут спрятать адрес подложного сайта в ссылке, которая выглядит как настоящий электронный адрес банка. Вместо этого скопируйте ссылку в адресную строку браузера или настройте свою программу для работы с электронной почтой таким образом, чтобы она работала только с обычным, неформатированным текстом, с которым подобные трюки не проходят.
- Не заполняйте полученные по электронной почте анкеты, предполагающие ввод личных данных. Подобную информацию безопасно вводить только на защищенных сайтах. Как узнать, является ли сайт защищенным? Убедитесь, что его адрес начинается с "https://" и найдите пиктограмму, похожую на запертый висячий замок, в правом нижнем углу окна браузера. Поскольку мошенники могут подделать и то, и другое, дважды щелкните мышью на значке замка и проверьте, совпадает ли адрес, указанный в сертификате безопасности, с текстом в адресной строке браузера. Если у вас остались сомнения, а вам необходимо провести операцию, требующую раскрытия ваших личных данных, воспользуйтесь телефоном.
- Регулярно проверяйте состояние своих банковских счетов (в том числе счетов, к которым привязаны дебетовые и кредитные карты) и просматривайте банковские выписки, чтобы убедиться в отсутствии "лишних" операций. При возникновении малейших подозрений немедленно обратитесь в банк.

- Проверяйте все даты, указанные в теле сообщения. Если какая-либо дата просрочена (например, если срок, к которому вам необходимо выполнить указанные в письме действия, уже истек), это должно вызвать у вас подозрения.
- Если электронное сообщение адресовано не вам лично (например, если оно начинается со слов "Уважаемый клиент"), это также подозрительно.
- Повод насторожиться есть и в случае, когда кроме вас электронное сообщение имеет других адресатов. Даже если банк решил связаться с вами по поводу ваших личных учетных данных по электронной почте, что само по себе крайне маловероятно, он не станет посылать копию сообщения другим людям.
- Орфографические, грамматические и синтаксические ошибки, а также неуклюжий стиль письма – типичные признаки фишингового сообщения.

Что такое компьютерное вымогательство (ransomware)?

Ransomware (от англ. ransom – выкуп) – это вредоносный код, с помощью которого киберпреступники вымогают у пользователей деньги. Вирус, червь или троянская программа шифрует данные на жестком диске зараженного компьютера и создает файл "readme", в котором пользователю предлагается заплатить за расшифровку своих файлов, переведя средства на счет злоумышленника с помощью указанной в файле "readme" системы электронных платежей.

Как защититься от кибервымогательства?

- Следуйте приведенным выше советам по защите компьютера от вредоносного кода и хакерских атак.
- Регулярно сохраняйте резервные копии данных. До сих пор специалистам "Лаборатории Касперского" удавалось восстанавливать данные, зашифрованные известными программами, относящимися к категории ransomware. Но киберпреступники используют все более сложные алгоритмы шифрования, и однажды мы, возможно, окажемся не в состоянии восстановить зашифрованную кибервымогателями информацию. При наличии резервной копии данных вы всегда сможете их восстановить.
- НИКОГДА не платите киберпреступникам. Если у вас нет резервной копии данных, обратитесь в службу технической поддержки производителя антивирусного решения, установленного на вашем компьютере – возможно, ваши данные удастся спасти.

О программах дозвона на платные сайты (rogue dialers)

Программы дозвона на платные сайты (rogue dialers) с помощью вашего модема набирают платные телефонные номера вместо обычных номеров, по которым вы дозваниваетесь до серверов своего интернет-провайдера. Эти программы устанавливаются на компьютере без вашего ведома и работают скрытно. Первым признаком заражения часто служит телефонный счет, сумма которого значительно больше той, к которой вы привыкли. В счете также могут быть указаны платные телефонные номера, по которым вы не звонили.

Как защититься от программ дозвона?

Не забывайте регулярно проводить полную антивирусную проверку своего компьютера и следуйте другим приведенным выше рекомендациям по защите вашего компьютера от вредоносных программ.

