Не стоит забывать, что следы пребывания в сети Интернет хранятся долго. Прокси и анонимайзеры не всегда помогают скрыться. Веди себя в Интернете вежливо и будь осторожен при общении с незнакомцами в сети.

Помни, что небрежное отношение к личной информации приводит к ее утере!

Будь осторожен в открытых и небезопасных сетях. Подключение к ложной сети может моментально лишить тебя всей персональной информации, хранящейся в твоем электронном устройстве, так как преступнику станут доступны твои пароли и другая информация.

Также опасно оставлять свои учетные данные на чужом устройстве.

Простые правила, которые следует соблюдать при работе в открытых сетях или с чужой техникой:

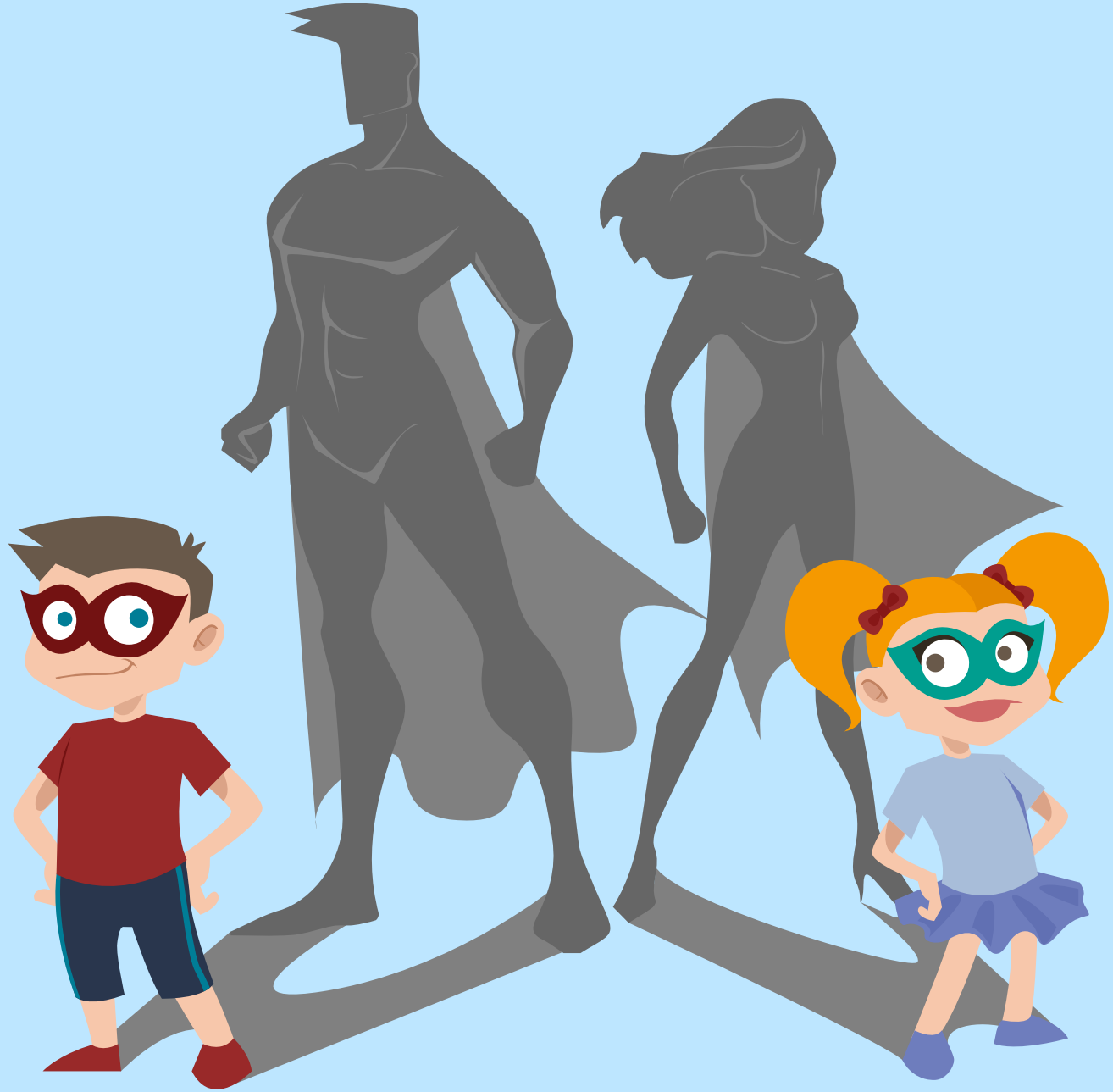
- При работе с публичным устройством используй пункт «чужой компьютер»;
- Используй режим «приватный просмотр» в браузере;
- Не забывай использовать кнопку «выйти» при завершении работы с сайтом;
- Отказывайся от сохранения пароля на чужом устройстве.
- Не оставляй без присмотра устройства доступа в сеть;
- Используй всегда сложные пароли, состоящие из прописных и заглавных латинских букв и цифр, а также символов.

