

Правила безопасности школьников в сети Интернет

Фишинг. Никогда не переходите по ссылке, указанной в сообщении. Помните, что, перейдя по ссылке, вы можете получить на телефон вирус или оформить подписку на платные услуги. Даже если сообщение пришло от знакомого человека, убедитесь, что именно он отправитель.

Мошеннические магазины. Никогда не перечисляйте деньги на электронные кошельки, не убедившись в благонадежности продавца. Внимательно изучите его рейтинг, почитайте отзывы других покупателей, поищите о нем информацию в интернете. Подумайте, почему товар продается так дешево, узнайте, какие гарантии предоставляет продавец. Оплатите покупку при получении.

Крик о помощи. Никогда не отправляйте никаких денежных средств по координатам, указанным в сообщении, не перезванивайте на номер, с которого оно пришло, не отправляйте ответных СМС. Самым правильным решением будет позвонить родственнику или другу, от имени которого пришло сообщение, и убедиться, что с ним все в порядке.

Цифровая гигиена. Никогда не размещайте в открытом доступе и не передавайте информацию личного характера, которую можно использовать во вред: данные геолокации, даты отъезда, номера карт, информацию о родителях. Помните, что злоумышленники могут сохранить и использовать видео- и аудиотрансляции, данные вашей переписки.

Кибербуллинг. Никогда не отвечайте на оскорбительные сообщения. Тем более не стоит мстить обидчику ответными сообщениями. Ваши ответные оскорбления или унижение собеседника сделают ситуацию только хуже, а может быть, приведут к еще большим проблемам.