Вредоносные программы дозвона используют подключенный к компьютеру модем. Соответственно, если у вас широкополосное подключение, программы дозвона вам не страшны. Однако, переходя с коммутируемого подключения на широкополосное, не забудьте отключить кабель модема от телефонной розетки и убрать иконки модемных соединений с рабочего стола. Это предотвратит случайное использование модемного соединения. Если вам почему-либо понадобится вернуться к коммутируемому доступу (например, при сбоях в работе широкополосной связи), снова включите кабель модема в телефонную розетку и установите коммутируемое соединение – Пуск | Настройка | Сетевое окружение (Start | Settings | Network connections).

Что такое беспроводная сеть?

Большинство современных компьютеров поддерживают беспроводной доступ в сеть. Другими словами, они могут подключаться к интернету (и к другим устройствам, поддерживающим беспроводную связь) без сетевого кабеля. Главное преимущество беспроводных соединений – возможность работать с интернетом в любой точке дома или офиса (если позволяет расстояние между компьютером и устройством беспроводного доступа в сеть). Однако если не принять мер к обеспечению безопасности беспроводной сети, возможны следующие потенциально опасные ситуации:

1. Хакер может перехватить передаваемые или получаемые вами данные.
2. Хакер может получить доступ к вашей беспроводной сети.
3. Ваш канал доступа в интернет может быть захвачен другим лицом. How do I secure my wireless network?

Как обеспечить безопасность беспроводной сети?

Обеспечить безопасность устройства беспроводного доступа и, соответственно, свести к минимуму связанный с этим видом доступа риск можно с помощью следующих несложных шагов:

- Измените пароль администратора в своем беспроводном устройстве. Хакеру легко выяснить, какой пароль устанавливается по умолчанию производителем устройства, и использовать этот пароль для доступа в вашу беспроводную сеть. Избегайте паролей, которые легко подобрать или угадать (см. указания в разделе, посвященном выбору паролей).
- Включите шифрование трафика: лучше всего использовать протокол WPA, если ваше устройство его поддерживает (если нет, используйте WEP-шифр).
- Отключите трансляцию идентификатора сети (SSID broadcasting; SSID – Service Set Identifier, идентификатор сети), чтобы ваше беспроводное устройство не транслировало в эфир информацию о том, что оно включено.
- Смените идентификатор сети (SSID) вашего устройства. Если оставить идентификатор, установленный по умолчанию производителем устройства, злоумышленник, узнав этот идентификатор, сможет легко "засечь" вашу беспроводную сеть. Не используйте имена, которые легко угадать (см. указания в разделе, посвященном выбору паролей).
- Следуйте приведенным выше советам по защите компьютера от вредоносных программ и хакерских атак.

Что такое спам?

Спам – это анонимные незапрошенные массовые рассылки электронной почты, т.е. электронный эквивалент бумажной рекламной корреспонденции, засоряющей обычные почтовые ящики.

На долю спама приходится около 70-80% всех электронных сообщений, получаемых пользователями. Аналитики "Лаборатории Касперского" обрабатывают от 300 тыс. до 600 тыс. спам-сообщений в сутки. Спам чаще всего используется для рекламы товаров и услуг. Спамеры рассылают большое количество рекламных сообщений и наживаются на тех, кто на них отвечает.

Обычно немногие пользователи откликаются на спам-сообщения, но и этого спамерам хватает для получения прибыли. Разбор почты, содержащей большое количество спам-сообщений, отнимает много времени и сил. Спам засоряет почтовые ящики, загружает интернет-каналы и занимает много места на жестком диске. Кроме того, спам используется для рассылки вредоносных программ: спам-сообщения могут содержать зараженные вложения или ссылки на сайты, где размещены вредоносные программы (вредоносный код может загрузиться автоматически при посещении вредоносного сайта и заразить компьютер, если на нем не установлены обновления, закрывающие уязвимости операционной системы и отдельных приложений).

Для рассылки электронных сообщений спамеры используют ботнеты. Ботнет – это сеть, состоящая из зараженных компьютеров. Злоумышленники контролируют их, используя для этого троянские программы или иной вредоносный код. Зараженные машины рассылают спам автоматически. При этом владельцы таких машин не подозревают, что спамеры удаленно управляют их компьютерами. Используя хорошую антивирусную программу, вы сводите вероятность подобного захвата вашего компьютера к минимуму.

How can I protect myself from spam?

Как защититься от спама?

Ниже изложены правила, которые (вместе с приведенными выше советами по защите вашего компьютера от вредоносных программ и хакерских атак) помогут свести к минимуму количество получаемого вами спама.

- Не отвечайте на спам-сообщения. Спамеры часто регистрируют подобные ответы, чтобы выявить действующие адреса электронной почты. Таким образом, ответ на спам-письмо лишь увеличивает риск получения вами спама в дальнейшем.
- Не проходите по ссылкам, якобы предлагающим "отписаться от рассылки", поскольку этим вы подтверждаете, что ваш адрес электронной почты активно вами используется. Спамеры будут и дальше включать его в свои рассылки.
- Пользуйтесь несколькими адресами электронной почты: одним для личной переписки и как минимум еще одним для регистрации в форумах, чатах, списках рассылки и других общедоступных сервисах и сайтах.
- Для личной переписки подберите адрес электронной почты, который трудно угадать. Спамеры конструируют возможные адреса с помощью очевидных имен, слов и чисел. Подойдите к решению этой задачи творчески (и разумеется, не используйте в адресе свое имя и фамилию).

- Не публикуйте частный адрес электронной почты на общедоступных ресурсах. Если у вас нет выбора, пишите свой адрес так, чтобы применяемые спамерами автоматические средства сбора адресов не могли его обнаружить (например, "joe-точка-Smith-собака-mydomain-точка-com" вместо "joe.smith@mydomain.com").
- Рассматривайте адреса электронной почты, которые вы используете на общедоступных ресурсах, как временные. Если на адрес начинает приходить спам, просто смените его.

Почему важны пароли?

Один из основных способов защиты конфиденциальной информации – использование пароля с целью заблокировать доступ к вашим личным данным (банковским реквизитам и т.п.) для других пользователей.

С ростом популярности интернета защита информации с помощью паролей играет все более важную роль. Сейчас у всемирной компьютерной сети пользователей больше, чем когда-либо ранее. Возможности ее использования также значительно расширились и включают электронные банковские услуги, онлайн-покупки и исследования, проводимые с помощью интернет-ресурсов. Кроме того, теперь мы рассматриваем виртуальное пространство как среду для общения. В последние годы в интернете появились социальные сети, такие как "Одноклассники.ru", "В контакте.ru" и др. Их участники обмениваются разнообразной информацией о своей личной жизни, а также музыкой, фотографиями и видеороликами.

К сожалению, чем больше пользователи сообщают о себе в сети, тем выше риск кражи их личных данных (identity theft) киберпреступниками, которые в дальнейшем мошенническим путем приобретают товары и услуги от имени пользователей и даже крадут деньги непосредственно с банковских счетов своих жертв.

Поскольку пароли успешно защищают конфиденциальную информацию, их важность трудно переоценить. Все ваши учетные записи в интернете должны быть защищены паролями. Но выбирать пароль нужно осмотрительно.

Как выбрать "правильный" пароль?

Следуя перечисленным ниже правилам, вы сможете выбрать пароль, угадать который будет непросто.

- Выбирайте пароли, которые вам будет легко запомнить и не придется записывать (в том числе вносить в файл на вашем компьютере). Такой файл может быть стерт, поврежден или украден киберпреступниками.
- Не сообщайте никому свой пароль. Если с вами связался (например, по телефону) представитель некой организации и попросил сообщить ваш пароль, не раскрывайте свои личные данные: вы не знаете, кто на самом деле находится на другом конце провода.
- Если онлайн-магазин или веб-сайт прислал вам по электронной почте сообщение с подтверждением регистрационной информации и новым паролем, как можно скорее зайдите на соответствующий сайт и смените пароль.

