Система Образование

РЕКОМЕНДОВАНО Министерством образования и науки

КАК БЕЗОПАСНО ПОЛЬЗОВАТЬСЯ СМАРТФОНОМ, ПЛАНШЕТОМ

Эта памятка поможет тебе безопасно пользоваться мобильными устройствами

Смартфоны и планшеты содержат в себе взрослый функционал и могут конкурировать со стационарными компьютерами. Однако средств защиты для подобных устройств пока 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.

Советы по безопасному использованию мобильных устройств

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

ПАМЯТКА

для школьников

СПРАВОЧНИК РУКОВОДИТЕЛЯ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

Как защититься от компьютерных вирусов

Рекомендовано Минобрнауки

КОМПЬЮТЕРНЫЙ ВИРУС – это программа, которая может создавать свои копии. Вирусы повреждают или уничтожают файлы на зараженном компьютере и всю операционную систему в целом. Чаще всего распространяются вирусы через интернет.

1. **Загрузи современную операционную систему.** Используй современные операционные системы с высоким уровнем защиты от вредоносных программ.

2. **Обновляй операционную систему.** Включи режим автоматического обновления операционной системы. Если в системе нет такого режима, регулярно устанавливай обновления самостоятельно. Загружай их с официального сайта разработчика.

3. **Используй права пользователя.** Работай на компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ автоматически установиться.

4. **Не рискуй.** Используй антивирусные программные продукты проверенных производителей с автоматическим обновлением баз.

5. **Ограничь доступ к своему компьютеру.** Не разрешай посторонним пользоваться своим компьютером.

6. **Выбирай тщательно источники.** Копируй и загружай файлы только с проверенных съемных носителей или интернет-ресурсов. Не открывай файлы, которые получил из ненадежных источников. Даже те, которые прислал твой знакомый. Уточни у него, отправлял ли он тебе их.

ПАМЯТКА для школьников

Как безопасно пользоваться смартфоном, планшетом

1. **Будь осторожен**. Когда тебе предлагают бесплатный контент, в нем могут быть скрыты платные услуги.

2. **Думай, прежде чем отправить СМС, фото или видео.** Ты точно знаешь, где они окажутся в конечном итоге?

3. **Обновляй операционную систему смартфона.** Это дополнительная защита.

4. **Используй антивирусные программы для смартфонов.** Регулярно обновляй их.

5. **Не загружай приложения от неизвестного источника.** Они могут содержать вредоносное программное обеспечение.

6. **Зайди в настройки браузера и удали cookies.** Сделай это сразу после того, как ты выйдешь с сайта, где вводил личную информацию.

7. **Проверяй платные услуги на твоем номере.** Иногда могут активировать новые.

8. **Не всем давай номер телефона.** Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь.

9. **Выключай Bluetooth, когда не используешь его.** Иногда проверяй, не забыл ли выключить.

Система Образование

РЕКОМЕНДОВАНО Министерством образования и науки

КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

Эта памятка поможет тебе защитить личные данные

Обычной кражей денег и документов 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 (от английского слова **fishing** – рыбная ловля), главная цель которого состоит в получении конфиденциальных данных пользователей – логинов и паролей.

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.

Система
Образование

РЕКОМЕНДОВАНО
Министерством
образования и науки

КАК ЗАЩИЩАТЬ СВОЮ ЦИФРОВУЮ РЕПУТАЦИЮ

Эта памятка поможет тебе защитить свою цифровую репутацию

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 задумываешься о том, что фотография, размещенная 5 лет назад, может стать 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.

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.

ПАМЯТКА

для школьников

СПРАВОЧНИК РУКОВОДИТЕЛЯ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

Как безопасно пользоваться сетью Wi-Fi

Wi-Fi – это беспроводной способ передачи данных с помощью радиосигналов. В кафе, отелях, аэропортах часто можно бесплатно выйти в интернет через Wi-Fi. Но общедоступные сети Wi-Fi небезопасны.

1. **Не передавай личную информацию через общедоступные сети Wi-Fi.** Желательно не вводить пароли доступа, логины и номера.

2. **Используй и обновляй антивирусные программы и брандмауэр.** Так ты обезопасишь себя от закачки вируса на устройство.

3. **Отключи функцию «Общий доступ к файлам и принтерам» при использовании Wi-Fi.** Эта функция закрыта по умолчанию, однако некоторые пользователи активируют ее 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. **Используй только защищенное соединение через HTTPS, а не HTTP.** То есть при наборе веб-адреса вводи именно «https://».

6. **Отключи функцию «Подключение к Wi-Fi автоматически» в мобильном телефоне.** Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

ПАМЯТКА

для школьников

СПРАВОЧНИК РУКОВОДИТЕЛЯ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

Как безопасно общаться 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 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 то, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить.

4. **Не используй реальное имя.** Когда в сети разговариваешь с незнакомыми людьми, не называй и не используй реальное имя. Не раскрывай информацию о себе: место жительства, место учебы и прочее.

5. **Не сообщай свое местоположение.** Избегай размещения фотографий в интернете, где ты изображен на местности, по которой можно определить местоположение.

6. **Используй сложные пароли.** При регистрации пиши сложные пароли. Они должны содержать не менее восьми знаков и включать в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак.

7. **Используй разные пароли.** Для социальной сети, почты и других сайтов создавай разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не ко всем сразу.

ПАМЯТКА для родителей

СПРАВОЧНИК РУКОВОДИТЕЛЯ **ДОШКОЛЬНОГО УЧРЕЖДЕНИЯ**

Как защитить от вредной информации ребенка

Рекомендовано Минобрнауки

Дети в этом возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры, но могут и посещать сайт, искать информацию. Поэтому просматривайте отчеты программ по ограничению использования интернета (родительский контроль), временные файлы. Так у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако вы будете по-прежнему знать, какие сайты посещает ребенок.

СОВЕТЫ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ ИНТЕРНЕТА

1. Создайте домашние правила посещения интернета при участии ребенка и требуйте их выполнения.
2. Требуйте от ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что вы наблюдаете не за ним, а потому что беспокоитесь о его безопасности и всегда готовы ему помочь.
3. Поставьте компьютер с подключением к интернету в общую комнату, чтобы ребенок находился под присмотром во время использования интернета.
4. Используйте специальные детские поисковые машины.
5. Используйте средства блокирования нежелательного контента как дополнение к стандартному родительскому контролю.