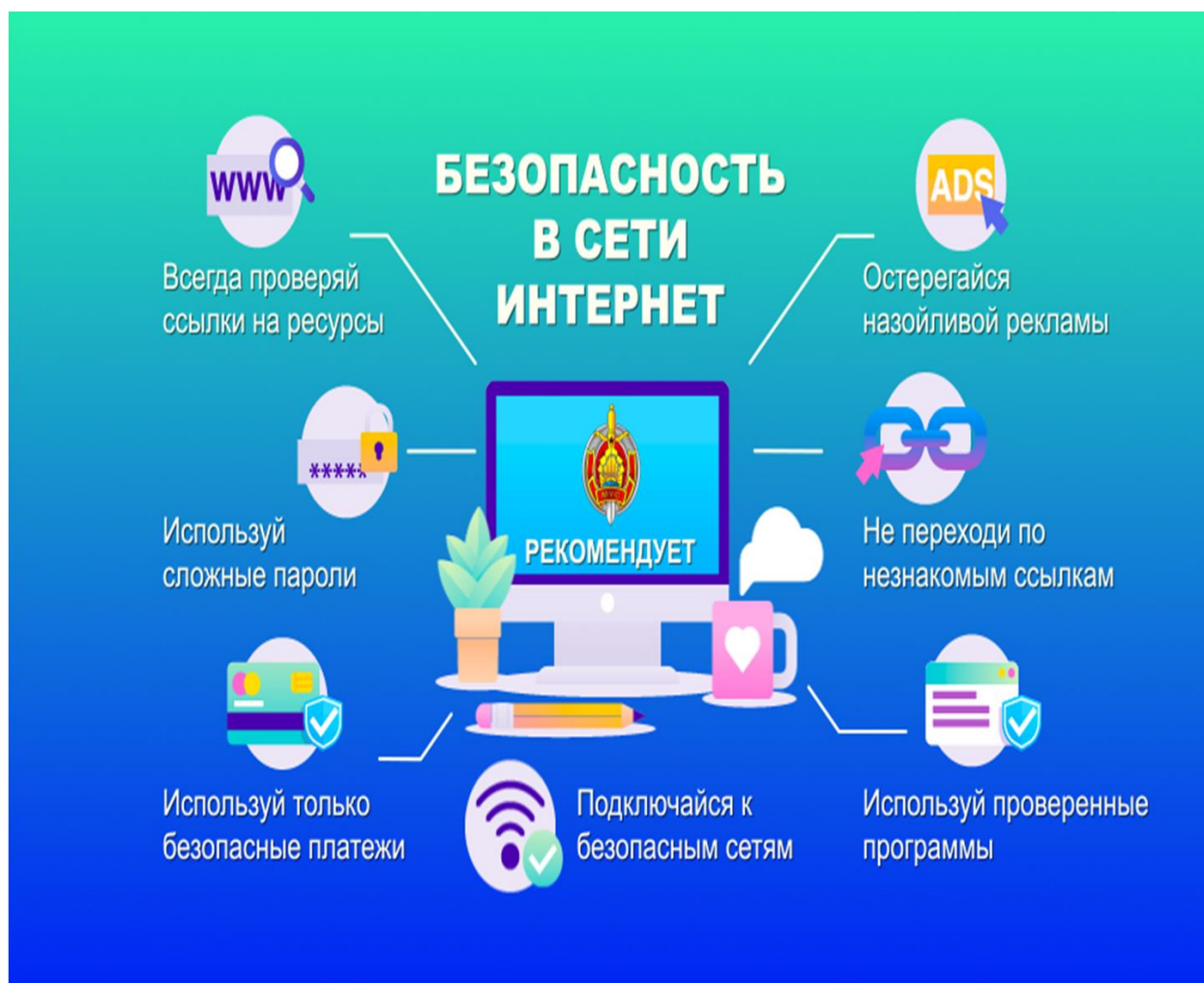


Кибербезопасность для подростков: как уберечься от угроз в интернете



Цифровая гигиена: правила жизни в сети, которые должен знать каждый

Интернет — не игра, а отражение реальности

Соцсети, мессенджеры и игры — такая же часть жизни подростка, как школа и улица. И здесь, как в реальном мире, есть правила безопасности, «свои» и «чужие», а также угрозы. Знание этих правил — не ограничение свободы, а инструмент для уверенного и безопасного использования всех возможностей цифрового мира.

