Приложение

Рекомендации для детей по личной безопасности и профилактике попадания в мошеннические схемы в сети Интернет

Чтобы не стать жертвой мошенников или других преступлений в сети Интернет, не стать участником каких-либо сомнительных махинаций подросткам необходимо соблюдать некоторые правила безопасности:

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 можешь думать, что общаешься с симпатичной девочкой, и можешь рассказать, какой у тебя компьютер и сколько их вообще, когда родители приходят с работы и многое другое. Помни, что 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. Мошенники часто скрываются под маской интересных собеседников на форумах и в группах в соцсетях. Они заводят с подростком виртуальную дружбу на почве общих интересов и втираются в доверие ради будущей выгоды. Когда контакт налаживается, они выдумывают различные предлоги, чтобы получить необходимую им информацию. Например, мошенники просят ребенка прислать фотографии банковских карт или паспортов родителей. Этих данных может оказаться достаточно, чтобы украсть деньги со счета или оформить кредит на чужое имя.

2) Не сообщать личную информацию

Никогда и ни при каких обстоятельствах нельзя сообщать информацию личного характера. К персональным данным относится: Ф.И.О., дата рождения, домашний адрес, номера телефона, банковских карточек, пароли. Эту информацию нельзя никому сообщать в переписках, комментариях, онлайн-играх. Если у тебя в сети кто-то 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

Для загрузки приложений необходимо использовать только Google Play или App Store. Если скачать программу с первого попавшегося ресурса, то можно легко поймать вирус, из-за которого не только может выйти из строя компьютер, ноутбук, планшет или телефон, но и в руках у злоумышленников окажутся номера банковских карт родителей.

4) Не переходить по подозрительным ссылкам

Нельзя нажимать на подозрительные ссылки, которые приходят по электронной почте или в сообщениях. Например: «Ты стал обладателем нового iPhone — переходи по ссылке, чтобы забрать его». Тебе лучше знать, что 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. Игроков заманивают низкими ценами и «уникальными акциями». И не стоит заблуждаться, в подобные ловушки могут попасть не только дети, но и взрослые Проявляй осторожность при совершении онлайн –покупок. Злоумышленники могут использовать фейковые страницы для онлайн-покупок. Прежде чем совершать платежи в Интернете, их нужно согласовывать со взрослыми.

6) Не ставить геометки под фото

По ним злоумышленники могут легко узнать, где ты живёшь или учишься. Не надо рассказывать о каждом своём перемещении и особенно указывать домашний адрес или номер своей школы в соцсетях.

7) Не верить в быстрый и лёгкий заработок

Стремление найти подработку и самому заработать деньги на новый телефон — это похвально. Но дети в поисках заработка могут быть очень наивны. Порядочный работодатель не будет просить перевести деньги перед оформлением на работу. И ещё — что нельзя верить предложениям заработать сразу много денег, практически ничего не делая. Есть большая опасность, что тебя могут использовать «вслепую». В последнее время злоумышленники делают предложения о заработке в социальных сетях «ВКонтакте», «Одноклассники», а также мессенджерах «Telegram», «WhatsApp» и др. Такой «легкий» заработок может «вскружить» голову. Так, тебя могут попросить забрать крупную сумму денег и перечислить на определенный счет, а часть суммы предложат оставить себе в качестве вознаграждения. На первый взгляд может показаться, что это очень выгодное предложение! Но вместо заработка ты получишь крупные неприятности, так как можешь стать соучастником преступления, например мошенничества.

8) Не доверять сообщениям о крупном выигрыше

Неожиданное сообщение о крупном выигрыше, который якобы можно получить после оплаты комиссии, тоже должно вызывать подозрение. Нередко мошенники рассылают письма и сообщения, в которых обещают нежданный выигрыш или от имени популярных блогеров запускают рекламу «беспроигрышных лотерей». Но затем за доставку «приза» или какие-то другие дополнительные услуги просят оплатить небольшую комиссию. Для этого надо пройти по ссылке и ввести данные банковской карты. Но на самом деле ссылка ведет на фишинговый сайт, и вместо призов доверчивый пользователь получает убытки.

9) Не верить в крупное обогащение

Мошенники могут убедить тебя вложить деньги в «сверхприбыльный проект» (спойлер — в финансовую пирамиду). До выплат вкладчикам дело обычно не доходит. Собрав деньги как можно большего числа людей, организаторы исчезают. Порой обманщики предлагают «быстро заработать», просто зарегистрировавшись на сомнительном сайте. Надо только выполнять задания или делать букмекерские ставки. Для вывода «заработка» они просят оплатить комиссию. В итоге деньги вместе с данными карты оказываются в руках махинаторов.

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». Помни, что так действуют мошенники! Попавшись на их удочку, ты подаришь свои деньги чужому человеку. Обратись за советом к взрослым.

11) Не доверяйте сообщениям об оказании помощи от имени своих друзей или знакомых!

Киберпреступники взламывают аккаунты в соцсетях, а затем от чужого имени рассылают сообщения по списку друзей. Начинают разговор с банального «Как дела?» и практически сразу переходят к жалобам на жизнь и просят в долг. Или со словами «Лови фотки с дня рождения!» вместо ссылки на фотографии присылают вредоносный вирус. Он крадет с гаджета персональные данные, логины и пароли от личных кабинетов, в том числе от банковских. Могут быть и более сложные махинации.

Основное правило безопасности, которое ты должен знать: в любой непонятной ситуации нужно посоветоваться со взрослым, которому доверяешь!

И еще несколько советов по безопасности в сети Интернет:

Защити аккаунты дважды. Необходимо установить сложный пароль, менять его каждые 3 месяца и дополнительно подключить двухфакторную аутентификацию везде, где это возможно (почта, VK, Telegram…). Старайся не использовать одинаковые пароли для нескольких сервисов.

Защити свои устройства. Обновляй программы для ПК и мобильные приложения, а также версию операционной системы. Периодически обновляй версию прошивки роутера. Разработчики сами уведомят о новом обновлении, следуй рекомендациям своевременно. Обязательно блокируй устройства, не подключай их к неизвестным Wi-Fi сетям.

Защити данные. При вводе данных на сайте или в приложении обрати внимание на адрес страницы сайта. Мошенники любят создавать приложения и сайты, похожие на оригинал, с целью хищения логинов/паролей и данных банковской карты.

Кликай внимательно. В случае получения ссылки, не спеши! Проверь отправителя, текст и саму ссылку. Их мошенники обычно рассылают в почте, мессенджерах и SMS для заражения устройств или хищения данных.

Контролируй публичную информацию о себе. В социальных сетях все же стоит ограничивать некоторую информацию о себе: адрес, данные карт и паспорта, информацию о покупках и поездках. Иногда преступники используют открытую информацию, чтобы подобрать способ атаки на пользователя.

Не забывай, что Интернет помнит все!