Информационная памятка для обучающихся для размещения на официальных

Интернет-ресурсах.

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

***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, 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.*

*Методы защиты от вредоносных программ:*

1. *Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;*
2. *Постоянно устанавливай пачти (цифровые заплатки, которые автоматически устанавливаются с целью дорабтки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;*
3. *Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;*
4. *Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;*
5. *Ограничь физический доступ к компьютеру для посторонних лиц;*
6. *Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проференных источников;*
7. *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***

*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, которая является такой же технологией. Это аббревиатура «Wi-Fi». Такое название было дано с намеком на стандарт высший звуковой техники Hi-Fi, что в переводе означает «высокая точность».*

*Да, бесплатный интернет-доступ в кафе, отелях и аэропортах 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:*

1. *Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;*
2. *Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;*
3. *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;*
4. *Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;*
5. *Ипользуй только защищенное соединение через HTTPS, а не НТТР, т.е. при наборе веб-адреса вводи именно «https://»;*
6. *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, 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.*

*Основные советы по безопасности в социальных сетях:*

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. *Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;*
5. *Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое 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 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.*

*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 неанонимных идентификации пользователя является обязательной.*

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

*Основные советы по безопасной работе с электронными деньгами:*

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. *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, имеется возможность передавать файлы.*

*Основные 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, кого знаешь и кто первый в рейтинге;*
2. *Не указывай в личной почте 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. *Если есть возможность написать самому свой личный вопрос, используй эту 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 файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;*
8. *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:*

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. *Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;*
4. *Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;*
5. *Соблюдай свой виртуальную честь смолоду;*
6. *Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;*
7. *Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;*
8. *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:*

1. *Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;*
2. *Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?*
3. *Необходимо обновлять операционную систему твоего смартфона;*
4. *Используй антивирусные программы для мобильных телефонов;*
5. *Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;*
6. *После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;*
7. *Периодически проверяй какие платные услуги активированы на твоем номере;*
8. *Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;*

1. *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. 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.*

*Основные советы по безопасности твоего игрового аккаунта:*

1. *Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;*
2. *Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;*
3. *Не указывай личную информацию в профайле игры;*
4. *Уважай других участников по игре;*
5. *Не устанавливай неофициальные патчи и моды;*
6. *Используй сложные и разные пароли;*
7. *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 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. На английском языке phishing читается как фишинг (от fishing — рыбная ловля, password — пароль).*

*Основные советы по борьбе с фишингом:*

1. *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;*
2. *Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;*
3. *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;*
4. *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;*
5. *Установи надежный пароль (PIN) на мобильный телефон;*
6. *Отключи сохранение пароля в браузере;*
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;*

***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:*

1. *Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;*
2. *В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей»;*
3. *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 , и 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.*

*Использование «пиратского» программного обеспечения может привести к многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установленный не легальная программа. Не стоит также забывать, что существует легальные и бесплатные программы, которые можно найти в сети.*

***О портале***

*Сетевичок.рф – твой главный советчик в сети. Здесь ты можешь узнать о безопасности в сети понятным и доступным языком, а при возникновении критической ситуации обратиться за советом. А также принять участие в конкурсах и стать самым цифровым гражданином!*