Часть 1: Главные цифровые угрозы: что это и как выглядит?

1. Кибербуллинг (травля в сети): Оскорбительные сообщения, комментарии, создание унижительных мемов, травля в общих чатах.
2. Груминг: Знакомство взрослого злоумышленника с ребенком под видом сверстника с целью установления доверительных отношений для последующих личных встреч или получения интимных фото/видео.
3. Фишинг и мошенничество: Ссылки на фейковые сайты, ворующие логины и пароли, розыгрыши «айфонов», просьбы перевести деньги «заблокированному другу».
4. Кража личных данных и шантаж: Использование ваших фото, информации для создания фейковых страниц или вымогательства («заплати, иначе выложу твои переписки»).
5. Вредоносный контент: Пропаганда насилия, суицида, экстремизма, деструктивных субкультур, порнография.

Часть 2: Правила цифровой гигиены: памятка для подростка

ЗАЩИТА ПРОФИЛЯ И ДАННЫХ:

- Сложный пароль. Используй комбинацию букв (заглавных и строчных), цифр и символов. Разный пароль для соцсетей и для почты/банка!
- Двухфакторная аутентификация (2FA). Подключи! Это главный щит аккаунта.
- Друзья — только те, кого знаешь в реальности. Не добавляй в друзья незнакомцев.
- Проверь настройки приватности. Ограничь круг лиц, который видит твои посты, фото, список друзей, отметки о местоположении.

БЕЗОПАСНОЕ ОБЩЕНИЕ:

- Не делись конфиденциальным. Никогда и никому не отправляй свои интимные фото или видео (это называется секстинг). Даже самому близкому человеку. Они могут стать публичными.
- Думай, прежде чем постить (Правило «бабушки»). Не выкладывай ничего, чего бы постеснялась показать бабушке или будущему работодателю. Интернет помнит все.

- Не встречайся с интернет-знакомыми без крайней нужды. Если идешь — только в людное место, с друзьями, предупреди родителей.

ПРОТИВОДЕЙСТВИЕ УГРОЗАМ:

- Не открывай подозрительные ссылки и файлы даже от друзей (их аккаунт могли взломать).
- Не верь в «легкие деньги» в сети. Бесплатный сыр — только в мышеловке.
- Если ты столкнулся с кибербуллингом или шантажом:
 1. НЕ УДАЛЯЙ доказательства (скриншоты, переписку).
 2. ЗАБЛОКИРУЙ агрессора.
 3. ПОЖАЛУЙСЯ администраторам платформы.
 4. РАССКАЖИ взрослому, которому доверяешь (родителям, школьному психологу).

Часть 3: Что могут сделать родители?

1. Не запрещать, а интересоваться. Спросите: «Во что ты играешь? Покажи своего блогера, почему он тебе нравится?»
2. Обсудите правила. Установите «семейное соглашение»: время за экраном, что можно и нельзя делать, почему важны настройки приватности.
3. Будьте tech-savvy (в теме). Узнайте о популярных среди подростков приложениях, их функциях и рисках.
4. Создайте атмосферу доверия. Договоритесь, что ребенок всегда может прийти к вам с проблемой из сети без страха, что вы отберете гаджет. Вы — его главная линия обороны.

Безопасность в интернете — это навык, который нужно тренировать, как умение переходить дорогу. Это не про тотальный контроль, а про критическое мышление, осознанность и умение защитить свои границы в

цифровом пространстве. Освоив эти правила, ты получаешь не ограничения, а настоящую свободу и силу уверенного пользователя.