Памятка для школьников

Как защититься от компьютерных вирусов

Компьютерный вирус - это программа, которая может создавать свои копии. Вирусы повреждают или полностью уничтожают файлы на зараженном компьютере и всю операционную систему в целом. В большинстве случаев распространяются вирусы через интернет.

1. Загрузи современную операционную систему. Используй современные операционные системы с высоким уровнем защиты от вредоносных программ.

2. Обновляй операционную систему. Включи режим автоматического обновления операционной системы. Если в системе нет такого режима, регулярно устанавливай обновления самостоятельно. Загружай их с официального сайта разработчика.

3. Используй права пользователя. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ автоматически установиться.

4. Не рискуй. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;

5. Ограничь физический доступ к своему компьютеру. Не разрешай посторонним пользоваться своим компьютером.

6. Выбирай тщательно источники. Копируй и загружай файлы только с проверенных съемных носителей или интернет - ресурсов. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Памятка для школьников

Как безопасно пользоваться сетью Wi-Fi

Wi-Fi - это беспроводной способ передачи данных с помощью радиосигналов.В кафе, отелях и аэропортах часто можно бесплатно выйти в интернет черезWi-Fi. Но общедоступные Wi-Fi сети не являются безопасными.

1. Не передавай свою личную информацию через общедоступные Wi-Ficети. Желательно не вводить пароли доступа, логины и номера.

2. Используй и обновляй антивирусные программы и брандмауер. Темсамым ты обезопасишь себя от закачки вируса на твое устройство.

3. При использовании Wi-Fi отключи функцию "Общий доступ к файлам ипринтерам". Данная функция закрыта по умолчанию, однако некоторыепользователи активируют ее для удобства использования в работе или учебе.

4. Не используй публичный WI-FI для передачи личных данных.Например, для выхода в социальные сети или в электронную почту;

5. Используй только защищенное соединение через HTTPS, а не HTTP. Тоесть при наборе веб-адреса вводи именно https://.

6. В мобильном телефоне отключи функцию "Подключение к Wi-Fiавтоматически". Не допускай автоматического подключения устройства ксетям Wi-Fi без твоего согласия.

Памятка для школьников

Как безопасно общаться в социальных сетях

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей.

2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы.

3. Защищай свою репутацию. Держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить.

4. Не используй свое реальное имя. Когда в сети разговариваешь с незнакомыми людьми, не называй и не используй реальное имя. Не раскрывай информацию о себе: место жительства, место учебы и прочее.

5. Не сообщай свое местоположение. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;

6. Используй сложные пароли. При регистрации в социальной сети пиши сложные пароли. Они должны содержать не менее восьми знаков и включать в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак.

7. Используй разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Памятка для школьников

Как безопасно расплачиваться электронными деньгами

Электронные деньги - это очень удобный способ платежей, однако существуютмошенники, которые хотят получить эти деньги.

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов - анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в персонифицированных идентификация пользователя является обязательной.

1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства.

2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;

3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли - это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, $tR0ng!;;

4. Береги личные данные. Не вводи свои личные данные на сайтах, которым не доверяешь.

Памятка для школьников

Как безопасно пользоваться электронной почтой

Электронная почта - это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

1. Выбери правильный почтовый сервис. В интернете много бесплатных. Однако почту лучше заводить на популярном сервисе, которым уже пользуются твои знакомые.

2. Не пиши о себе в адресе почты. Не указывай в почтовом адресе личную информацию. Например, лучше выбрать "музыкальный_фанат@" или "рок2013" вместо "тема13".

3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;

4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль.

5.Используй проверочный вопрос. Придумай сам свой личный вопрос для идентификации, если сервис дает такую возможность.

6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах.

7. Не открывай вложения писем. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

8. Выходите из почты. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на "Выйти".

Памятка для школьников

Как защититься от кибербуллинга или виртуального издевательства

Кибербуллинг - преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт.

2. Управляй своей киберрепутацией.

3. Выясни, кто стоит за анонимным аккаунтом. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом.

4. Не веди хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно.

5. Соблюдай свою виртуальную честь смолоду.

6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.

7. Блокируй отправку сообщений. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.

8. Сообщи о факте агрессивного поведения в сети. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

Памятка для школьников

Как безопасно пользоваться смартфоном, планшетом

1.Будь осторожен. Когда тебе предлагают бесплатный контент, в нем могут быть скрыты платные услуги.

2.Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?

3.Обновляй операционную систему смартфона. Это дополнительная защита.

4.Используй антивирусные программы для смартфонов. Регулярно обновляй их.

5.Не загружай приложения от неизвестного источника. Они могут содержать вредоносное программное обеспечение.

6. Зайди в настройки браузера и удали cookies. Сделай это сразу после того, как ты выйдешь с сайта, где вводил личную информацию.

7. Проверяй платные услуги на твоем номере. Иногда могут активировать новые.

8. Не всем давай номер телефона. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь.

9. Выключай Bluetooth, когда ты им не пользуешься. Не забывай иногда проверять это.

Памятка для школьников

Как безопасно играть Online

Online-игры - это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

1. Блокируй неадекватов. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков.

2. Пожалуйся администраторам игры на поведение агрессивного игрока. Желательно приложить какие-то доказательства в виде скринов.

3. Будь осторожен. Не указывай личную информацию в профайле игры.

4. Следи за своим поведением. Уважай других участников по игре.

5. Устанавливай проверенные утилиты. Избегай неофициальных патчей и модов.

6. Берегись от взлома. Используй сложные и разные пароли;

7. Не отключай антивирус во время игры. Пока ты играешь, твой компьютер могут заразить.

Памятка для школьников

Как защититься от фишинга или кражи личных данных

Фишинг (от английского слова fishing - рыбная ловля) – вид нтернет-мошенничества. Его главная цель получить конфиденциальные данные пользователей - логины и пароли.

1. Следи за своим аккаунтом. Если ты подозреваешь, что твой аккаунт взломали, то необходимо заблокировать его и сообщить администраторам ресурса об этом как можно скорее.

2. Используй безопасные веб-сайты. в их числе - сайты интернет-магазинов и поисковых систем.

3. Используй сложные и разные пароли. Если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем.

4. Предупреди своих знакомых, которые добавлены у тебя в друзья, если тебя взломали. От твоего имени будет рассылаться спам и ссылки на фишинговые сайты.

5. Спрячь данные. Установи надежный пароль (PIN) на мобильный телефон.

6. Отключи сохранение пароля в браузере. Сохраненные пароли крадут чаще.

7. Не открывай файлы и другие вложения в письмах. Даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Памятка для школьников

Что такое авторское право

Чтобы использовать возможности цифрового мира, нужно соблюдать права наинтеллектуальную собственность. Термин интеллектуальная собственностьотносится к различным творениям человеческого ума, начиная с новыхизобретений и знаком, обозначающих собственность на продукты и услуги, изаканчивая книгами, кинофильмами и музыкальными произведениями.

Авторские права – это права на интеллектуальную собственность – напроизведения науки, литературы и искусства. Авторские права выступают какгарантия возможностей автора заработать на результатах своего труда,получить известность и признание. Никто без разрешения автора не можетвоспроизводить его произведение, распространять, публично демонстрировать,продавать или размещать в интернете.

«Пиратское» программное обеспечение несет в себе многие риски: от потериданных до блокировки устройства, где установлена нелегальная программа. Незабывайте, что в Сети можно найти легальные и бесплатные программы сосходным функционалом.