ДЕТИ И ИНТЕРНЕТ

Рекомендации
Академии правоохранительных органов
при Генеральной прокуратуре РК

Сегодня на современного ребенка влияет окружающий его мир, наполненный цифровыми технологиями.

Что дают ребенку эти модные технологические устройства?

- ✓ способность выхода в интернет, возможности которого безграничны. Все дети умело пользуются интернетом, входят в социальные сети, группируются по интересам, учатся, получают полезную информацию, организуют дискуссии и развиваются.
- ✓ позволяют быть оперативными. Использование смартфонов, помогает быстро решать общественные и личные вопросы.
- ✓ оказывают помощь в процессе обучения.

Что делать?

Несмотря на все риски, нельзя Интернет назвать злом и не нужно его сторониться. Соблюдение определенных правила поведения в сети оградят вашего ребенка от угроз и опасностей интернета и помогут ему развивать навыки и получать новые знания.

Однако,
вместе с положительными тенденциями и пользой интернета, он содержит и опасности, которые могут оказать негативное влияние на еще не сформировавшуюся личность.

В чем опасность интернета?

негативное влияние на психику ребенка. Интернет содержит много разного запрещенного контента, имеющего свободный доступ - порнография, экстремизм, терроризм, суицид, рекламирование алкоголя, наркотиков.

убивает время.

Неограниченное время пребывания в Интернете отвлекает детей от реального мира, отрицательно сказывается на их успеваемости и здоровье.

опасные знакомства.

В Интернете обитают разные люди, в т.ч. с корыстными и негативными намерениями. Например, в результате общения в сети, ребенок подвержен риску вовлечения в радикальную религиозную группу, секту, либо общество самоубийц.

азартные игры

Интернет не просто информационная база. Он также содержит много ресурсов, вызывающих зависимость, в том числе финансовую. К ним можно отнести азартные игры, интернет-казино.

Правила поведения в сети!

1. ***Не раскрывай свои личные данные!***

При регистрации на каком-либо сайте (социальные сети, интернет-магазин и т.д.) не стоит указывать все свои личные сведения. Не обязательно вводить свои настоящие данные.

При переписке с друзьями в соц.сетях, форумах, по электронной почте не указывайте персональные сведения о себе и родителях, адресе проживания, месте учебы, местах работы, номерах банковских карточек.

Помните! Любой безобидной на первый взгляд информацией, размещенной в сети, могут воспользоваться преступники!

2. ***Интернет знакомства не безопасны!***

Не стоит доверять всем в сети, кто пытается с вами подружиться! Не стоит приглашать новых интернет знакомых к себе домой или ходить в гости к ним.

Помните! Многие преступники с помощью интернета совершают свои преступления (кражи квартир, похищение детей и т.д.)!

3. ***Используй средства защиты от интернет-угроз (антивирусные программы, брандмауэр)!***

Не стоит доверять подозрительным письмам, которые пришли на почтовый ящик, даже если они от друзей из списка ваших контактов. Перед открытием вложенного файла, обязательно проверьте его на наличие вирусов.

Если подозрительное письмо пришло от друзей, из списка контактов, то для убеждения в безопасности письма и вложенного в него файла, созвонитесь с отправителем.

Помните! Вирусы могут уничтожить важные для вас данные или заблокировать к ним доступ, похитить их с целью последующего выкупа!

4. ***Используй безопасные браузеры для детей!***

Например, «Gogul» **(http://gogul.tv),** «KIDO'Z» **(http://kidoz.net/),** разработанные специально для детей и содержащие интернет ресурсы, одобренные психологами и педагогами.

5. Используй безопасные поисковики!

Интернет предлагает разнообразные безопасные поисковики, например «АгА» **(http://www.big-big.ru/poiskoviki/agakids.ru.html), (http://www.agakids.ru/).** Он выдает безопасные страницы при поиске. Можно использовать виртуальную поисковую систему для детей: «Quintura **(http://www.irdir.info/ru/ext/dir-resource/6682/).**

6. Используй функцию конфиденциальности!