- Не используйте для защиты своих данных очевидные пароли, которые легко угадать: имя вашего супруга (супруги), ребенка, домашнего животного, регистрационный номер машины, почтовый индекс и т.п.
- Не используйте в качестве пароля реальные слова, которые киберпреступники могут найти в словаре.
- Используйте буквы как нижнего, так и верхнего регистра, а также цифры и другие символы – например, знаки препинания.
- Если возможно, используйте в качестве пароля словосочетание, а не отдельное слово.
- Не используйте один и тот же пароль для разных учетных записей.
- Не прибегайте к "ротации" паролей, когда "пароль1", "пароль2", "пароль3" и т.д. используются попеременно для разных учетных записей.
- Убедитесь в том, что установленное на вашем компьютере программное обеспечение для защиты от интернет-угроз блокирует попытки перехвата или кражи паролей злоумышленниками.

Безопасность детей при пользовании интернетом

При использовании интернета детьми возможны следующие ситуации, угрожающие как безопасности вашего компьютера, так и личной безопасности ребенка:

22. "Попутные" заражения (т.е. вредоносные программы, загружаемые автоматически при просмотре зараженных сайтов).
23. Заражение при использовании файлообменных (P2P) сетей, дающих другим пользователям доступ к вашему компьютеру.
24. Нежелательная реклама, в том числе всплывающие окна и рекламные программы, которые часто устанавливаются автоматически вместе с бесплатным ПО, загружаемым из интернета.
25. Получение ребенком информации сексуального характера (или иной неприемлемой информации).
26. Загрузка ребенком из интернета пиратских материалов (например, музыкальных или видеофайлов).
27. Ребенка могут обманным путем убедить предоставить личные данные (его собственные или ваши).
28. Ребенок может стать жертвой запугивания через интернет.
29. Ребенок может стать жертвой домогательств педофила (например, в онлайн-чатах).

Как защитить ребенка при пользовании интернетом?

Чтобы свести к минимуму риск перечисленных выше угроз, вы можете принять следующие меры:

- Поговорите со своими детьми о возможных опасностях, с которыми может быть сопряжено их пребывание в интернете.
- Постарайтесь включить работу на компьютере в число дел, которыми вы занимаетесь всей семьей.
- Поощряйте своих детей обсуждать с вами свой онлайн-опыт, в особенности его тревожные или неприятные аспекты.
- Сформулируйте правила, указывающие, что вашим детям разрешается делать в интернете, а что нет. Данные правила должны давать четкие ответы

на следующие вопросы (помните, что по мере взросления детей ваши ответы могут и должны меняться):
    - Можно ли регистрироваться на сайтах социальных сетей и других веб-сайтах?
    - Можно ли делать покупки через интернет?
    - Можно ли использовать программы мгновенного обмена сообщениями? Если ответ "да", объясните детям, что они не должны общаться с незнакомыми им пользователями.
    - Можно ли участвовать в онлайн-чатах?
    - Можно ли загружать музыкальные и видеофайлы, а также программы?
- Следуйте приведенным в настоящем руководстве советам по защите компьютера от вредоносных программ и хакерских атак и объясните своим детям, почему это важно для их и вашей безопасности.
- Многие решения Internet Security позволяют ограничить доступ с вашего компьютера к информации определенного характера. Кроме того, в состав браузера Internet Explorer входит модуль "Ограничение доступа" (Content Advisor) – Сервис | Свойства обозревателя | Содержание (Tools | Internet Options | Content).

Что делать с зараженным компьютером

Понять, заражен ваш компьютер или нет, не всегда легко. Авторы современных вирусов, червей и троянских программ прилагают значительные усилия, чтобы скрыть присутствие вредоносного кода в системе. Вот почему так важно следовать советам, приведенном в настоящем руководстве – в частности, установить на своем компьютере антивирусное ПО класса Internet Security, загружать обновления, закрывающие уязвимости операционной системы и отдельных приложений, и регулярно сохранять резервные копии данных.

Что делать, если мой компьютер заражен вирусом, червем или троянской программой?

Перечислить все характерные признаки заражения сложно, потому что одни и те же симптомы могут быть вызваны как воздействием вредоносного ПО, так и иными программными или аппаратными проблемами. Вот лишь несколько примеров:

- Ваш компьютер ведет себя странно, непривычно.
- На экране появились неожиданные сообщения или изображения.
- Вы слышите неожиданные звуки, воспроизводимые в случайном порядке.
- Происходит неожиданный запуск программ.
- Ваш персональный сетевой экран сообщает, что некое приложение пытается соединиться с интернетом, хотя вы эту программу не запускали.
- Ваши друзья получают от вас по электронной почте сообщения, которых вы не посылали.
- Ваш компьютер часто зависает, или программы стали выполняться медленно.
- Вы получаете множество системных сообщений об ошибке.
- При включении компьютера операционная система не загружается.
- Вы обнаружили пропажу или изменение файлов или папок.

