



Управление Роскомнадзора по Иркутской области информирует...

Правила безопасности в сети Интернет для тебя и твоих друзей

Компьютерные вирусы



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.

Способы защиты от вредоносных программ:

- Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ.
- Постоянно устанавливай патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика операционной системы. Если существует режим автоматического обновления, включи его.
- Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоём персональном компьютере.
- Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз.
- Ограничь физический доступ к компьютеру для посторонних лиц.
- Используй внешние носители информации, такие как флешка, диск или файл из Интернета, только из проверенных источников.
- Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI



С помощью *WI-Fi* можно получить бесплатный интернет-доступ в общественных местах: кафе, отелях, торговых центрах и аэропортах. Также он 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 передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера.
- ✓ Используй и обновляй антивирусные программы и брандмауэр. Тем самым ты обезопасишь себя от закачки вируса на твое устройство.
- ✓ При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе.
- ✓ Не используй публичный WI-FI для передачи личных данных, например, для выхода в социальные сети или в электронную почту.
- ✓ Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://».
- ✓ В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Социальные сети

Социальная сеть – это сайт, который предоставляет возможность людям осуществлять общение между собой в Интернете.

Чаще всего в социальных сетях 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.

Основные советы по безопасности в социальных сетях:

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



- 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.

- 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.

- Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее.

- Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твоё местоположение

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

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

Электронные деньги

Электронные деньги – это очень удобный способ платежей, однако существуют мошенники, которые пытаются 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 **два вида**: анонимные и неанонимные. Разница в том, что **анонимные** – это те, в которых разрешается проводить операции без идентификации пользователя, а в **неанонимных** идентификации пользователя является обязательной.

Также следует различать электронные фиатные деньги (*равны государственным валютам*) и электронные нефидатные деньги (*не равны государственным валютам*).

Основные советы по безопасной работе с электронными деньгами:

- 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.

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



- 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, StROng!
- Не вводи свои личные данные на сайтах, которым не доверяешь.

Электронная почта



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, в электронной почте имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

- ✓ Надо выбрать правильный почтовый сервис. В Интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге.
- ✓ Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13».
- ✓ Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS.
- ✓ Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль.
- ✓ Если есть возможность написать самому свой личный вопрос, используй эту возможность.
- ✓ 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.
- ✓ 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.
- ✓ После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

Кибербуллинг или виртуальное издевательство



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

Основные советы по борьбе с кибербуллингом:

- 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.
- Управляй своей киберрепутацией.
- Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом.
- Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно.
- Веди себя вежливо.
- Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.
- Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.
- Если ты свидетель кибербуллинга, то 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.

Мобильный телефон



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 ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

- Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги.
- Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
- Периодически обновляй операционную систему твоего смартфона.
- Используй антивирусные программы для мобильных телефонов.

- Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение.
 - После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies.
 - Периодически проверяй какие платные услуги активированы на твоём номере.
 - Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь.
 - Bluetooth должен быть выключен, когда ты им не пользуешься.
- Не забывай иногда проверять это.

Фишинг или кража личных данных



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).

Основные советы по борьбе с фишингом:

- ✓ Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее.
- ✓ Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем.
- ✓ Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем.
- ✓ Если твой аккаунт взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что он взломан и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты.
- ✓ Установи надежный пароль (PIN) на мобильный телефон.
- ✓ Отключи сохранение пароля в браузере.
- ✓ 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.