В интернете старайтесь не использовать свое настоящее имя.

7. Не реагируй на яркие рекламы!

Не стоит кликать по рекламным уведомлениям или ярким картинкам в интернете.

Помните! За красивой рекламой или сообщением о выигрыше могут стоять интернет мошенники, готовые похитить ваши данные или причинить материальный ущерб, заразить компьютер вредоносной программой или заблокировать систему!

8. Будь осторожен при сканировании QR-кодов!

Не стоит реагировать на каждый обнаруженный, в том числе интернете QR-код ради любопытства.

Помните! Открыв графическую ссылку вы можете попасть на фишинговый или вредоносный сайт!

9. Обращай внимание на адрес сайта!

Перед открытием любого интернет ресурса убедитесь в правильности адреса. Использование в адресе даже одной неправильной буквы или символа может привести на вредоносный сайт.

10. Обновляй программное обеспечение

Постоянное обновление программы позволяет поддерживать защиту вашего компьютера.

Помните!
Киберпреступники ищут уязвимости в программном обеспечении!

Что должны знать родители?

- ***чем интересуется ребенок, посещая интернет.***
- ***какие сайты больше всего он посещает.***
- ***с кем в сети он общается.***
- ***в каких группах он состоит.***

Как родители могут защитить своего ребенка в сети?

- ✓ создайте график для посещения ребенком интернета;
- ✓ установите на компьютер (ноутбук) программу «родительский контроль» (при помощи «Интернет Цензора» настройте «белые списки» страниц, разрешенных к посещению).
- ✓ установите пароль на компьютер;
- ✓ используйте программу контроля доступа «Rejector.ru» (на официальном сайте);
- ✓ установите на компьютере безопасный режим для ребенка;
- ✓ расскажите ребенку об опасностях, с которыми он может столкнуться в Интернете.

Ребенок должен понять - не всякая информация достоверная и не каждому можно доверять, нельзя участвовать в онлайн аукционах и пользоваться без вашего ведома платежными интернет системами, нельзя публиковать в сети домашний адрес, много рассказывать о себе и своей семье, хвастаться дорогими гаджетами и покупками, нельзя общаться с посторонними взрослыми людьми, особенно если они просят прислать фото или предлагают встретиться;

- ✓ установите с ребенком доверительные отношения (поговорите о том, какие сервисы, сайты ему интересны и какие можно посещать. ограничьте права пользователя;
- ✓ научите ребенка реагировать на киберагрессию.

(договоритесь с ребенком, что в случае получения им оскорбительных писем или угроз, он должен рассказать вам об этом. Объясните, что хамство в сети является признаком плохого воспитания и неуверенности в себе.

Лучший способ защититься – игнорировать оппонента, внести его в черный список самостоятельно или через модератора).

- ✓ расскажите ребенку, что в интернете можно столкнуться с мошенниками, которые могут нанести вам материальный ущерб или уничтожить ваши программы, важную информацию (он должен понять, что никому нельзя передавать личные данные, банковские счета родителей, ПИН коды, пароли, данные родителей, адреса, место учебы);
- ✓ приложения и игры в смартфон можно скачивать только с официальных сервисов: AppStore, Google Play и Windows Market (с других ресурсов не безопасно).
- ✓ отключите мобильный интернет через оператора связи (если есть необходимость запрета выхода в интернет через смартфон).

Помните!

Какие бы эффективные меры защиты или программы вы не использовали, ничто не заменить живое общение!

Больше общайтесь со своим ребенком и интересуйтесь его проблемами!

Информация предоставлена **Региональным хабом по противодействию глобальным угрозам** (проект Академии правоохранительных органов при Генеральной прокуратуре РК).

Контакты: +7(7172)71-20-19, 71-20-33
7171425@prokuror.kz
7171433@prokuror.kz

ASTANA REGIONAL HUB FOR COUNTERING GLOBAL THREATS