Основные правила безопасности

В интернете, как и в жизни, есть правила безопасности. Соблюдай их.

Социальная сеть

Расскажи родителям о своих друзьях в сети.

Подумай, с кем ты общаешься в сети, кто скрывается за ником.

Безопасное общение в интернете

Если ты подружился с кем-то в онлайн-пространстве, проанализируй ваше общение:

- он попросил держать дружбу и вашу переписку в секрете от друзей и родителей?
- интересовался персональными данными или информацией о семье?
- при общении с ним ведешь себя не так, как обычно, как будто тобой манипулируют?
- просит сделать то, что противоречит твоим принципам?

Если на вопросы ты ответил «да», то это опасная дружба и общение стоит прекратить.

Компьютерный вирус

Попроси родителей установить антивирус на твой компьютер.

Мошенники в интернете

Остерегайся мошенников! Расскажи родителям о людях, которым ты не доверяешь, но которые продолжают общаться с тобой в соцсетях.

Цени свое время

Живи реальной жизнью: читай книги, гуляй с родителями, играй с друзьями на улице.

Московская областная комиссия
по делам несовершеннолетних
и защите их прав:

г. Москва, проспект Мира, д. 72

8 (498) 602-10-93

Горячая линия «Дети в беде»:

8 (903) 100-49-09

Время работы телефона:
с 9.00 до 20.00 в рабочие дни

Единый телефон доверия
для детей, подростков и их родителей:

8 (800) 20-00-122

Национальный центр помощи
пропавшим и пострадавшим детям

8 (800) 700-56-76

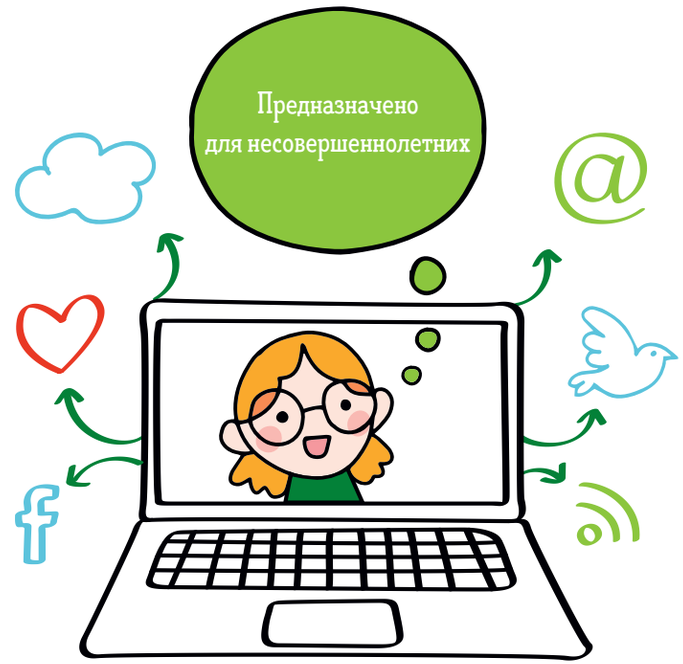
(телефон горячей линии)

ГАУ МО «Издательство «Подмосковье» по заказу ГУИП МО
ООО «Типография А2Пресс» 115088, г. Москва, 2-й Южнопортовый проезд, д. 26а, стр. 12
Заказ , тираж 20 000 экз., 2020 г.

МОСКОВСКАЯ ОБЛАСТНАЯ КОМИССИЯ
ПО ДЕЛАМ НЕСОВЕРШЕННОЛЕТНИХ
И ЗАЩИТЕ ИХ ПРАВ

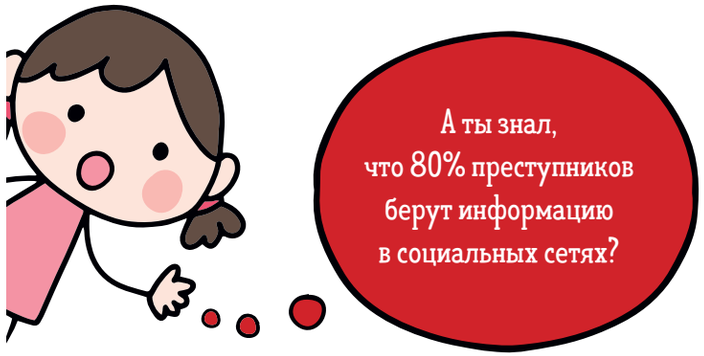
Кибербезопасность

Как уберечь себя в Сети и не стать жертвой злоумышленников



Как не стать интернет-жертвой?!

