Памятка для обучающихся об информационной безопасности детей

НЕЛЬЗЯ

1. Всем подряд сообщать свою частную информацию (настоящее имя, фамилию, телефон, адрес, номер школы, а также фотографии своей семьи и друзей)
2. Открывать вложенные файлы электронной почты, когда не знаешь отправителя
3. Грубить, придираться, оказывать давление – вести себя невежливо и агрессивно
4. Не распоряжайся деньгами твоей семьи без разрешения старших – всегда спрашивай родителей
5. Не встречайся с Интернет - знакомыми в реальной жизни - посоветуйся со взрослым, кому доверяешь.

ОСТОРОЖНО

1. Не все пишут правду. Читаешь о себе неправду в Интернете – сообщи об этом своим родителям или опекунам
2. Приглашают переписываться, играть, обмениваться – проверь, не ли подвоха
3. Незаконное копирование файлов в Интернете – воровство
4. Всегда рассказывай взрослым о проблемах в сети – они всегда помогут
5. Используй настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и других порталах

МОЖНО

1. Уважай других пользователей
2. Пользуешься Интернет - источником – делай ссылку на него
3. Открывай только те ссылки, в которых уверен
4. Общаться за помощью взрослым – родители, опекуны и администрация сайтов всегда помогут
5. Пройди обучение на сайте «Сетевичок» и получи паспорт цифрового гражданина!

Информационная памятка для обучающихся для размещения на официальных Интернет-ресурсах.

С каждым годом молодежи в интернете становится всё больше, а школьники один из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка поможет тебе безопасно находиться в сети.

Компьютерные вирусы – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут уничтожить все файлы и данные

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 доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика
3. Работай на своем компьютере под правами пользователя, а не администратора.
4. Используй антивирусные программы
5. Ограничь физический доступ к компьютеру для посторонних лиц
6. Используй внешние носители информации, такие как флешка, диск и т.д
7. Не открывай компьютерные файлы, полученные из ненадёжных источников

Советы по безопасности работе в общедоступных сетяхWI-Fi

1. Не передавай свою личную информацию через общедоступные WI-FI сети. Работая в них, желательно не выводить пароли доступа, логины и какие-то номера
2. Используй и обновляй антивирусные программы и брандмауер.
3. При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам»
4. Не используй публичный Wi-Fi для передачи личных данных, например для выхода в социальные сети
5. Используй только защищённое соединение через HTTPS, а не HTTP
6. Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Основные советы по безопасности в социальных сетях:

1. Ограничить 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.
3. Защищай свою репутацию – держи её в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь.

4. Если ты говоришь с людьми, которых не знаешь, не используй своё реальное имя и другую личную информацию

5. Избегай размещения фотографий в Интернете, где ты изображён на местности, по которой могут найти твоё местоположение.

6. При регистрации в социальной сети необходимо использовать сложные пароли и для разных социальных сетей используй разные пароли. Тогда если тебя взломают то злоумышленники получат доступ только у одному месту, а не во все сразу.

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

Основные советы по безопасной работе с электронными деньгами:

1. Привяжи к счёту мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету.

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

3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль.

4. 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.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис.

2. Не указывай в личной почте личную информацию. Лучше выбрать музыкальный_фанат@ или рок2013@

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 надёжный, устойчивый к взлому пароль

5. Если есть возможность написать самому свой личный вопрос, используй эту возможность.

6. Используй несколько почтовых ящиков. Для личных переписок и для регистрации на сайтах.

7. Не открывай файлы и другие вложения в письмах, даже ели они пришли от твоих друзей.

8. После окончания работы на почтовом сервисе не забудь нажать на «Выйти»

Кибербуллинг – преследование сообщениями, содержащими оскорбления, агрессию, запугивание, хулиганство.

Основные советы по борьбе с кибербуллингом:

1. Не бросаться в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, лучше успокоиться.

2. Управляй своей киберрепутацией.

3. Анонимность в сети мнимая. Существуют способы выяснить. Кто стоит за анонимным аккаунтом.

4. Не стоит вести хулиганский образ жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно.

5. Соблюдай свою виртуальную честь смолоду

6. Игнорируй единичный негатив. Оскорбительные сообщения лучше игнорировать.

7. Бан агрессора. В программах обмена мгновенными сообщениями, можно добавить агрессатора в бан (чёрный список)

8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь.

Мобильный телефон

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

Основные советы для безопасности мобильного телефона:

1. Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нём 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 обновить 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. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь.

8. Периодически проверяй какие платные услуги активированы на твоём номере.

9. Bluetooth должен быть выключен, когда им не пользуешься. Не забывай иногда проверять это.

Online игры

Современные online игры – это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

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
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 и 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.

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. Таки 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 предупредитьвсех 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 надёжные пароль (PIN) на мобильном телефоне.
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 – это негативная или позитивная информация в сети о тебе. Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких – это все 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 размещённая 5 лет назад, стала причиной отказа принять тебя на работу.

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.

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.

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!