УРОК №57. ПРАВИЛА БЕЗОПАСНОСТИ РАБОТЫ В СЕТИ ИНТЕРНЕТ

ЗАДАНИЕ:

1.Изучить тему.
2.Составить конспект урока.
3.Пройти онлайн-тест №4 в разделе «Информатика» на портале: https://testedu.ru/.

С каждым годом молодежи в интернете становиться больше, и, как правило, это одна из категорий самых активных пользователей Рунета.

Социальные сети — это один из самых востребованных ресурсов Интернета. Благодаря им сделан огромный шаг вперёд в деле информатизации общества. Это настоящий подарок для любителей интерактивного общения. Казалось бы, чем можно навредить человеку, сидя за монитором? Между тем, помимо огромного количества возможностей, интернет несет и проблемы.

Компьютерные вирусы

Компьютерный вирус – 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. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

• Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;

• Постоянно устанавливай обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;

•Ограничь физический доступ к компьютеру для посторонних лиц;

•Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;

• Работай на своем компьютере под правами пользователя, а не администратора.

• Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;

• 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

Да, бесплатный интернет-доступ в общественных местах является отличной возможностью 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 какие-то номера;

• Используй и обновляй антивирусные программы и брандмауер. 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

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно. 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 твое 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 хотят получить эти деньги.

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.
• 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. Также кроме передачи простого текста, 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;

• Соблюдай свой виртуальную честь смолоду;

•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. 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:

• 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, 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 твоем 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

Обычной кражей денег и документов сегодня уже никого не удивиfшь, 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.

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.

• Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, 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.

Цифровая репутация

Цифровая репутация - это негативная или позитивная информация в сети о тебе. 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 интернете. 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 окружающее 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.

Подставная работа

Интернет уже настолько стал частью нашей жизни, что никого уже не удивишь различными способами *Интернет* заработка. Тем более, что заработок в Интернете во многом может превосходить заработок в реальной жизни и на реальных работах. Есть множество сайтов, которые якобы предлагают различную легкую работу пользователю за неплохие деньги. И вроде вначале не возникает никаких вопросов, насколько может быть законна такая работа, ведь с первого взгляда все довольно честно. Также не возникает у новоиспеченных работников вопросов о том, как обстоят дела с безопасностью на таких сайтах, и не может ли быть сама работа опасной для персональных данных пользователя. Одним из примеров такой работы может быть работа, которая заключается в том, что *пользователь* регистрируется на различных сервисах под своими данными и потом передает эти аккаунты работодателю. Казалось бы, на первый взгляд, нет ничего необычного, работа несложная, *пользователь* делает регистрации, а работодатель платит за это деньги. Но только на первый взгляд такая работа выглядит честной и порядочной, на самом деле работодатель может использовать такие аккаунты для того, чтобы распространять вредоносные программы. Ваш аккаунт может быть использован в любых целях, которые нужны злоумышленнику, вплоть до рекламы каких-либо порнографических вещей, что уже само *по* себе является аморальным.

Также некоторые злоумышленники предлагают работу *по* распознаванию букв с картинки (капча- *распознавание* символов с картинки). При этом они говорят о том, что ничего нелегального в этом нет, а само *распознавание* производится в целях какого-либо научного исследования. *Пользователь* при этом может не знать о том, что такой труд может быть использован для того, чтобы обходить защиту многих сайтов от автоматической регистрации. То есть на стороне злоумышленника создаются различные аккаунты на сайте, основной преградой которых остается как раз капча, которую уже самостоятельно заносят пользователи. Естественно, такие аккаунты могут быть использованы как угодно и в любых целях.

Стоит отметить и то, что не все подобные предложения о работе могут являться предложениями от злоумышленников. Некоторые из таких предложений могут быть предложениями серьезных компаний, которые действительно заинтересованы в различных научных исследованиях в области распознавания символов. Так же и предложения, которые связаны с регистрацией на различных сайтах, вполне могут быть предложениями, которые происходят от вполне честных людей с честными намерениями. Для того, чтобы понять добросовестность человека, который предлагает работу, необходимо проверить его в различных источниках на наличие положительных или отрицательных отзывов на этого человека. Если доминирует большое количество отрицательных отзывов о человеке, то будет лучше поискать другую работу в сети *Интернет*. Также, если у новоиспеченного работодателя нет каких-либо документов, подтверждающих его причастность к крупной компании или научной лаборатории, но этот работодатель говорит, что он на самом деле причастен, то такому работодателю лучше не доверять.