

Обман в интернете и социальных сетях и – очень распространенное явление. Помни, что твои собеседники могут оказаться не теми, за кого они себя выдают. Ты думаешь, что тебе пишет твой друг, с которым ты знаком в реальной жизни, но может оказаться так, что его аккаунт взломан, кто-то создал копию его личности и тебе пишет мошенник. Поэтому если собеседник просит тебя сделать что-то необычное или просит денег, обязательной проверь его. Если это человек, с которым ты знаком в реальном мире, позвони ему. Задай вопрос, ответ на который можете знать только вы вдвоем. Если ты понимаешь, что твой собеседник не тот, за кого себя выдает, обратись в службу поддержки, чтобы заблокировать этот аккаунт. Сообщи другу, если поймешь, что его аккаунт взломан. Если не знаешь как себя вести, обратись на горячую линию помощи детям.

Фальшивые сайты и аккаунты в социальных сетях

В социальных сетях и в интернете мы часто получаем сообщения, в которых нам предлагают купить товар с большой скидкой или получить выигрыш за предоплату, скачать бесплатно рингтон или игру. Цель таких сообщений в том, чтобы убедить тебя отправить на счет мошенников деньги или ввести данные своей банковской карты. Например, ты заказываешь что-либо через социальную сеть или пишешь комментарий о желании сделать заказ. Мошенник находит тебя и предлагает купить аналогичный товар с большой скидкой. Просит оплатить все сразу, а получив деньги исчезает. Существуют разные способы хищения и обмана. Поэтому будь внимательным, когда сообщаем сведения о себе. Так, например, бывают: Фальшивые сайты — сайты-подделки, созданные для того, чтобы украсть персональные данные (логины, пароли или номера и коды банковских карт) Как обезопасить себя? Всегда проверяй адресную строку сайтов. Тебе на почту может прийти письмо от известного сайта с просьбой подтвердить пароль или проверить учетные данные, при переходе на данный сайт он будет выглядеть как настоящий, НО адресная строка будет отличаться. Значит, это сайт-подделка. Не надо переходить по таким ссылкам! Если ты засомневался, то лучше зайди на сайт прямо, написав его название в адресной строке браузера.

Письма, которые ведут на сайты-подделки, чаще всего:

- не содержат личного обращения по имени и фамилии
- содержат ссылку, нажав на которую, ты якобы решишь все вопросы
- сообщают о негативных последствиях, если ты этого не сделаешь. Например, пишут: «Если не пройдешь по ссылке, то твой аккаунт заблокируют прямо сейчас»

Плата за подписки

Под платой за подписку может скрываться кража денег с баланса телефона. Подписка происходит через USSD-запрос или отправку СМС-сообщения. Будь внимателен, нажимая кнопки «смотреть», «подписаться» или «скачать». Ты можешь случайно подписаться на платные сервисы или платный развлекательный контент. Иногда нажимая на эти кнопки, ты автоматически соглашаешься с условиями подписки.

