Фотокамера на телефоне

- Если ты сделал «не хорошую» фотографию, то ни с кем ею не делись. подумай о том, как это будет выглядеть со стороны и к чему это может привести.
- Избегай фотографирования и видеосъемки других людей без их разрешения. Это может иметь серьезные юридические последствия для тебя.

Взаимодействие с людьми

- Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь.
- Не давай чужие номера без их разрешения.

Если украли телефон

- Немедленно обратись к оператору связи с просьбой заблокировать сим-карту, а также, если есть необходимость, в полицию.
- Установи надежный пароль (PIN). Таким образом если у тебя украдут телефон, то злоумышленники не получат твою личную информацию. Сам пароль в телефоне не сохраняй.

Основные советы по защите

- 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.
- Не принимай предложения, которые звучат слишком хорошо, чтобы быть правдой.
- При покупке телефона проверь детали договора по оказанию услуг связи - покупай только то, что тебе необходимо.
- Подумай, прежде чем нажимать на кнопку «Загрузить». Не открывай мультимедийные сообщения (MMS) и вложения в сообщениях электронной почты и SMS. Они могут содержать вредоносное программное обеспечение и перевести тебя на вредоносный веб-сайт.
- Необходимо обновлять операционную систему твоего смартфона.
- Существуют версии антивирусных программ 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.
- Также если у тебя на телефоне хранится много важной и личной информации.
- Периодически проверяй у оператора связи, какие платные услуги активированы на твоем номере.
- Перед поездкой на отдых отключай приложения (игры, погода), которые делают запросы через интернет.

ГБУ РЦПМСС «Сайзырал» 667001,
Республика Тыва, г. Кызыл,
ул. Рабочая,56, тел., факс 5-33-20
e-mail: rzpmss@yandex.ru
Подготовила Шактар-оол Б.В.,
педагог-психолог

Государственное бюджетное учреждение
Республиканский Центр психолого-
медико-социального сопровождения

Мобильный телефон

Кызыл-2019

Мобильный телефон

Сейчас мобильный телефон выполняет не только функцию разговора по телефону, но и множество других функций: фотографирование, выход в интернет и работа с файлами. Средств защиты для телефонов и планшетов пока очень мало. Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств. Удачным примером стандарта безопасности является BlackBerry. Это смартфон, у которого один сервер для электронной почты, шифрование информации, возможностями удаленного уничтожения данных на устройстве. Однако его доля в мире мала, а в России еще меньше.

Доступ к почтовому ящику

Многие, как только берут свой смартфон в руки, сразу вбивают свои данные и делают доступ к своей электронной почте с мобильного телефона. Да, это удобно, однако, если твой мобильный телефон взломают или ты его потеряешь, то преступники получат доступ к твоему почтовому ящику, а если он твой основной почтовый ящик, то они смогут получить доступ к любому твоему профилю.

Также они могут получить доступ ко всей твоей переписке, а также ко всем сервисам, привязанным к почтовому ящику. Кроме этого они могут рассылать от твоего имени спам и зараженные файлы твоим знакомым.

Интернет-мессенджер

Благодаря интернет-технологиям и смартфонам очень популярна стала интернет-телефония типа Skype и обмен мгновенными сообщениями типа ICQ, вайбер, ватсап. Твой профиль, деньги, твои контакты и вся переписка могут оказаться в руках чужих людей, которым нельзя доверять. Кроме этого они могут рассылать от твоего имени спам и зараженные файлы твоим знакомым.

Документы и заметки

За последние несколько лет появилось огромное количество приложений, предназначенных для работы с документами и заметками. Емкость памяти телефона уже превышает обычную флешку, что не ограничивает тебя в добавлении и ведении новых документов. Но эти документы могут тебе очень сильно навредить, если они попадут злоумышленникам. Также некоторые люди используют подобные сервисы для хранения паролей, что дает злоумышленникам дополнительную выгоду от получения твоего телефона.

Деньги на твоем счету

Одной из главной целью может стать счет твоего номера телефона.

Злоумышленники могут получить к нему доступ, и через специальные схемы вывести с твоего счета все деньги и вогнать тебя в долги перед оператором связи.

Примером может стать подключение без твоего ведома услуги, за которую будут сниматься деньги с твоего счета. Данная схема может работать постоянно, а главное ты не будешь понимать, куда уходят твои деньги.

bluetooth

Bluetooth - это быстрый и удобный способ обмена контентом - фотографиями, музыкой и другими файлами. Но важно знать, что когда ты включаешь свой Bluetooth, то люди, находящиеся поблизости, могут получить доступ к файлам в твоем телефоне и к твоим контактам.

Также, кроме потери личной информации из телефона, сам телефон после заражения или повреждения может потерять свою производительность.

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

- Если ты используешь bluetooth, то измени настройки так, чтобы телефон был «невидимый», а также установи пароль для доступа.
- Устройство bluetooth должно быть блокировано или не видно окружающим.
- Измени пароль по умолчанию, чтобы окружающие не знали имени устройства, и не смогли идентифицировать тебя и модель телефона.