РЕГИОНАЛЬНЫЙ ЦЕНТР СПОРТИВНОЙ ПОДГОТОВКИ ПО АДАПТИВНЫМ ВИДАМ СПОРТА
Красноярский край

Компьютерные вирусы

КИБЕРБЕЗОПАСНОСТЬ В СЕТИ «ИНТЕРНЕТ»

Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению (копированию). В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Как защитить себя от компьютерных вирусов?

1. Используйте современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;

2. Постоянно устанавливайте патчи (обновления, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивайте их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включите его;

3. Работайте на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на вашем персональном компьютере;

4. Используйте антивирусные программные продукты известных производителей, с автоматическим обновлением баз;

5. Ограничьте физический доступ к компьютеру для посторонних лиц;

6. Используйте внешние носители информации, такие как флешка, диск или файл из Интернета, только из проверенных источников;

7. Не открывайте компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислали ваши знакомые. Уточните, отправляли ли они данные файлы.

РЕГИОНАЛЬНЫЙ ЦЕНТР СПОРТИВНОЙ ПОДГОТОВКИ ПО АДАПТИВНЫМ ВИДАМ СПОРТА
Красноярский край

Сети WI-FI

КИБЕРБЕЗОПАСНОСТЬ В СЕТИ «ИНТЕРНЕТ»

С помощью WI-Fi можно получить бесплатный интернет-доступ в общественных местах: кафе, отелях, торговых центрах и аэропортах. Так же WI-Fi является отличной возможностью выхода в Интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работы в общедоступных сетях Wi-fi

Не передавайте свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-либо номера

Используйте только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводите именно «https://»

При использовании Wi-Fi отключите функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе

Используйте и обновляйте антивирусные программы и брандмауэр. Тем самым вы обезопасите себя от закачки вируса на свое устройство

В мобильном телефоне отключите функцию «Подключение к Wi-Fi автоматически».
Не допускай автоматического подключения устройства к сетям Wi-Fi без вашего согласия

Не используйте публичный WI-FI для передачи личных данных, например, для выхода в социальные сети или в электронную почту

РЕГИОНАЛЬНЫЙ ЦЕНТР СПОРТИВНОЙ ПОДГОТОВКИ ПО АДАПТИВНЫМ ВИДАМ СПОРТА
Красноярский край

Социальные сети

КИБЕРБЕЗОПАСНОСТЬ В СЕТИ «ИНТЕРНЕТ»

Социальная сеть - это сайт, который предоставляет возможность людям осуществлять общение между собой в интернете. Чаще всего в них для каждого человека выделяется своя личная страничка, на которой он указывает о себе различную информацию, начиная от имени, фамилии и заканчивая личными фотографиями. 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

Советы по безопасности в социальных сетях

Во-первых,

1. Ограничьте список друзей. У вас в друзьях не должно быть случайных и незнакомых людей;

2. Защищайте свою частную жизнь. Не указывайте пароли, телефоны, адреса, дату своего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как вы и ваши близкие планируете провести каникулы;

Во-вторых,

3. Защищайте свою репутацию - держите ее в чистоте и задавайте себе вопрос: хотели бы вы, чтобы другие пользователи видели, что вы загружаете? Подумайте, прежде чем что-то опубликовать, написать и загрузить;

4. Если вы говорите с людьми, которых не знаете, не используйте свое реальное имя и другую личную информацию: имя, место жительства, место работы (учебы) и прочее

В-третьих,

5. Избегайте размещения фотографий в Интернете, где вы изображены на местности, по которой можно определить ваше местоположение;

6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;

7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда, если вас взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу

РЕГИОНАЛЬНЫЙ ЦЕНТР СПОРТИВНОЙ ПОДГОТОВКИ ПО АДАПТИВНЫМ ВИДАМ СПОРТА
Красноярский край

Электронные деньги

КИБЕРБЕЗОПАСНОСТЬ В СЕТИ «ИНТЕРНЕТ»

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 не анонимных идентификации пользователя является обязательной. Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Советы по безопасной работе с электронными деньгами

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

2 Используйте одноразовые пароли. После перехода на усиленную авторизацию вам уже не будет угрожать опасность кражи или перехвата платежного пароля

3 Выберите сложный пароль. Преступникам будет непросто 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, StROng!

4 Не вводите свои личные данные на сайтах, которым не доверяете.

РЕГИОНАЛЬНЫЙ ЦЕНТР СПОРТИВНОЙ ПОДГОТОВКИ ПО АДАПТИВНЫМ ВИДАМ СПОРТА
Красноярский край

Электронная почта

КИБЕРБЕЗОПАСНОСТЬ В СЕТИ «ИНТЕРНЕТ»

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.

