1. Тема: «Учимся защищать свой компьютер»

Содержание работы: Электронные сетевые риски - защита своих данных, создание надежных паролей, антивирусные программы. Правила скачивания и использования программ и контента.

Основной материал для занятия

Электронные (кибер-) риски — это возможность столкнуться с хищением персональной информации, риск подвергнуться вирусной атаке, онлайн-мошенничеству, спам-атаке, шпионским программам и т.д. Подростки в интернете сталкиваются с теми же рисками, что встречаются им в обществе. В сетевом пространстве угрозы могут исходить от кого угодно и откуда угодно – без географической или какой-то другой привязки. Что такое «опасный» контент, сегодня пытаются определять, основываясь на «современных общественных нормах», которые также достаточно трудно формулируемы. В числе прочих рисков отдельно стоит упомянуть электронные – это риски, связанные с потерей данных, заражением устройства компьютерным вирусом и т.д.

Одной из причин заражения вирусной программой является просмотр спама – ненужного, иногда вредного послания. Современная спам-рассылка распространяется в сотнях тысяч экземпляров всего за несколько десятков минут. Чаще всего спам идет через зараженные вредоносными программами пользовательские компьютеры — зомби-сети. Проблемы с рекламными рассылками (спамом) у частного пользователя начинаются в тот момент, когда его email-адрес попадает в базу данных к спамерам.

Например, Вы получили письмо. В тексте письма есть неуместные знаки препинания, похожие на опечатки: лишние пробелы или обилие заглавных букв (пример — Dear Arsen!!! we CONGR.ATULATE you !!). Сразу можем определить, что это спам. Таким образом спамеры стараются избежать почтовых фильтров, отсеивающих слова и фразы, характерные для спам-сообщений.

Откуда спамеры узнают ваш адрес?

Проблемы с рекламными рассылками (спамом) начинаются в тот момент, когда email-адрес пользователя попадает в базу данных к спамерам. Например, некоторые интернет-магазины, конференции, форумы и т. п. требуют регистрации с указанием работающей электронной почты. Иногда переданные таким образом адреса попадают к спамерам.

А также спамеры определяют веб-адреса следующими способами:

1) сканируя веб-сайты;

2) сканируя доски объявлений, форумы, чаты, Usenet News и так далее;

3) подбирая «легкие» адреса (nur@, bek@, alex@, info@, sales@, support@) по словарю имен и частых слов;

4) подбирая «короткие» адреса (aa@, ann@, bb@, abc@) простым перебором.

Исходя из этого, можно рекомендовать следующие меры:

Заведите себе два адреса — частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный — для публичной деятельности (форумов, чатов и так далее).

1) Адрес для переписки никогда не должен публиковаться в открытом доступе.

2) Адрес для переписки не должен быть легким в запоминании или «красивым». Ваше имя или красивое слово — не подходят.

3) Если нужно сообщить свой приватный адрес (в конференции, на сайте) — делайте это способом, непригодным для автоматического прочтения сборщиком адресов. «student-DOT-собака-mail-точка-ру» — хороший способ. Если речь идет о публикации на сайте, можно опубликовать адрес в виде картинки.

4) Адрес для публикации нужно заранее считать временным. Не стоит его жалеть — вы всегда можете завести новый. Как правило, спам начинает приходить на него через несколько дней после публикации. Поскольку этот адрес могут использовать не только спамеры (туда будет приходить и нормальная почта), стоит его периодически просматривать. Вы можете читать почту, приходящую на него, раз в неделю или раз в месяц.

Еще одним электронным риском является вредоносное ПО (Программное Обеспечение), которое использует широкий спектр методов для распространения и проникновения в компьютеры, не только через диски или другие носители, но и через электронную почту посредством спама или скачанных из Интернета файлов.

К вредоносным программам относятся вирусы, черви и «троянские кони» – это компьютерные программы, которые могут нанести вред вашему семейному компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом и даже использовать ваш компьютер для распространения своих копий на компьютеры ваших друзей, родственников, коллег и по всей остальной глобальной Сети.

