ПАМЯТКА

«БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ»

Советы взрослым: как обезопасить детей в интернете

- Используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него.
    - Узнайте, в каких соцсетях зарегистрирован ваш ребенок, просматривайте его страницу.
- Поощряйте детей сообщать обо всем странном или отталкивающем и реагируйте спокойно, если что-то такое им действительно встретится.
- Научите детей думать перед тем, как нажимать на любые кнопки и ссылки, особенно в электронных письмах.

7–8 лет

1. В этом возрасте еще можно требовать от ребенка соблюдения временных норм "экранного времени".
*2. Включите в поисковиках фильтры **безопасного поиска, блокировку сомнительных сайтов** в браузере. Подключите функцию **родительского контроля**.*
*3. Подключите услуги **блокировки платного контента**, не кладите много денег на счет детского телефона. Убедитесь, что все ваши счета закрыты надежными паролями.*
4. Создайте семейный электронный ящик: детям еще рано иметь собственные адреса.
5. Приучите детей советоваться с вами, прежде чем публиковать или скачивать что-либо.
6. Не забывайте беседовать с детьми об их друзьях в интернете, как если бы речь шла о друзьях в реальной жизни.
7. Расскажите детям про сайты "для взрослых" и их опасность.
*8. Установите на все детские гаджеты качественные **антивирусы** от проверенных компаний.*
9. Приучите ребенка сообщать вам о любых угрозах или тревогах, связанных с интернетом.
10. Обращайте внимание на возрастной рейтинг игр и приложений, которыми пользуется ребенок.

9–12 лет

1. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по интернету.
2. Приучите детей никогда не выдавать личную информацию в интернете без вашего разрешения. Аккаунты в соцсетях лучше вести под вымышленным именем и без фотографий.
3. Создайте ребенку **ограниченную учетную запись** для работы на компьютере.
4. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте и мессенджерам, чтобы вы убедились, что они не общаются с незнакомцами.
5. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.
6. Расскажите детям, что далеко не все, что они могут прочесть или увидеть в интернете – правда. Приучите их спрашивать о том, в чем они не уверены.
7. Расскажите детям о том, что публичный и школьный Wi-Fi может быть небезопасным, научите их подключаться через **защищённый VPN-канал**.
8. Установите ПО, которое может **проверять и обновлять настройки конфиденциальности** в социальных сетях.
9. Обсудите с ребенком опасный контент, с которым он может столкнуться: порнографию, пропаганду расовой ненависти, насилия и самоубийства.

13–17 лет

1. Используйте средства блокирования нежелательного контента как дополнение к стандартному родительскому контролю.
2. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
3. Приучите себя знакомиться с сайтами, которые посещают подростки.

4. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.
5. Посоветуйте детям скачивать приложения только из официальных магазинов и избегать сомнительных источников.

Как детям вести себя в интернете

Как в жизни, так и в интернете необходимо соблюдать простые правила приличия и безопасности.

- Не разглашай личную информацию! Если на каком-то сайте запрашивают **персональные данные** (имя, фамилию, адрес, дату рождения, номера документов), ни в коем случае не вводи их без взрослых.
- В соцсетях тоже не стоит рассказывать о себе слишком много: не указывай номер школы, **не ставь геолокацию** и отключи привязку фотографий к местоположению. Если тебе нет 15-16 лет, лучше вообще не публиковать свои фотографии. По возможности пользуйся псевдонимом.
- Пароль – тоже очень личная информация, держи его в тайне. Не пересылай его по электронной почте, **не пользуйся сервисами, которые сохраняют пароли**. Придумывай сложные, уникальные пароли.
- Не переписывайся **с незнакомцами**. Мошенник, педофил, злобный тролль может скрываться под любой маской. Поэтому никому, кроме оффлайн-знакомых, не доверяй личных сведений. Особенно тебя должно насторожить, если твой собеседник:

- явно намного старше тебя;

- просит прислать фото или какие-то данные;

- имеет очень маленький круг друзей в соцсетях;

- шантажирует или оскорбляет тебя.

- Если ты решил встретиться с человеком, с которым общался только онлайн, назначь встречу в общественном месте и приведи с собой друзей. Обязательно скажи взрослым, куда собираешься идти.
- Помни, что **из интернета ничего нельзя удалить.** Все, даже то, что выложено в закрытой группе или отправлено личным сообщением, ушло в Сеть, и стереть окончательно уже ничего нельзя. Ни в коем случае нельзя выкладывать фотографии документов. А фото других людей стоит выкладывать только в случае, если они на это согласны.
- Фишинг — это способ выманивать у человека его данные: логин, название учетной записи и пароль, используя сайт-двойник, очень похожий на настоящий. Учись отличать **поддельные сайты**.
- Аккуратнее с онлайн-покупками. Все сервисы, которые принимают деньги, должны иметь **зеленый значок «https»** рядом с названием.
- **Проверяй информацию.** Не стоит верить сайтам, на которых много рекламы, ссылок, шокирующих заголовков. Сомнительный факт можно проверить, обратившись ещё к двум-трем источникам, поискав информацию на других языках. Пример надежного источника – "Википедия", но и в ней бывают ошибки.
- Уважай себя, заботься о своей репутации. Не распространяй в интернете неприличную, компрометирующую кого-то информацию. Оскорбление в интернете ранит так же, как и в реальной жизни. **Никогда не участвуй в травле!** За грубое поведение тебя могут заблокировать или исключить из сообщества. И сам не терпи агрессию, блокируй или удаляй тех, кто тебя унижает.
- Если что-то в интернете кажется тебе опасным, **сообщи об этом взрослому**, которому доверяешь.
- Соблюдать эти правила нужно не только в соцсетях, но и в **онлайн-играх**. Опасайся манипуляций со стороны товарищей по команде.

" Родители должны быть чуткими к поведению своего сына или дочери, чтобы вовремя помочь, поддержать, разговорить, найти нужные слова, чтобы дать объективную оценку происходящему.

А до детей достаточно донести одно главное правило: не делай в интернете того, чего не сделаешь в реальной жизни. Ведь сегодня оффлайн и онлайн уже так тесно переплетены, что почти не отличаются.

" Невозможно всегда находиться рядом с ребенком и постоянно его контролировать. Доверительные отношения, доброжелательный диалог зачастую может быть гораздо конструктивнее, чем постоянное «отслеживание» посещаемых сайтов и блокировка контента.»