- Загорается индикатор доступа к жесткому диску, хотя вы не запускали никаких программ.
- Ваш браузер ведет себя неадекватно – например, вы не можете закрыть окно обозревателя.

Если вы обнаружили один или несколько перечисленных выше симптомов, не пугайтесь. Возможно, причиной сбоев является не вирус, червь или троянская программа, а иная программная или аппаратная проблема. В любом случае, вам следует предпринять следующие шаги:

- Отключите компьютер от интернета.
- Если ваш компьютер подключен к локальной сети, отключите его от сети.
- Если операционная система не загружается, загрузите компьютер в безопасном режиме (включите компьютер, нажмите и удерживайте клавишу F8, затем выберите Безопасный режим (Safe Mode) в открывшемся меню) или загрузитесь с диска аварийного восстановления.
- Если вы давно не сохраняли резервную копию своих данных, сделайте это сейчас.
- Убедитесь в том, что на вашем компьютере установлены новейшие версии антивирусных баз. Если возможно, используйте для загрузки обновлений не свой компьютер, а компьютер у друзей или на работе: если ваш компьютер заражен, то подключение к интернету позволит вредоносной программе отправить важную информацию злоумышленникам или переслать копию своего кода пользователям, чьи адреса сохранены на вашем компьютере.
- Проведите полную антивирусную проверку компьютера.
- Если в результате проверки обнаружен вирус, червь или троянская программа, следуйте указаниям производителя антивирусного ПО. Хорошие антивирусы предлагают лечение зараженных объектов, помещение подозрительных объектов в карантин и удаление троянских программ и червей. Они также создают отчет со списком зараженных файлов и вредоносных программ, обнаруженных на компьютере.
- Если антивирусное решение не обнаружило вредоносных программ, то ваш компьютер, скорее всего, не заражен. Проверьте программное и аппаратное обеспечение, установленное на компьютере (удалите нелицензионные программы и ненужные файлы), и установите последние обновления операционной системы и прикладных программ.
- Если у вас возникли проблемы с удалением вредоносных файлов, проверьте, нет ли на сайте производителя установленного у вас антивирусного ПО информации о специальных утилитах, необходимых для удаления конкретной вредоносной программы.
- Если необходимо, обратитесь за помощью в службу технической поддержки производителя установленного на вашем компьютере антивирусного ПО. Узнайте у специалиста службы технической поддержки, как отправить образец зараженного файла в антивирусную лабораторию на анализ.

В заключение: замечание о краже личных данных

Помните, что безопасность важна не только при работе в интернете. Преступники, промышляющие кражей личных данных, могут использовать информацию, хранящуюся на физических носителях, для доступа к учетным записям пользователей в интернете. Приобретите шредер (устройство, режущее бумагу – лучше всего не только вдоль, но и поперек) и уничтожайте все документы,

содержащие персональные данные (имя, адрес, дату рождения и т.п.), прежде чем их выбросить.

Глоссарий

Рекламные программы (AdWare)

Это общий термин, обозначающий программы, которые демонстрируют пользователям рекламу (чаще всего, в виде всплывающих баннеров), и программы, перенаправляющие результаты поиска на рекламные сайты. Рекламные программы часто включаются в состав бесплатного (freeware) или условно-бесплатного (shareware) ПО. Если вы загрузили бесплатную программу, рекламная утилита может быть установлена на ваш компьютер без вашего ведома.

Некоторые троянцы тайно загружают рекламные программы с веб-сайтов и устанавливают их на компьютерах пользователей. Если на вашем компьютере не установлены последние обновления браузера, закрывающие уязвимости приложения, то хакерские утилиты (иногда называемые перехватчиками браузера, потому что они нарушают его нормальную работу, заставляя браузер устанавливать программы без вашего ведома) могут загрузить рекламные программы на ваш компьютер. Перехватчики браузера могут изменять настройки обозревателя, перенаправлять неверно или не полностью введенные адреса на конкретные сайты, перенаправлять поиск на платные (часто порнографические) сайты, а также менять домашнюю страницу обозревателя.

