

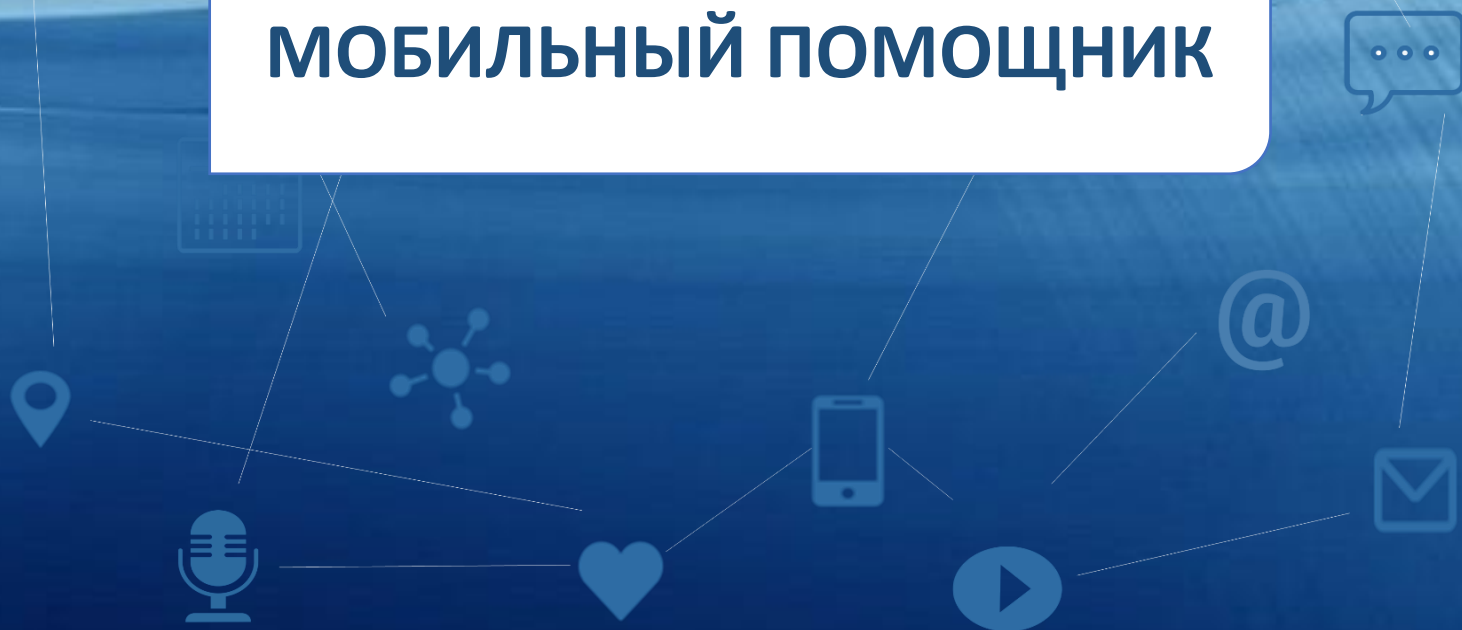


ГБОУ ВО «ВОЛЖСКИЙ ИНСТИТУТ ЭКОНОМИКИ, ПЕДАГОГИКИ И ПРАВА»

РЕГИОНАЛЬНЫЙ РЕСУРСНЫЙ ЦЕНТР ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ И ЦИФРОВОЙ ГРАМОТНОСТИ ДЕТЕЙ



МОБИЛЬНЫЙ ПОМОЩНИК



1. Не добавлять незнакомых взрослых в друзья

Часто мошенники заводят в социальных сетях странички «сверстников», добавляются в друзья и вступают в переписку с детьми. Ты думаешь, что общаешься со сверстником, и можешь рассказать, какой у тебя компьютер и сколько их вообще, когда родители приходят с работы и многое другое. За фотографией на аватарке может скрываться мошенник, и, если он узнает, когда родителей не будет дома, из квартиры могут пропасть ценные вещи или произойти другие неприятности.

2. Не сообщать личную информацию

Никогда и ни при каких обстоятельствах не сообщай информацию личного характера: персональные данные (Ф. И. О., дата рождения, домашний адрес, номера телефона, банковских карточек, пароли). Не сообщай эту информацию никому в переписках, комментариях, онлайн-играх. Если кто-то с сети попросит номер телефона или адрес, сначала нужно ответить: «Спрошу разрешения у родителей». Обычно после такого сообщения мошенники исчезают.

3. Не скачивать программы с сомнительных сайтов

Используй для загрузки приложений только Google Play или App Store. Скачав программу с первого попавшегося ресурса, можно легко поймать вирус, из-за которого не только сломается техника, но и окажутся у злоумышленников номера банковских карт родителей. В любой непонятной ситуации нужно посоветоваться с взрослым, которому ты доверяешь.

4. Не переходить по подозрительным ссылкам

Нельзя нажимать на подозрительные ссылки, которые приходят по электронной почте или в сообщениях. Например: «Посмотри, что здесь о тебе говорят», «Ты стал обладателем нового iPhone — переходи по ссылке, чтобы забрать его». Такие сообщения отправляют мошенники и при переходе по ссылке на компьютер или смартфон попадёт опасный вирус.

5. Ничего не оплачивать в интернете

В мобильных приложениях и играх есть платный контент. Это рискованно. Идёшь на это? Тогда платежи в интернете нужно согласовывать со взрослыми. Оплачивать покупки и переводить куда-либо деньги делай только после разрешения взрослых.

6. Не ставить геометки под фото

По ним злоумышленники легко узнают, где ты живёшь и учишься. Конечно, нет ничего страшного в том, что ты поставил геометку на фотографии, например со школьной экскурсии. Но, рассказывать о каждом своём перемещении и особенно указывать домашний адрес или номер своей школы в соцсетях не стоит.

7. Не верить в быстрый и лёгкий заработок

Этот совет больше касается подростков. Стремление найти подработку и самому заработать деньги на новый телефон - это похвально. Порядочный работодатель не будет просить перевести деньги перед оформлением на работу. Нельзя верить предложениям заработать сразу много денег, практически ничего не делая.

8. Не доверять сообщениям о крупном выигрыше

Неожиданное сообщение о крупном выигрыше, который якобы можно получить после оплаты комиссии, тоже должно вызывать подозрение. Не участвуй в сомнительных конкурсах в социальных сетях.

9. Перепроверять сообщения о помощи от друзей и родственников

Иногда мошенники взламывают аккаунты в соцсетях и рассылают всем друзьям сообщения с просьбой перевести деньги. Не торопись с помощью, свяжись по телефону с человеком, со странички которого пришло сообщение, чтобы самому узнать, нужны другу деньги или нет. Или посоветуйся с родителями.

10. Не верить всему, что пишут в сообщениях

Каждый из нас хотя бы раз получал сообщение примерно такого содержания: «Пополнял счёт и ошибся номером, верните, пожалуйста, деньги». Это схема мошенничества и попавшись на неё, ты подаришь свои деньги чужому человеку. В этом случае нужно обратиться к взрослым.

Твое правило

