Что надо знать

об Интернет-безопасности?

Интернет - это виртуальное пространство, которое обладает как плюсами так и минусами.
Зачастую огромные возможности, предоставляемые нам службами и ресурсами этой глобальной сети, перечеркиваются реальными угрозами нашему спокойствию и безопасности.
За безопасностью пользователей следят как государственные структуры, так и сотрудники Интернет-сервисов.
Тем не менее, ежедневно появляются новые жертвы, чаще всего пострадавшие от собственной неосведомленности.
Предлагаем Вам ознакомиться с основами безопасной работы с интернет-сервисами и ресурсами.

Некоторые полезные советы:

7 советов по компьютерной безопасности

БЕЗОПАСНОСТЬ В СЕТИ

Обычно подготовка к школе заключалась в укладывании в портфель карандашей, тетрадей и учебников. Сегодня в начале этого списка нередко находится компьютер. Ознакомьтесь с этими советами, чтобы защитить компьютеры, которыми вы пользуетесь в школе, от вирусов, хакеров, программ-шпионов и других возможных атак.

1. Соблюдайте основные меры компьютерной безопасности

Перед тем, как отправиться в путешествие по интернету, необходимо выполнить три важных действия для усиления компьютерной защиты.

1. **Активизации брандмауэра**
2. **Обновления антивирусных программ**
3. **Обновления программного обеспечения**

2. Не открывайте файлы, полученные от неизвестных корреспондентов

Электронная почта и мгновенные сообщения позволяют быстро обменяться информацией с друзьями, родственниками и одноклассниками. Но если не проявить необходимой осторожности, электронная почта и мгновенные сообщения могут распространить вирусы и черви. Основная масса вредоносных программ попадает в компьютер через электронную почту теми, кто нечаянно попытался открыть зараженный файл. Не дайте себя одурачить! Ни в коем случае нельзя открывать файл, вложенный в письмо электронной почты или мгновенное сообщение, если его отправитель неизвестен и вы не ожидаете получения файла. Дополнительные сведения, которые помогут защититься от вирусов и червей, можно найти в разделе Как защититься от вирусов. Советы по безопасному использованию служб мгновенных сообщений можно получить в разделе Советы по безопасности мгновенного обмена сообщениями и защите личной информации.

3. Как бороться со спамом и сетевыми мошенниками

Нужно также освоить способы борьбы со спамом и сетевым мошенничеством. Чтобы узнать, как освободить время для школьных дел и развлечений, избавившись от необходимости удалять спам, прочитайте разделы «Как предотвратить получение спама по электронной почте» и «Пять запрещенных и три необходимых действия, позволяющих справиться со спамом в электронной почте»
Мошенничество phishing представляет собой еще одну угрозу конфиденциальности ваших данных. У вас могут украсть номер кредитной карты, пароли, учетную информацию или другие личные данные. Для ознакомления со способами защиты обратитесь к разделу Мошеннические письма: пять способов защиты личных данных.

4. Как защититься от программ-шпионов

Ваш браузер погряз во всплывающих окнах? На экране компьютера появились панели, которые вы не загружали? Возможно, вы стали жертвой программы-шпиона. Она занимается сбором вашей личной информации, не предупреждая об этом и не спрашивая на то разрешения. Получить эту вредоносную программу можно при скачивании музыки или программ обмена файлами; загрузки бесплатных игр с подозрительных сайтов или других программ. Чтобы ознакомиться с признаками программ-шпионов и узнать, как избежать заражения компьютера, прочитайте раздел Что из себя представляет программа-шпион?

5. Принимайте необходимые меры предосторожности, пользуясь беспроводной связью

В настоящее время многие высшие учебные заведения и колледжи оснащены беспроводными сетями. Это дает возможность путешествовать по интернету, находясь в библиотеке, кафе или учебной аудитории. Возможно, вы уже пользовались беспроводными сетями дома, в аэропорту, кафетериях или даже общественных парках. Такие сети очень удобны, но их использование сопряжено со снижением уровня безопасности. Если вы устанавливаете беспроводную сеть дома, прочитайте раздел Защита домашней сети и обратите особое внимание на информацию о безопасности. Прочитайте также раздел Безопасное использование беспроводных сетей общего пользования, чтобы получить три дополнительных совета по безопасности WiFi-соединений.

6. Пароль защищает ваш компьютер и блокирует возможность его использования

Пароли являются первой линией защиты от злоумышленников, шутников или беспечного соседа по комнате. Если вы не пользуетесь паролем для входа в компьютер, кто угодно может получить доступ. Прямо сейчас, не откладывая в долгий ящик, воспользуйтесь нашими рекомендациями по созданию надежных паролей и всегда блокируйте доступ к компьютерной системе на то время, когда вы с ней не работаете. (Чтобы «запереть» компьютер с операционной системой Windows,

удерживайте нажатыми клавиши «Windows + L». Когда понадобится возобновить работу, следуйте инструкциям на экране)

7. Делайте резервные копии результатов работы (а также игр и других развлекательных программ)

Образ студента, оставшегося без своей курсовой работы из-за того, что он забыл сделать резервную копию, стал уже почти штампом. Тем не менее многие до сих пор не находят времени на копирование. Пользователи Windows XP, могут воспользоваться программой Архивация данных, которая выполнит за вас эту работу. О том, как ею пользоваться, читайте в разделе удобное копирование с помощью Архивации данных Windows XP.