6 ГЛАВА

Безопасная работа в сети интернет

Откуда появляются вредоносные программы на компьютере

Как и в жизни, в интернете необходимо соблюдать определенные правила безопасности. Здесь тоже есть мошенники, которые попытаются проникнуть в компьютер, чтобы воспользоваться вашими персональными данными, чаще для перепродажи. Внедрившись в вашу систему, они могут от вашего имени рассылать письма или совершать атаки на другие компьютеры. Это все равно что, украв ваш паспорт, действовать от вашего имени.

Чтобы встроиться в ваш компьютер, злоумышленнику достаточно установить на него программу. Она может быть установлена без вашего разрешения. Такие программы называют вредоносными. Число типов и видов вредоносных программ очень велико, и постоянно появляются все новые. Среди них имеются вирусы, трояны, руткиты, кейлоггеры и т.д.

Вредоносные программы могут быть присланы в письме на ваш электронный почтовый ящик, вы можете занести вирус с флэш-накопителя, скачать вредоносную программу из интернета, случайно нажав на появившееся окно. Также на компьютере может появиться вирус при закачивании той или иной программы из интернета. Поэтому никогда не переходите по незнакомым ссылкам, есть шанс занести на компьютер вредоносную программу.

Виды мошенничества в Сети

Один из самых распространенных видов мошенничества – фишинг, когда обманным путем преступники стараются получить доступ к конфиденциальным данным: логинам и паролям. Например, вы можете получить письмо или сообщение, что заблокирована ваша банковская карта и нужно перейти на сайт, чтобы подтвердить ее данные. При этом ссылка ведет на фальшивый сайт банка, который очень похож на настоящий и может отличаться лишь одной буквой в адресе.

Часто используется голосовой фишинг – вишинг. Вам может поступить письмо от якобы банка с просьбой позвонить по номеру телефона. Голосовой автоответчик просит вас ввести данные вашей карты. В результате мошенники получают доступ к вашим данным.

Бывает, что мошенники представляются банковским работникам и сообщают о том, что с вашей карты прошла подозрительная оплата или взят кредит на ваше имя. Просят скорее подтвердить ваши данные. При любых подобных звонках прерывайте разговор и сами звоните в банк.

Также в Сети на сайтах есть немало примеров **кибермошенничества**. Вам могут предложить отправить СМС. И с вашего телефона будут периодически сниматься определенные суммы.

Могут сообщить, что вы стали победителем конкурса, и попросить для получения приза заполнить форму. Вписать ваши паспортные данные, номер и полные данные вашей кредитной карты.

Встречаются варианты, когда предлагают выкупить товар по очень низкой цене. И сначала предлагают перевести деньги. Имейте в виду, это тоже могут быть мошенники.

Как определить, что компьютер заражен вредоносной программой

- Компьютер часто зависает – он включен, запущены программы, но не реагирует на нажатие клавиш и манипуляции мышью.
- Изменяется внешний вид окон программ и системных сообщений Возникают схожие с системными сообщения, содержащие шутки или бессмысленные наборы символов.
- Невозможно открыть диск или какую-либо папку.
- Компьютер внезапно перезагружается, хотя скачков напряжения и команд на перезагрузку не было.
- Клавиши на клавиатуре «меняются ролями» – например, «пробел» вдруг начинает срабатывать как клавиша Esc.
- Перестают открываться все или некоторые интернет-сайты (как правило, первыми блокируются сайты антивирусных компаний).
- Изменяются настройки браузера (зачастую сбрасываются опции безопасности и подменяется домашняя страница).
- Папки или файлы изменяются без участия пользователя.

Что такое антивирусная программа и как ее выбрать

Антивирусная программа (далее – антивирус) – это специальная программа, предназначенная для борьбы с различными вирусами и вредоносными программами. Антивирус рекомендуется устанавливать на любой компьютер, желательно до первого выхода в интернет.

При выборе антивируса необходимо обратить внимание на следующий параметр: восстановление («лечение») зараженных файлов и папок. Для антивируса обязательно должно быть предусмотрено постоянное обновление. Поскольку вирусы совершенствуются, должна совершенствоваться и программа, которая борется с ними. Как правило, обновление происходит автоматически при подключении к интернету. Но также можно обновлять антивирус и вручную, зайдя в программу.

Основные задачи антивирусов:

- Проверка файлов и программ на наличие вирусов.
- Контроль интернет-соединения: получаемой и отправляемой информации.
- Сканирование электронной почты.
- Восстановление поврежденных файлов.

Самые распространенные антивирусные программы:

- Антивирус Касперского.
- Eset NOD32.
- Dr. Web.
- McAfee VirusScan.

Установка демонстрационной версии антивирусной программы

Все антивирусные программы – лицензионные и платные. Вы можете приобрести их в магазине. В коробке будет ключ (код) для активации программы. 6.1. Раньше в комплект входил диск с установочными файлами. Теперь антивирусные программы предлагают скачать с сайта производителя. Как правило, это демо-версия, которая будет активна определенный период до 30 дней. Чтобы ее продлить, нужно будет либо купить антивирус (лицензионный ключ) в магазине либо провести оплату на сайте.

6.1

Чтобы скачать демо-версию программы с сайта производителя, необходимо:

1. Зайдите на сайт, например, **www.drweb.com**.
2. Выберите «Демо для дома» в разделе «Скачать».
3. Выбрать антивирус для вашей операционной системы.
4. Следовать инструкциям программы установки антивируса.

Если вы уже имеете серийный номер или ключевой файл интересующего вас продукта, то вам необходимо ввести его в соответствующих полях ввода. Если вы еще не приобрели продукт, то вы можете установить демоверсию продукта, а в дальнейшем приобрести лицензию.