ГОУ ДПО ТО
“ИПК И ППРО ТО”

ТУЛА, УЛ. ЛЕНИНА, Д. 22

ПАМЯТКА

ПО БЕЗОПАСНОЙ РАБОТЕ В ИНТЕРНЕТЕ



Чем опасны сайты-подделки?

Кража паролей.
Распространение вредоносного ПО.
Навязывание платных услуг.
Чтобы не стать жертвой мошенника внимательно проверяйте адрес сайта, а также используйте функционал браузера: «избранное» и «закладки».

Как обманывают в Интернете?

Просят подтвердить пароль или логин.
Предлагают бесплатный антивирус, а устанавливают вредоносные ПО, вирусы.
Просят отправить платное СМС.

Что делать, если ты сомневаешься?

Закрой страницу. Если блокировка пропала, значит все в порядке.
Проверь систему антивирусом!
Смени пароли к аккаунтам, которые используешь.

Осторожно, спам!

Спам – это массовая рассылка незапрашиваемых получателем электронных сообщений коммерческого и некоммерческого содержания.
Идя на поводу у СПАМа, есть риск:

- Отправить платное СМС, оплатить навязанную услугу.
- Получить платную подписку на ненужную информацию.
- Потерять учетные и (или) иные данные.
- Стать жертвой обмана.

Мобильные устройства/Мобильный интернет

Твой мобильный телефон содержит важную информацию, за сохранностью которой необходимо следить. Это:

- Список контактов.
- Личные фотографии/видеозаписи.
- Данные доступа к электронной почте и другим аккаунтам в сети.
- Данные о банковских картах и платежах.

При использовании мобильных устройств необходимо соблюдать несколько простых правил:

- Установи мобильную версию антивируса на мобильное устройство.
- Устанавливай приложения только из проверенных источников.
- Отключи автоподключение к сети Wi-Fi.
- Внимательно изучай права, запрашиваемые мобильными приложениями.

БУДЬ ВНИМАТЕЛЕН!

Настрой безопасность браузера и почтовой программы (подключи антифишинг, защиту от спама и другие встроенные средства защиты)!

Используй дополнительные расширения браузеров, например AddBlock (позволяет блокировать СПАМ и рекламные блоки), WOT (показывает рейтинг сайта среди интернет-пользователей)!

Используй Антивирус и файерволл!

Проверяй надежность поставщика услуг, используй информационные сервисы «who is»!

Персональные данные – твоя частная собственность. Прежде чем публиковать их и (или) передавать третьим лицам, подумай, стоит ли?

Кому и зачем нужна твоя личная информация?

По данным статистики, 80 % преступников берут информацию в социальных сетях.

Личная информация используется для кражи паролей.

Как избежать этого?

При регистрации в социальных сетях используй только имя или псевдоним.

Ограничь доступ к личной информации в настройках приватности.

Не делись информацией о своем местонахождении и материальных ценностях.

Не доверяй свои секреты незнакомым людям.