Общаясь в социальных сетях, будь предельно внимательным: не рассказывай подробностей своей жизни, старайся не включать в список друзей незнакомых людей. Иногда незнакомец в сети может оказаться мошенником или хакером и совершить в отношении тебя преступление – завладеть учетными данными, платежными реквизитами, персональной информацией.



Предотвращаем риск в социальных сетях

- регистрируйся под псевдонимом
- настрой приватность
- не делись информацией о своем местонахождении и имуществе
- не доверяй свои секреты незнакомцам из интернета.

Открытые сети. Чужая техника

При подключении к открытой сети (метро, кафе и т. д.) ты оставляешь персональные данные, в их числе логин с паролем (если заходишь на страницу в соцсети, на электронную почту). Получив доступ к твоим персональным данным, злоумышленники могут украсть аккаунт в социальных сетях, получить доступ к электронным платежным системам или банковским картам.

Предотвращаем риск при использовании открытых сетей и чужой техники

- при работе с публичными устройствами используй пункт «чужой компьютер» и не сохраняй на нем свой пароль
- используй режим «приватного просмотра» в браузере
- пользуйся кнопкой «выйти» при завершении работы с ресурсами
- используй только сложные пароли и безопасные соединения

Электронные финансы

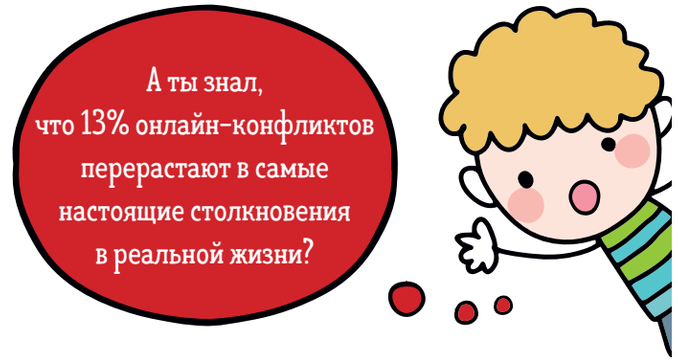
Интернет-транзакции, электронная коммерция, мобильный банкинг, кредитные карты в сети Интернет – актуальные тренды. Но будь внимательным и не пренебрегай основными правилами.

Предотвращаем риск стать жертвой финансового мошенничества

- делай длинные и сложные пароли для платежных систем
- не переходи по ссылкам, набирай адрес сайта самостоятельно
- имя протокола должно выглядеть следующим образом: https://...
- осуществляй транзакции только на домашнем компьютере
- внимательно относись к оповещениям своего банка
- не отказывайся от SMS-оповещения! Они помогают контролировать операции
- по возможности не отключай GPS
- постарайся оборудовать телефон своими биометрическими параметрами

Кибербуллинг как «Бойцовский клуб»

Если ты столкнулся с кибербуллингом, то обязательно сообщи об этом родителям или педагогам. Кибербуллинг может быть столь же опасным и болезненным, как и конфликт в реальной жизни.



Виды кибернападок: оскорбление, клевета, публичное разглашение личной информации, преследование, угроза физической расправы.

Помни: кибербуллинг может повлечь наступление юридической ответственности, в лучшем случае – административной.

Предотвращаем риск стать жертвой кибербуллинга

- не вступай в словесные перепалки в соцсетях, форумах, даже если их участниками являются твои друзья
- чаще меняй пароли в соцсетях.
- игнорируй оскорбляющие тебя сообщения и сообщи об этом взрослым
- не угрожай хулигану
- не выкладывай в сети компрометирующую тебя информацию
- добавь злоумышленника в черный список/удали из друзей