

Основные советы для безопасности мобильного телефона:

1. 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, зайти в настройки браузера и удали cookies (небольшие фрагменты данных, которые содержат информацию о пользователе и его действиях на сайт);
7. Периодически проверяй какие платные услуги активированы на твоём номере;
8. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь.

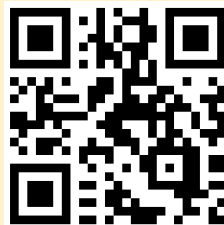
ЗНАКОМЬТЕСЬ: САЙТ ДЛЯ ВАС

На сайте КМЦРБ Вы можете:

- осуществить поиск необходимого издания по электронному каталогу;
- получить ряд информационных услуг онлайн;
- познакомиться с онлайн мероприятиями;
- получить информация о конкурсах и викторинах, библиотеках района, о центре правовой информации, краеведении...

Мы стараемся, чтобы на страницах нашего сайта вы чувствовали себя так же комфортно, как в стенах библиотеки.

Библиотека — это открытый стол идей, за который приглашается каждый. Все что мы делаем, мы делаем для вас - наш читатель!



Ответственный за выпуск: Николаева О.Н.
Составитель: Иванько Н.В.
Наш адрес: 353180, Краснодарский край,
г. Кореновск, ул. Красная, 140
Телефоны: (86142) 4-20-99, 4-58-81
Эл. почта: muk-korlibrary@yandex.ru
Сайт <http://www.korbibl.ru>
Адрес web-сайта:
www.korbibl.ru

Муниципальное бюджетное учреждение
культуры МО Кореновский район
«Кореновская межпоселенческая центральная
районная библиотека»

ТВОЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

Информационный буклет



г. Кореновск
2024

Советы по безопасности работы 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 твоё устройство;
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 или в электронную почту;
5. Используй только защищенное соединение через HTTPS, а не HTTP, 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.



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.