Вирусное ПО (программное обеспечение), которое рассылает спам в социальной сети может быть установлено на ваш компьютер с любого сайта. И от вашего лица могут регулярно рассылаться абсолютно любые сообщения, избавиться от которых не поможет ни одна защита самого сайта. Хотя бы просто по той причине, что в этом случае потребуется не защита вашей страницы, а современное антивирусное программное обеспечение. Поэтому не забывайте обновлять свою антивирусную программу и следить за защитой своего компьютера. Вероятность наткнуться на подобные вредоносные программы очень велика.

Программы-шпионы и рекламное программное обеспечение могут стать причиной возникновения ряда проблем: надоедливых всплывающих окон, несанкционированной установки инструментов и иконок, перенаправления на непристойные сайты, случайных ошибок и снижения производительности системы. Эти вредоносные программы, установленные на Вашем компьютере без Вашего согласия, могут контролировать, а в некоторых случаях, и управлять Вашим ПК. Чтобы снизить риск заражения подобными

программами, необходимо использовать антишпионское и антирекламное ПО. На самом деле, многие эксперты рекомендуют использовать, по меньшей мере, два разных ПО для более широкого охвата спектра вредоносных программ.

Помимо негативного воздействия на компьютер и мобильное устройство, можно стать жертвой еще одного вида кибер-преступления — кибер-мошенничества. В самом широком смысле мошенничество — это умышленный обман или злоупотребление доверием с целью получения какой-либо выгоды. Мошенничество в сети Интернет (кибермошенничество) — один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный и финансовый ущерб.

Как узнать, что ваш компьютер заражен?

Учитывая, что вирусы обычно хорошо замаскированы внутри обычных файлов, непрофессионалу трудно их обнаружить. Несмотря на это, даже неопытный пользователь, как правило, замечает, что с компьютером происходит что-то неладное: он медленно работает, появляются непонятные сообщения, а иногда он просто «зависает» и только перезагрузка может вывести его из этого состояния. Существуют определенные признаки, по которым, с высокой степенью вероятности, можно утверждать, что компьютер заражен вирусами:

- медленная реакция на действия пользователя, особенно при запуске программ;

- искажение содержимого файлов и каталогов или их полное исчезновение;

- частые сбои и зависания компьютера;

- самопроизвольное появление на экране сообщений или изображений;

- несанкционированный запуск программ;

-зависание или странное поведение интернет-браузера;

- невозможность перегрузки компьютера (операционная система не загружается).

Однако нужно помнить, что ничто не может дать стопроцентной гарантии защиты вашего компьютера. Поэтому в любом случае Вы должны быть крайне внимательны, когда получаете сообщения по электронной почте от неизвестного адресата с вложением, когда скачиваете файлы из сети Интернет, пользуетесь чужими носителями информации или открываете файлы, скопированные с чужого компьютера.

Советы для безопасного Интернет-серфинга

– Используйте и регулярно обновляйте брандмауэр, антивирусное и антишпионское программное обеспечение.

– Регулярно устанавливайте обновления, предлагаемые поставщиками операционной системы, браузера и другого программного обеспечения.

– Не открывайте вложения и ссылки электронной почты от неизвестных Вам отправителей.

– Проверяйте все вложения электронной почты и загрузки, используя антивирусное программное обеспечение.

– Не скачивайте и не устанавливайте программы от неизвестных поставщиков. Отключайте Java, JavaScript и ActiveX в браузере (если это возможно).

– Регулярно делайте резервные копии важных данных, хранящихся на компьютере.

– Регулярно осуществляйте техническое обслуживание Вашего компьютера, такое, как очистка диска и дефрагментация.

– Создайте загрузочный диск на случай повреждения данных на Вашем компьютере.

Используйте только лицензионные антивирусные программы

Все знают, что установка антивируса – это первый шаг к защите компьютера. Тем не менее многие подходят к нему несерьезно и устанавливают программы сомнительного происхождения. Как бы парадоксально это не выглядело, но бывают случаи, когда бесплатные антивирусы не защищают, а наоборот загружают вредоносные программы. Поэтому если вы все-таки решили надежно обезопасить компьютер, выбирайте проверенных производителей или обратитесь к нам, и мы установим современную антивирусную программу.

Тщательно подбирайте программное обеспечение

Первый совет касается не только антивирусных программ, но и всей операционной системы. Если у вас стоит нелегальная версия, шансы на ее заражение вирусами резко возрастают. В этом случае лучше не полениться и провести диагностику системы и всех установленных на ней программ. В идеале – переустановить версию на более новую. При необходимости мы можем сделать и то, и другое.

