

Информационная безопасность учащимся ГБОУ «Романовская школа»



Безопасность данных и правила общения в сети Интернет

НЕЛЬЗЯ:

- Сообщать свои персональные данные: ФИО, телефон, адрес проживания, прописки, обучения, серию и номер паспорта, номер карты или банковского счёта, а также отправлять фотографии свои, своих близких и важных документов (паспорта, медицинского полиса, свидетельства о рождении). Исключением являются проверенные сайты муниципалитета, такие, как «Мос.ру» и «Госуслуги»;
- Открывать вложенные файлы электронной почты, пришедшие с незнакомого адреса
- Переходить по ссылкам, безопасность которых не подтверждена;
- Грубить, придираться, оказывать давление — вести себя невежливо и агрессивно;
- Проводить оплату услуг через интернет без одобрения родителей или опекунов;
- Приходить на встречи с интернет-знакомыми в реальной жизни, не уведомив близких об этом и не получив их совета.

Безопасность данных и правила общения в сети Интернет

ОСТОРОЖНО:

- Большая часть сайтов в сети Интернет содержит неподтверждённую информацию. Не следует использовать её для подготовки к занятиям, не проверив в надёжных источниках: энциклопедиях, справочниках, учебниках;
- При обнаружении в сети Интернет клеветы на себя или своих близких следует обратиться к родителям или опекунам;
- Не стоит близко общаться с собеседниками, которые избегают личных встреч, отказываются от видеозвонков и не имеют с вами общих знакомых.
- Обо всех происшествиях в Интернете следует сообщать взрослым.
- Скачивать файлы с сайтов, не являющихся официальными, можно только при наличии на устройстве антивирусных программ.
- Следует использовать настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и других порталах.

Безопасность данных и правила общения в сети Интернет

МОЖНО:

- Общаться с другими пользователями уважительно и не отвечать на оскорбления: возможно, они являлись изначальной целью диалога;
- Делать ссылку на использованный интернет-источник, указывая дату обращения.
- При возникновении конфликтных ситуаций обращаться к администраторам сайтов, родителям или опекунам;
- Использовать услуги блокировки рекламы (AddBlock);
- Вовремя продлевать действие антивирусных программ.

Информационная памятка для обучающихся для размещения на официальных Интернет-ресурсах

С каждым годом молодежи в интернете становится больше, а школьники являются одними из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь учащимся безопасно находиться в сети.



Компьютерные вирусы

- это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. 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 вирусы распространяются через интернет.



Методы защиты от вредоносных программ:

- Используй современные операционные системы, имеющие высокий уровень защиты от вредоносных программ;
- Постоянно устанавливай пачти (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. 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.

Cети Wi-Fi



- Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд «WECA», что обозначало словосочетание «Wireless Fidelity», который переводится как «беспроводная точность». До нашего времени дошла другая аббревиатура: «Wi-Fi». Такое название было дано с намеком на стандарт высшей звуковой техники Hi-Fi, что в переводе означает «высокая точность».
- Бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью для выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работе 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 номера телефонов;
- Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закладки вируса на твоё 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 входа 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



Социальные сети активно входят в нашу жизнь, многие люди работают там на постоянной основе, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой от всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, притом 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 информацию: место жительства, место учебы и прочее;
- Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
- При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр, 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 ко всем сразу.

Электронные деньги



— это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор отсутствуют соответствующие законы об их обороте. В России они также функционируют, и относительно их оборота существуют и действуют законы, где их разделяют на несколько видов – анонимные и не анонимные. Разница в том, что с анонимными деньгами разрешается проводить операции без идентификации пользователя, а с неанонимными идентификация пользователя является обязательной.

Основные советы по безопасной работе с электронными деньгами:

- Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ. 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, \$tR0ng!;
- Не вводи свои личные данные на сайтах, которым не доверяешь.

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 прикреплять к сообщениям 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, где зарегистрировано большинство пользователей: Yandex.ru, Mail.ru, Gmail.com.
- Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13»;
- Используй двухэтапную авторизацию: помимо ввода пароля используй 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. Основной - для частной переписки с адресатами, которым ты доверяешь. Этот электронный адрес не стоит 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 выйти из почтового ящика.

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;
- 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;

Мобильные устройства

- Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока недостаточно. 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:

- Ничего не является по-настоящему бесплатным. 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?
- Необходимо обновлять операционную систему твоего смартфона;
- Используй антивирусные программы для мобильных телефонов;
- Не загружай приложения от неизвестного источника, они могут содержать вредоносное программное обеспечение;
- После того как ты выйдешь с сайта, где вводил личную информацию, зайти в настройки браузера и удали cookies;
- Периодически проверяй, какие платные услуги активированы на твоём номере;
- Давай свой номер мобильного телефона только тем людям, которых ты знаешь и кому доверяешь;
- Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Online игры



- Современные онлайн-игры – это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Пользователи исследуют игровой 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 самую 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.

Основные советы по безопасности твоего игрового аккаунта:

- Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;
- Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скриншотов;
- Не указывай личную информацию в профайле игры;
- Уважай других участников по игре;
- Не устанавливай неофициальные патчи и моды;
- Используй сложные и разные пароли;
- Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Фишинг или кража личных данных

- Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет и продолжают заниматься «любимым» делом.
- Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого 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 тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзья, о том, что тебя взломали 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.

Цифровая репутация

- Цифровая репутация - это негативная или позитивная информация о тебе в сети. Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на твоей реальной жизни. «Цифровая репутация» - это твой имидж, который формируется из информации о тебе в сети Интернет.
- Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких – все это накапливается в сети.
- Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу.
- Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

- Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
- В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей»;
- Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

Авторское право

- Современные школьники – активные пользователи цифрового пространства. Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.
- Термин «интеллектуальная собственность» относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.
- Авторские права – это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете.