Информационная памятка для обучающихся

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.

1.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.

2.Методы защиты от вредоносных программ:

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

постоянно устанавливай (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС;

используй режим автоматического обновления при наличии;

работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;

используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;

не допускай 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.

3.Сети WI-FI

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в Интернет. Но многие эксперты считают, что общедоступные WiFi сети не являются безопасными.

3.1. 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 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.

4.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.

4.1. 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.

5.Электронные деньги

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

Электронный деньги разделяют на несколько видов электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

5.1. 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.;

не вводи свои личные данные на сайтах, которым не доверяешь.

6. 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.

6.1. 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;

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».

7. Кибербуллинг или виртуальное издевательство

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

7.1. 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.

8. 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.

8.1. 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.

9. 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.

9.1. 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 скринов;

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.

10. 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 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).

10.1. 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 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;

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.

11. 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.

11.1. 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.