Регулярно обновляйте работу антивирусной программы

Не стоит забывать, что установка лицензионной антивирусной программы – это только полдела. Для эффективной защиты нужно постоянно следить за ее состоянием: проводить проверку компьютера и съемных носителей, удалять найденные вредоносные файлы и обновлять антивирусную базу. Обычно при нелицензионном антивирусе с этим возникают большие сложности, так как его базы устаревают очень быстро.

Установите специальные программы – фаервол или брандмауэр

Антивирус – программа полезная и нужная, однако даже он не гарантирует 100%-й результат. Некоторые вирусы уже научились «обходить» их защиту и использовать лазейки (так называемые уязвимости) в операционной системе. Поэтому для более надежной защиты лучше установить дополнительный сервис со странным на первый взгляд названием, но очень полезными функциями – **фаервол**. Это своеобразный «щит», который контролирует установку программ и приложений, а также отбивает атаки «троянов» и других вирусов. Если вы задумались над тем, нужен ли такой полезный инструмент, как фаервол, ответим – однозначно, да!

Периодически сохраняйте важные файлы в безопасном месте

И речь идет вовсе не о компьютере. Главная задача – наоборот перенести информацию в максимально удаленное от вашего компьютера место. Например, скопировать на съемный носитель (флешку или внешний диск). В идеале – создать резервную копию на облачном сервере в интернете. Не знаете, как это сделать? Мы проконсультируем вас в этом вопросе и покажем все нюансы.

Не открывайте сомнительные ссылки и всплывающие окна в браузере

Помните, что вредоносные программы не могут попасть в компьютер без вашей помощи. Очень часто это происходит, когда вы переходите по неизвестным ссылкам или кликаете на интригующие картинки или сообщения, которые вас заинтересовали заманчивой информацией. Чтобы «залезть» в компьютер, вирусу может быть достаточно одного вашего нажатия на крестик при закрытии окна. Таким образом он активизируется. От подобного «мусора» помогут избавиться специальные программы-блокировщики и фаерволы, которые можно установить самостоятельно или с нашей помощью.

Проверяйте подлинность сайтов, на которые переходите

Одно из главных правил безопасности – не заходить на неизвестные и подозрительные сайты без острой необходимости. Если уж сильно нужно посетить сайт, который привлек ваше внимание, проверяйте подлинность адреса в строке браузера. Сверяйте название в результатах поиска и адресной стоке после перехода на сайт. Если они не будут совпадать, возможно, вы перешли на сайт-подделку, на котором содержаться вирусы.

Не запускайте неизвестные программы в интернете

Бывает, что в браузере появляются окна с уведомлениями следующего характера «Программа пытается загрузить на ваш компьютер расширение. Разрешить установку?». Даже не дочитывая до конца многие выбирают ответ «Да», тем самым добровольно пуская к себе вирусы. Заметив подобные предложения с неизвестным вам содержанием, лучше отклоните их. Правильнее загружать программы и расширения с проверенных источников, уменьшая риски.

Не открывайте неизвестные письма и вложения в почте

Представьте ситуацию, что на вашу электронную почту пришло письмо со странным названием от друга, родственника или знакомого. С одной стороны, вы

догадываетесь, что человек вряд ли бы выслал вам его. Но с другой любопытство все-таки берет верх, и вы открываете сообщение. Стоить загрузить на первый взгляд безобидные вложения из этого письма – документы, фотографии rar- или zip-архивы – и вирус возьмется за дело. О том, что открывать письма от неизвестных людей опасно вдвойне, надеемся, вы знаете. Это касается не только почты, но и скайпа, а также социальных сетей.

Уделяйте больше внимания личной информации

В таком публичном месте, как интернет, излишняя внимательность и осторожность никогда не повредит. Возьмите за правило создавать разные и сложные пароли для отдельных аккаунтов (почта, скайп, социальные сети и т. д.). Понятно, что всегда есть риск их забыть или перепутать. В этом случае запишите их на листочке или используйте более современные методы, сохранив их в браузере. Если вы не знаете, как это сделать, мы поможем облегчить задачу. Главная задача – максимально обезопасить ваши данные. Не оставляйте телефон и e-mail в открытом доступе и публичных местах. И уж тем более не передавайте свой логин и пароль неизвестным лицам.