Как правило, рекламные программы никак не проявляют себя в системе: они не устанавливают свои ярлыки в меню Пуск | Программы (Start | Programs), не показывают свою пиктограмму в системном лотке (system tray) в правом нижнем углу экрана и не фигурируют в списке запущенных задач. Процедуры их удаления из системы чаще всего отсутствуют, а попытки удалить подобные программы вручную могут вызвать сбои в использующих их приложениях.

Ботнет (botnet)

Сеть компьютеров, управляемых киберпреступниками с помощью троянской или иной вредоносной программы.

Чат (Chat room)

Способ общения через интернет в режиме реального времени. Все, что надо делать пользователю в чате, – это печатать свои сообщения. Любой, кто зарегистрирован в чате, может принимать участие в общей беседе.

Мошенническое ПО (CrimeWare)

Любые вредоносные программы, используемые киберпреступниками для получения денег.

DoS-атака

DoS-атаки (DoS – сокр. Denial of Service, т.е. отказ в обслуживании) направлены на затруднение или прекращение нормального функционирования веб-сайта, сервера

или иного сетевого ресурса. Хакеры добиваются этой цели различными способами – чаще всего они создают чрезмерную нагрузку на сервер путем отправки большого числа запросов, что нарушает нормальную работу сервера и может полностью вывести его из строя.

Распределенная DoS-атака (DDoS-атака, distributed Denial-of-Service attack) отличается от обычной DoS-атаки тем, что производится с нескольких компьютеров одновременно. Обычно хакер использует один зараженный компьютер в качестве т.н. "мастера" ботнета и координирует с его помощью атаку, проводимую остальными компьютерами ботнета – "зомби". Заражение как "мастера", так и "зомби" обычно осуществляется путем загрузки троянской программы или иного вредоносного кода с использованием уязвимостей в приложениях, установленных на компьютерах-жертвах.

Хакер (hacker)

Первоначальное значение этого термина – "талантливый программист". Теперь хакерами называют людей, использующих уязвимости в программном обеспечении для взлома компьютерных систем.

Системы мгновенного обмена сообщениями(Instant messaging systems)

Программы мгновенного обмена сообщениями позволяют общаться в режиме реального времени с пользователями, занесенными в ваш личный список контактов.

Интернет (internet)

Интернет (иногда также называемый "Сетью") – это глобальная система соединенных между собой компьютерных сетей.

Интернет вырос из сети ARPANET, организованной в 1969 году американским государственным агентством ARPA (Advanced Research Projects Agency – Агентство по передовым исследовательским проектам) для обеспечения взаимодействия между компьютерными сетями высших учебных заведений и исследовательских организаций.

На сегодняшний день к интернету подключены бесчисленные компьютеры по всему миру. Связь между ними устанавливается на основе общедоступной телекоммуникационной инфраструктуры. Слаженную работу этой структуры обеспечивают протоколы TCP/IP (Transmission Control Protocol/Internet Protocol – протокол управления передачей данных/интернет-протокол). TCP разбивает данные на сетевые пакеты, передающиеся через интернет, а затем вновь собирает эти пакеты в единое целое по прибытии к месту назначения. IP обеспечивает адресацию пакетов при их передаче к месту назначения.

"Поверх" TCP/IP работают другие протоколы, выполняющие конкретные функции, необходимые пользователям интернета: в частности, протоколы FTP (передача файлов), SMTP (передача электронной почты) и HTTP (передача данных через всемирную паутину World Wide Web).

Интернет-провайдер (ISP)

Интернет-провайдер (ISP – Internet Service Provider) предоставляет пользователям и организациям доступ к интернету. Интернет-провайдеры обычно имеют т.н. "точки доступа" к интернету: у них есть оборудование, необходимое для предоставления интернет-доступа большому числу пользователей, а также выделенные IP-адреса. Некоторые интернет-провайдеры пользуются инфраструктурой, предоставляемой поставщиками телекоммуникационных услуг, у других есть собственные выделенные линии.