Советы по безопасной работе с электронной почтой

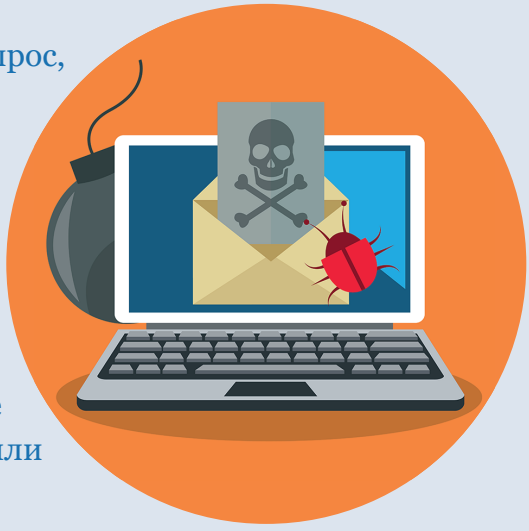
1. Надо выбрать правильный почтовый сервис. В Интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, которых вы знаете и кто из них первый в рейтинге;

2. Не указывайте в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «рома13»;

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

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

5. Если есть возможность написать самому свой личный вопрос, используйте эту возможность;



6. Используйте несколько почтовых ящиков. Первый для частной переписки с адресатами, которым вы доверяете. Этот электронный адрес не надо использовать при регистрации на форумах и сайтах;

7. Не открывайте файлы и другие вложения в письмах даже если они пришли от ваших друзей. Лучше уточни, отправляли ли они вам эти файлы;

8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудьте нажать на «Выйти».

РЕГИОНАЛЬНЫЙ ЦЕНТР СПОРТИВНОЙ ПОДГОТОВКИ ПО АДАПТИВНЫМ ВИДАМ СПОРТА
Красноярский край

Кибербуллинг или виртуальное издевательство

КИБЕРБЕЗОПАСНОСТЬ В СЕТИ «ИНТЕРНЕТ»

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернетсервисов

Как бороться с кибербуллингом?

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

Ведите себя вежливо

Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все ваши действия и сохраняет их. Удалить их будет крайне затруднительно

Не бросайтесь в бой. Успокойтесь. Если вы начнете отвечать оскорблениями на оскорбления, только больше разожжете конфликт

Управляйте своей киберрепутацией

Если вы свидетель кибербуллинга. Ваши действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь

Ограничьте доступ агрессору. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов

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

РЕГИОНАЛЬНЫЙ ЦЕНТР СПОРТИВНОЙ ПОДГОТОВКИ ПО АДАПТИВНЫМ ВИДАМ СПОРТА
Красноярский край

Мобильный телефон

КИБЕРБЕЗОПАСНОСТЬ В СЕТИ «ИНТЕРНЕТ»

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для персональных компьютеров, то же самое касается и мобильных приложений

Советы для безопасности мобильного телефона

1. Будьте осторожны, ведь когда вам предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги

2. Думайте, прежде чем отправить SMS, фото или видео. Вы точно знаете, где они будут в конечном итоге?

3. Необходимо обновлять операционную систему вашего смартфона;

4. Используйте антивирусные программы для мобильных телефонов;

5. Не загружайте приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;

6. После того как вы выйдете с сайта, где вводили личную информацию, зайдите в настройки браузера и удалите cookies;

7. Периодически проверяйте, какие платные услуги активированы на вашем номере мобильного телефона;

8. Давайте свой номер мобильного телефона только людям, которых вы знаете и кому доверяете;

9. Bluetooth должен быть выключен, когда вы им не пользуетесь. Не забывайте иногда проверять это.

РЕГИОНАЛЬНЫЙ ЦЕНТР СПОРТИВНОЙ ПОДГОТОВКИ ПО АДАПТИВНЫМ ВИДАМ СПОРТА
Красноярский край

Фишинг или кража личных данных

КИБЕРБЕЗОПАСНОСТЬ В СЕТИ «ИНТЕРНЕТ»

Главная цель фишинга - вида Интернет-мошенничества, состоит в получении конфиденциальных данных пользователей — логинов и паролей. На английском языке phishing читается как фишинг (от fishing — рыбная ловля, password — пароль)

Как бороться с фишингом?

Используйте сложные и разные пароли. Таким образом, если злоумышленники взломают ваш аккаунт, то получат доступ только к одному вашему профилю в сети, а не ко всем

Не открывайте файлы и другие вложения в письмах даже если они пришли от ваших друзей. Лучше уточните, отправляли ли вам эти файлы

Установите надежный пароль (PIN) на мобильный телефон

Отключите сохранение пароля в браузере

Используйте безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем

Следите за своим аккаунтом. Если вы подозреваете, что ваша анкета была взломана, необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее

Если вас «взломали», необходимо предупредить об этом всех знакомых, которые добавлены у вас в друзьях, так как, возможно, им от вашего имени будет рассылаться спам и ссылки на фишинговые сайты