КАК БЕЗОПАСНО ПОЛЬЗОВАТЬСЯ СЕТЬЮ WI-FI

Эта памятка поможет тебе безопасно пользоваться сетью Wi-Fi

Wi-Fi – это беспроводной способ передачи данных, использующий радиосигналы. Wi-Fi – аббревиатура от английского словосочетания Wireless Fidelity, что дословно переводится как беспроводная точность. Бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но общедоступные сети Wi-Fi не являются безопасными.

Советы по безопасному использованию Wi-Fi

1. Не передавай свою личную информацию через общедоступные сети Wi-Fi. 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 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. В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

КАК БЕЗОПАСНО ОБЩАТЬСЯ В СОЦИАЛЬНЫХ СЕТЯХ

Эта памятка поможет тебе безопасно общаться в социальных сетях

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.

Советы по безопасному общению 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 информацию: 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 ко всем сразу.

КАК БЕЗОПАСНО ПОЛЬЗОВАТЬСЯ ЭЛЕКТРОННОЙ ПОЧТОЙ

Эта памятка поможет тебе безопасно пользоваться электронной почтой

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.

Меры защиты электронной почты

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 «рок2018@» вместо «андрей2005@».

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. Этот 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».

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.

КАК БЕЗОПАСНО ИГРАТЬ ONLINE

Эта памятка поможет тебе безопасно играть в интернете

Online-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 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.

Меры защиты 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.