Клавиатурный шпион (keylogger)

Эти программы записывают последовательность клавиш, нажимаемых пользователем на клавиатуре. Хакеры используют клавиатурные шпионы для получения конфиденциальных сведений (регистрационных имен, паролей, номеров кредитных карт, PIN-кодов и т.п.). Троянские программы-бэкдоры (Backdoor Trojans) обычно имеют в своем составе клавиатурные шпионы.

Вредоносное ПО (MalWare)

Английский термин malware (сокр. от malicious software, т.е. "вредоносное ПО") применяется для обозначения любой программы, специально созданной для выполнения несанкционированных, часто вредоносных действий.

Одноранговый (Peer-to-Peer)

Термин "одноранговый" (P2P – peer-to-peer) описывает временные соединения, которые напрямую связывают пользователей, работающих с одними и теми же приложениями. Подобные соединения позволяют пользователям обмениваться музыкальными, видео- и иными файлами, находящимися на их компьютерах, поэтому одноранговые сети часто называют файлообменными. Популярными приложениями для обмена файлами являются Napster, Gnutella и Kazaa.

Фишинг (Phishing)

Особый вид киберпреступлений, связанный с получением личных финансовых реквизитов пользователей обманным путем. Киберпреступники создают подложный веб-сайт, как две капли воды похожий на сайт банка или сайт, через который проводятся финансовые взаиморасчеты (например, eBay). Затем злоумышленники обманным путем добиваются, чтобы пользователи посетили этот сайт и ввели на нем свои конфиденциальные данные (регистрационное имя, пароль, PIN-код и т.п.). Как правило, для привлечения внимания пользователей к подложному сайту злоумышленники рассылают большое число сообщений с гиперссылкой на него.

Компьютерное вымогательство(RansomWare)

Ransomware – это вредоносный код, используемый киберпреступниками для вымогания денег у пользователей. Вирус, червь или троянская программа шифрует данные на жестком диске и создает текстовый файл "readme", в котором жертве предлагается расшифровать данные в обмен на отправку автору программы денег с помощью указанной в файле системы электронных платежей.

Программа дозвона на платные сайты (Rogue dialer)

Программы дозвона набирают с помощью модема платный телефонный номер вместо того номера, который пользователь обычно использует для соединения со своим интернет-провайдером. Эти программы устанавливаются на компьютере без ведома пользователя и работают скрытно. Часто пользователь впервые обнаруживает проблему, лишь получив телефонный счет, сумма которого значительно превышает привычную. Кроме того, в счете за телефон могут быть указаны телефонные номера, на которые пользователь не звонил.

Руткит (Rootkit)

Этот термин, пришедший из мира операционной системы Unix, обозначает набор программ, с помощью которых хакеры пытаются получить несанкционированный доступ к компьютерам пользователей, оставаясь при этом незамеченными. Теперь руткитами также называют технологии, используемые для сокрытия действий троянских программ в системе Microsoft® Windows®. В последнее время руткиты становятся все более распространенными. Это, в частности, связано с тем, что многие пользователи входят в систему с правами администратора вместо того, чтобы создать отдельную учетную запись с ограниченным уровнем доступа.

Спам (spam)

Спам – это анонимные незатребованные массовые рассылки электронной почты, т.е. электронный эквивалент бумажной рекламной корреспонденции, засоряющей обычные почтовые ящики.

Шпионские программы (SpyWare)

Эти программы предназначены для сбора данных, хранящихся на компьютере, и пересылки их третьим лицам без ведома и согласия владельца компьютера. Подобные программы могут записывать последовательность нажимаемых на клавиатуре клавиш, собирать конфиденциальную информацию (пароли, номера кредитных карт, PIN-коды и т.п.) и адреса электронной почты, а также отслеживать поведение пользователя в интернете. Кроме того, шпионские программы неизбежно снижают производительность компьютера и снижают пропускную способность интернет-канала.

Троянская программа, или троянец (Trojan)

Термин "троянец" произошел от троянского коня – деревянной фигуры, с помощью которой, согласно легенде, греки обманным путем проникли в город Трою и захватили его. В классическом понимании троянец – это неспособная самостоятельно распространяться программа, предназначенная для выполнения вредоносных действий на компьютере-жертве.