Меры предосторожности в Сети

Во многих случаях лучшая защита для вашего компьютера – это ваш здравый смысл в сочетании с антивирусной программой.

- Никогда не предоставляйте ваши персональные данные людям, в личности которых вы недостаточно уверены. Это все равно, что отдать чужому человеку свой паспорт или ключи от дома.
- Посмотрите, от кого пришла информация с просьбой о подтверждении личных данных. В, казалось бы, известном вам адресе сайта крупной компании может быть изменена лишь одна буква.
- Внимательно относитесь к присланным вам ссылкам на сайты. Иногда это могут быть сообщения от хорошо знакомых вам людей. Просто их почтой или аккаунтом воспользовались мошенники. Если сомневаетесь, позвоните знакомым или напишите, поинтересовавшись, что он вам прислал.
- Игнорируйте спам. Старайтесь эти письма не открывать.

- Игнорируйте сообщения во всплывающих окнах.
- Запомните ваши пароли и PIN-коды. Не храните пароли в компьютере. Придумайте надежный пароль и запишите его в блокнот.
- Безопасность должна быть многоуровневой. Установите и регулярно обновляйте программные продукты, обеспечивающие безопасность компьютера (antivirus, antispyware и antimalware).

Безопасность при расчетах в Сети

Будьте осторожны при совершении онлайн-покупок. Мошенник может узнать номер вашей банковской карты. Используйте веб-сайты, которые обеспечивают безопасность сделок. Также ознакомьтесь с политикой конфиденциальности сайта.

- Все действия с денежными средствами должны подтверждаться банком – например, с помощью СМС.
- Никогда никому не говорите код с обратной стороны карты и пароли из СМС-сообщений от банка — их никогда не спросят сотрудники банка или службы поддержки сайта, где вы покупаете или продаете.
- Во время работы с денежными средствами не должны запускаться иные программы.
- При выборе интернет-магазина обращайте внимание на репутацию компании, положительные отзывы на форумах и контактную информацию для решения вопросов в случае каких-либо нештатных ситуаций.
- При оплате на сайте всегда проверяйте адрес страницы оплаты — он написан в строке браузера вверху страницы. Символы в адресной строке должны начинаться с https — это значит, что данные, которые вы введете в поля для оплаты, будут защищены. Также убедитесь, что в адресной строке корректно написано название сайта, на котором вы совершаете покупку — ошибка даже в одну букву означает, что перед вами подделка.
- Никогда не переходите по ссылкам, которые прислали вам другие пользователи сети, даже если это покупатели или продавцы.
- Не используйте для расчетов через интернет свою основную банковскую карту. Предпочтительно использовать специальные виртуальные карты необходимого номинала.
- Лучше не совершайте платежи с мобильного устройства, особенно если на нем не установлен антивирус. Не работайте со своим счетом в сетях общественного доступа.

Как создать надежный пароль

Один из необходимых способов защиты ваших данных – это создание надежного пароля к электронной почте, к вашим аккаунтам в социальных сетях, к программам и сервисам.

Каким не должен быть пароль

Многие думают, что замена некоторых букв на похожие по написанию цифры, набор русского слова в английской раскладке и инвертирование порядка букв в слове являются способами создания надежного пароля. Это не так.

Не используйте в пароле свое имя или имена своих родственников, клички домашних животных, номер телефона, адрес или дату рождения

Каким должен быть пароль

Чтобы ваш пароль практически невозможно было взломать, придерживайтесь следующих правил при его создании:

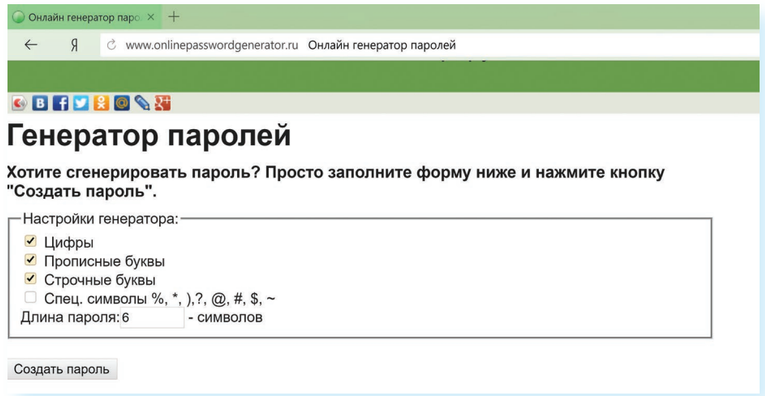
- В пароле должно быть от 8 до 12 символов. Чем длиннее будут ваши пароли, тем сложнее будет их взломать. Используйте не менее 8 символов в паролях, два из которых, по крайней мере, будут цифровыми.
- Используйте максимально возможное количество символов и их комбинации: строчные и прописные буквы, знаки препинания и другие символы – чем больше различных символов в вашем пароле, тем он безопаснее.
- Информация в паролях не должна иметь к вам прямого или косвенного отношения.

Вот пара примеров: **bKriH)23bmWx, j7NTr93BmDel4.**

Для создания надежных паролей существуют сайты-генераторы паролей 6.2. Один из таких ресурсов – **onlinepasswordgenerator.ru**.

Правила создания надежного пароля:

- Используйте от 8 до 12 символов в ваших паролях.
- Должно быть максимально возможное количество символов и их комбинации.
- Используйте в своих паролях информацию, которая не имеет к вам прямого или косвенного отношения.



6.2

Контрольные вопросы

1. Чем опасны для вас и компьютера вредоносные программы?
2. Какие виды мошенничества есть в сети интернет?
3. Зачем необходимо устанавливать на компьютер антивирусную программу?
4. Какие меры предосторожности следует соблюдать при работе в сети интернет?
5. Каким должен быть надежный пароль? Как его придумать?