

ОСТОРОЖНО, МОШЕННИКИ!

Мошенники очень хорошо знают психологию людей и умело используют всю доступную информацию из социальных сетей. Как же себя от них защитить?

Не соглашайся:

- вносить предоплату покупая что-либо в социальных сетях и на сайтах объявлений. Вполне возможно, что получив её, «продавец» перестанет отвечать на звонки.
- называть трёхзначный код на оборотной стороне банковской карты, PIN - код;
- сообщать пришедший на телефон код;
- переходить по ссылке в Интернете, в SMS - или MMS-сообщении на смартфоне;
- звонить по указанному в SMS - сообщении номеру телефона;
- отправлять SMS - сообщение на короткий номер;
- называть пароли от ваших личных страничек в социальных сетях;
- переводить деньги куда-либо поле получения SMS с просьбой о помощи. Сначала позвони родителям и узнай всё ли в порядке.



БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

ЧТО НУЖНО ЗНАТЬ КАЖДОМУ

СВЯЗАТЬСЯ С НАМИ

644023, г. Омск, ул. Комсомольский городок, д. 14
Телефон: +7 (3812) 32-35-90
metodist_pmss@mail.ru
www.центрпмсс.пф



В ИНТЕРНЕТЕ НЕ СТОИТ

- Сообщать всем свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, а также фотографии свои, своей семьи и друзей).
- Открывать вложенные файлы электронной почты от неизвестного отправителя.
- Вести себя невежливо и агрессивно (грубить, оказывать давление).
- Совершать покупки в интернете на непроверенных сайтах, вводить данные банковской карты.
- Прежде чем встречаться с интернет-знакомым посоветуйся со взрослым, которому доверяешь, предупреди его об этом.
- Переходить по сомнительным ссылкам, предлагающим большой выигрыш или смену пароля в соцсетях - так можно потерять доступ к своему аккаунту или заразить компьютер вирусом.

ОСТОРОЖНО!

- Не все пишут в интернете правду. Если ты увидишь неправдивую информацию о себе или ком-то другом - сообщи родителям.
- Незаконное копирование файлов в интернете - воровство.
- После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies.
- Используй настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и других порталах.
- В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только "для друзей", так ты сможешь обезопасить свои данные.
- Скачивай файлы только на безопасных сайтах. Прежде чем открывать любой из загруженных файлов просканируй его в антивирусной программе.
- Старайся не реагировать на обидные комментарии, хамство и грубость других пользователей. Всегда пытайся уладить конфликты с пользователями мирным путем, переведи всё в шутку или прекрати общение с агрессивными пользователями. Ни в коем случае не отвечай на агрессию тем же способом.

В ИНТЕРНЕТЕ НУЖНО

- Уважать других пользователей;
- Использовать безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем.
- Делать ссылку на интернет-источник, если используешь его для получения информации.
- Обращаться за помощью ко взрослым - родители и администрация сайтов всегда помогут решить возникшие трудности.
- Вовремя обновлять информационные системы, антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твоё устройство.
- Отключать функцию "Общий доступ к файлам и принтерам" при использовании Wi-Fi в общественном месте. Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учёбе дома.
- Использовать сложные (не менее 8 знаков) и разные пароли к своим аккаунтам. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем.
- Не проходить мимо кибербуллинга. Если ты стал(а) свидетелем оскорбления другого пользователя в сети, то нужно выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.