Неспособность к самостоятельному распространению отличает троянские программы от вирусов и червей. На заре развития вредоносных программ троянцы встречались нечасто, поскольку их приходилось распространять вручную. В наши дни развитие интернета и общедоступность всемирной паутины позволяют распространять троянские программы без особых сложностей.

Как правило, троянцы устанавливаются на компьютере скрытно и доставляют свой вредоносный "груз" без ведома пользователя. Существует множество видов

троянских программ, и каждый из них предназначен для выполнения конкретных вредоносных функций. Наиболее распространены бэкдоры (backdoors – утилиты удаленного управления компьютером), в состав которых часто входят клавиатурные шпионы (keyloggers), шпионские программы (Trojan Spies), программы для кражи паролей (password stealing Trojans) и троянские прокси-серверы (Trojan Proxies), позволяющие использовать компьютер для рассылки спама.

Вирус (Virus)

В наше время термин "вирус" часто используется для обозначения любых видов вредоносных программ. Но, строго говоря, вирус – это программный код, способный к самовоспроизведению путем заражения файлов, размещенных на жестком диске. Соответственно, чем дольше вирус остается незамеченным, тем больше зараженных файлов будет на компьютере. Вирусы могут распространяться как в пределах одной машины, так и передавая себя на другие компьютеры.

Уязвимость (Vulnerability)

Этот термин обозначает ошибку или пробел в защите приложения или операционной системы, позволяющий хакеру взломать компьютер. Хакеры создают вредоносный код, направленный на использование конкретных уязвимостей.

После обнаружения уязвимости (например, разработчиком уязвимого ПО) производитель программного обеспечения обычно создает "заплату" (patch) для ликвидации пробела в защите приложения. Таким образом, разработчики программ и специалисты в области компьютерной безопасности постоянно соревнуются с вирусописателями, которые стремятся первыми найти новые уязвимости.

Всемирная паутина (World Wide Web)

Интернет – это глобальная система соединенных между собой компьютерных сетей. Всемирная паутина (World Wide Web, сокр. WWW) делает огромный объем информации, хранящейся в интернете, доступным пользователям. Во всемирной паутине данные представляются в графической форме, и их удобно просматривать.

Создатель всемирной паутины – Тим Бернерс-Ли (Tim Berners-Lee), британский консультант по программному обеспечению. Он нашел способ отслеживать связи между единицами информации с помощью компьютера (в "реальном" мире подобную функцию выполняет тезаурус). Тим Бернерс-Ли также создал стандарты, позволяющие обмениваться данными через интернет. Он разработал язык гипертекстовой разметки HTML (Hypertext Markup Language) – стандартный метод кодирования информации в паутине – и схему адресации, основанную на универсальных указателях ресурсов URL (Universal Resource Locator), которая позволяет найти любую нужную интернет-страницу. Пример URL – http://www.kaspersky.ru/. Кроме того, Тим Бернерс-Ли является автором протокола передачи гипертекста HTTP (Hypertext Transfer Protocol) – стандарта передачи содержания веб-страниц через интернет. Всемирная паутина в том виде, в котором мы ее знаем, появилась в 1991 году и с тех пор непрерывно растет.

Тим Бернерс-Ли организовал Консорциум Всемирной паутины (the World Wide Web Consortium, сокращенно W3C) – организацию, устанавливающую веб-стандарты. W3C определяет Всемирную паутину как "мир информации, доступной через сеть; воплощение человеческих знаний".

Червь (Worm)

Червей часто рассматривают как разновидность вирусов. Однако между червями и вирусами есть существенные различия. Червь – это компьютерная программа, самостоятельно распространяющая свой код, но не способная к заражению других файлов. Червь устанавливается на компьютер-жертву и ищет возможность распространения на другие компьютеры. При этом, в отличие от вирусов, черви создают единственную копию своего кода на каждой машине; код червя существует на компьютере отдельно, а не дописывает себя в файлы, размещенные на жестком диске.

Полезные ссылки

- kaspersky.ru
- viruslist.ru
- getsafeonline.org
- antiphishing.org