Меры предосторожности при работе в интернете

Интернет - одно из величайших изобретений в истории. Но и в сети есть мошенники, которые охотятся за доверчивыми пользователями. Если соблюдать простые правила и быть внимательными, с мошенничеством в Интернете вы никогда не столкнетесь.

Фишинг - это хищение ваших личных данных пользователей в Интернете. Мошенники могут украсть ваш электронный адрес, пароль или даже номер кредитной карты, чтобы потом снять деньги с вашего банковского счета.

Большинство сервисов электронной почты позволяют пользователям сообщать о подозрительных письмах и фишинге. Если вы сообщите о том, что определенное письмо связано с фишингом, его автор будет заблокирован и больше не сможет отправлять вам сообщения.

Настороженно относитесь ко всем сайтам, где вас просят ввести личную информацию.

Мошенники могут прислать вам письмо от имени банка с предложением узнать, не находится ли ваша кредитная карта в списке мошенников. Никогда не отвечайте на такие письма.

Мошенники могут создать сайт, похожий на настоящий. Например, **www.goog.le.ru**. Когда вы введете свой логин и пароль на таком сайте, они могут быть украдены. Всегда проверяйте правильное написание сайта, на который заходите.

Никогда не вводите пароль на неизвестном вам сайте, на который вы попали по ссылке из электронного письма или сообщения. Лучше зайти на такую страницу напрямую из поисковика.

Как создать надежный пароль

Как создать надежный пароль для регистрации на сайтах или для создания почтового ящика:

1. В пароле обязательно должны быть буквы и цифры.

2. В качестве пароля можно использовать словосочетание. Например, вы можете придумать фразу «Мой внук Вася 1 раз в день присылает мне смешные письма», затем взять первую букву каждого слова, написав ее латиницей. В результате получится «MvV1rvdpmsp». Такой пароль злоумышленники угадать не смогут.

3. Используйте разные пароли для разных сайтов, а не один для всех. Не забывайте записывать их, иначе запутаете не только мошенников, но и себя.

4. Информация в паролях не должна иметь к вам прямого или косвенного отношения.

✓ *Не оставляйте памятки с паролями в доступных местах, на компьютере или на столе. Если вы храните пароль в файле на компьютере, назовите*

этот файл так, чтобы никто не мог понять, что в нем содержится. Не стоит называть его, например, «Мои пароли».

Как уберечься от компьютерных вирусов

Компьютерные вирусы - это вирусы, которые могут заразить файлы, сайты, а через них - компьютеры.

Откуда появляются вредоносные программы на компьютере?

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.

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.

Основные задачи антивирусов:

✓ Проверка файлов и программ на наличие вирусов (сканирование) в режиме реального времени.

✓ Контроль интернет-соединения (получаемой и отправляемой информации).

✓ Сканирование электронной почты.

- ✓ Защита от атак враждебных веб-узлов.
- ✓ Восстановление поврежденных файлов.

При выборе антивируса необходимо обратить внимание, чтобы он мог «лечить» зараженные файлы и папки. Для антивируса обязательно должно быть предусмотрено постоянное обновление. Поскольку вирусы совершенствуются, то 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. Самые распространенные антивирусные программы:

Антивирус Касперского
Eset NOD32
Dr. Web
McAfee VirusScan

Все антивирусные программы – лицензионные и платные. Вы можете приобрести их в магазине и установить с диска. В коробке также будет ключ (код) для активации программы. Также установочные файлы для антивирусной программы вы можете всегда скачать с сайта производителя.

Для начала можете установить на компьютер бесплатно демоверсию. Она рассчитана на 30 дней.

Советы

- ✓ Если вы попали на незнакомый сайт и что-то кажется вам подозрительным, закройте его, нажав на значок **X** в правом верхнем углу.
- ✓ Если на незнакомом сайте вам предлагают скачать программу, но она вам не нужна, откажитесь.
- ✓ Подумайте, прежде чем перейти по ссылке или загрузить файл. При переходе по незнакомым адресам ваш компьютер может быть атакован вредоносными приложениями или сайтами. Такие программы могут сканировать компьютер или отслеживать нажатия кнопок, чтобы похитить ваши пароли.
- ✓ Загружайте файлы только из надежных источников. Если что-то кажется вам подозрительным, не нажимайте на ссылку.

Спам и реклама в интернете

Спам - это письма, которые приходят на вашу электронную почту от рекламодателей или людей, которых вы не знаете. Не обязательно, но вполне возможно, что в этих письмах содержатся вирусы. Также из письма вас могут перенаправить на сайты, где попросят указать адрес вашей почты или номер кредитной карты.

Реклама в интернете чаще полезная, но также может быть и недобросовестной. Игнорируйте интернет-рекламу, которая предлагает неправдоподобно выгодные условия на покупку автомобиля или отдых за рубежом. Если пред-

ложение в рекламном объявлении выглядит слишком заманчиво, скорее всего, это обман.

✓ Не открывайте письма от компаний или людей, которых вы не знаете. Сразу удаляйте их из почты.

✓ Игнорируйте спам. Старайтесь эти письма не открывать.

✓ Игнорируйте сообщения во всплывающих окнах.

✓ Объявления на сайтах, в которых вас поздравляют с тем, что вы стали миллионным посетителем веб-сайта, предлагают призы за участие в опросе или рекламируют быстрый и несложный способ заработка («как разбогатеть, работая из дома всего два часа в день!») опасны. Не верьте им, как бы сильно этого не хотелось. Бесплатный сыр бывает только в мышеловке, даже в интернете.

Безопасность при расчетах в Сети

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

✓ Сравнивайте цены на аналогичные товары в других магазинах. Если цена на товар в одном из магазинов значительно ниже, будьте осторожны: узнайте больше о продавце и расспросите о состоянии товара.

✓ Сохраняйте все квитанции и чеки! Электронная или бумажная квитанция пригодится, если придется возвращать товар или оспаривать неправомерные списания с вашего счета.

✓ Проверяйте незнакомые магазины! Если вы ничего раньше не покупали в них, убедитесь, что они действуют легально. Например, поищите в интернете отзывы покупателей об этом магазине.

✓ Читайте написанное мелким шрифтом: перед покупкой изучите правила отгрузки и возврата товара, а также гарантийные обязательства.

✓ Будьте осторожны при совершении покупок: помните, что интернет - магазин, как и банк, никогда не будет требовать ваши пароли или пинкоды.

✓ Во время работы с денежными средствами не должны запускаться иные программы, тем более неизвестного назначения и от неизвестных отправителей. Возможность посещения внешних ресурсов и сайтов должна быть ограничена.

✓ Все действия с денежными средствами должны подтверждаться банком – например, с помощью СМС.

✓ При выборе интернет-магазина отдавайте предпочтение тем сайтам, которые имеют подтвержденную репутацию, положительные отзывы на форумах и контактную информацию для решения вопросов в случае каких-либо нештатных ситуаций.

✓ 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.

Безопасность должна быть многоуровневой. Установите и регулярно обновляйте программные продукты, обеспечивающие безопасность компьютера (antivirus, antispyware и antimalware).

Вопросы для повторения

1. Чем опасны для вас и компьютера вредоносные программы?
2. Какие есть виды мошенничества 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?