

СОВЕТЫ ПО БЕЗОПАСНОЙ РАБОТЕ В ИНТЕРНЕТЕ

СЛОЖНЫЙ ПАРОЛЬ

Если ты регистрируешься на сайте, в социальной сети или в электронной почте, придумай сложный пароль, состоящий из цифр, больших и маленьких букв и знаков. Чем сложнее пароль, тем сложнее взломать твой аккаунт. Помни, что твой пароль можешь знать только ты.



СОВЕТ ВЗРОСЛЫХ

Всегда спрашивай взрослых о непонятных вещах, которые ты встречаешь в Интернете: ты не знаешь, какой пункт выбрать, на какую кнопку нажать, как закрыть программу или окно. Они расскажут тебе, как поступить - что можно делать, а что нет.



ЛИЧНАЯ ИНФОРМАЦИЯ

Никогда не рассказывай о себе и знакомым людям в Интернете: где ты живешь и учишься, не сообщай свой номер телефона. Не говори никому о том, где работают твои родители и номера их телефонов. Эта информация может быть использована во вред тебе и твоим родителям.



НЕ ОТПРАВЛЯЙ СМС

Если в Интернете ты решил скачать картинку, игру или мелодию, а тебя просят отправить смс - не делай этого! Смс на короткие номера могут стоить несколько сотен рублей. Ты потеряешь деньги, которые мог бы потратить на что-то другое.



НЕ ЗАБУДЬ ВЫЙТИ

При использовании чужих компьютеров или мобильных устройств, не забывай выходить из своего ящика электронной почты или профилей в социальных сетях. Иначе, следующий пользователь этого устройства сможет просмотреть твою личную информацию.



ОСТОРОЖНО, НЕЗНАКОМЕЦ

Никогда не отвечай на сообщения от незнакомцев в Интернете и не отправляй им смс. Если незнакомый человек предлагает встретиться или пишет тебе оскорбительные сообщения - сразу скажи об этом взрослым! Не все люди являются теми, за кого себя выдают в Интернете!



БЕСПЛАТНЫЙ WI-FI

При выходе в Интернет через общественную Wi-Fi сеть, не совершай никаких покупок и оплаты, не проверяй личную электронную почту и не передавай конфиденциальную информацию. Злоумышленники могут похитить ваши пароли и данные.



ЗАЩИТИ КОМПЬЮТЕР

Попроси родителей или сам установи систему фильтрации SkyDNS на сайте www.skydns.ru. Она защитит тебя от потери денег и кражи паролей, а также будет блокировать большую часть рекламы, ускоряя загрузку страниц в Интернете.



1. Перед регистрацией нужно собрать сведения о социальной сети. Отзывы желательно искать на независимых интернет-ресурсах.

2. При регистрации в социальной сети нужно использовать сложный пароль. Это - залог того, что учётную запись не взломают и не узнают конфиденциальные данные ребёнка.

3. Не рекомендуется использовать при регистрации в социальной сети возможность указания данных почтового ящика ребёнка. Это может привести к неконтролируемому оповещению о его учётной записи тех, с кем когда-либо велась переписка.

4. Нельзя никому сообщать данные для входа в учётную запись в социальной сети. Мошенники иногда рассылают пользователям социальных сетей электронные письма, в которых под разными предлогами просят сообщить пароль.

5. После завершения работы в социальной сети нужно выполнять процедуру выхода. Если не выйти из учётной записи, а просто закрыть окно браузера, доступ к учётной записи могут получить посторонние. Особенно это справедливо при работе с учётной записью социальной сети на чужом компьютере.

6. Приучайте ребёнка к мысли, что каждого нового виртуального друга нужно сначала вызывать в любой видеочат, и лишь затем начинать делиться чем-то личным. Ключом к доверию ребёнка чаще всего становятся сообщества. По статистике подросток практически 100% добавит в друзья и начнёт общение с человеком, если тот состоит в том же значимом для ребёнка сообществе в соцсети. А дружба с организатором, или с кем-то из администрации игровых групп или групп по интересам – это особенно круто.

7. Воспользовавшись настройками учётной записи, ограничьте возможность связи с ребёнком посторонних.

8. Расскажите ребёнку о том, что переходить по ссылкам, которые кто-либо отправил ему в сообщении, опасно. Эти ссылки могут вести на сайты, распространяющие вредоносные программы. Опасно скачивать и открывать файлы, приходящие в сообщениях.

9. Объясните ребёнку, что он не должен никому сообщать каких-либо личных сведений

о себе. К таким сведениям относятся номер телефона, домашний адрес, время начала занятий в школе и другие. Эти данные могут быть использованы злоумышленниками. Такие сведения не следует публиковать даже в том случае, если опубликованная запись предназначена только для друзей. (На вашей странице в соцсети также не должно быть ни телефонов, ни геолокационных привязок к фотографиям, ни кликабельных ссылок на страницы ваших детей).

11. Расскажите ребёнку о том, что если он заметил что-то странное в своей учётной записи, то пароль к ней нужно немедленно сменить. На взлом учётной записи могут указывать следующие признаки: исчезли какие-нибудь фотоснимки, или, наоборот, появились новые, которых никто не выкладывал, на стене появились неожиданные записи.

12. Дружите! «Зафрендитесь» с ребёнком во всех соц. сетях, болтайте с ним во всех вайберах и воцапах, где он общается со своими друзьями. Пусть ребёнок знает, что вы – не враг его пространства, от которого нужно скрывать всё самое интересное. Не считайте, что закрыв ноутбук, ребёнок может решить проблемы, возникшие в его виртуальных компаниях. Для большинства детей то, что происходит с ними в интернет-общении более значимо, чем отношения с одноклассниками. Большинство детей не рассказывает родителям ни о травле, ни о ссорах, ни о сложностях в сети, потому что уверены, что родители не поймут или вовсе запретят выходить в интернет. Поощряйте откровенность ребёнка. Рано или поздно ваше терпение и внимание обязательно будет вознаграждено доверием. Пользуясь этими рекомендациями и ознакомив с ними ребёнка, вы значительно повысите уровень его безопасности в социальных сетях.

Специальное программное обеспечение для обеспечения безопасности детей:

Интернет Цензор. Это интернет-фильтр, который использует технологию "белых списков", составленных вручную. Приложение позволяет надёжно ограничивать доступ детей к нежелательным веб-сайтам.

Time Boss. Данное приложение предназначено для организации контроля за тем, как дети пользуются компьютером. Оно позволяет ограничивать время использования компьютера, вести подробные журналы работы, периодически делать копии экрана.

KinderGate. Приложение, которое позволяет организовать расширенную защиту ребёнка от посещения нежелательных сайтов на основе динамических механизмов анализа содержимого.

Средства мобильных операционных систем, направленные на защиту детей.

Ребёнок, который пользуется мобильным телефоном, подвергается двум основным видам рисков.

1. Совершения неоправданных затрат при использовании коротких номеров сервис-провайдеров.

2. Просмотр веб-страниц с нежелательным содержанием.

Основные услуги, характерные для данного направления защиты детей.

- Оператор МТС (<http://www.mts.ru>) предлагает набор услуг «Детский пакет».

- Оператор МегаФон (<http://megafon.ru>) предлагает услугу «Детский интернет».

- Оператор Билайн (<http://beeline.ru>) предлагает услугу «Стоп-контент».

По ссылкам ниже вы найдете подробные инструкции по безопасной настройке детских аккаунтов: (<http://stop-ugroza.ru/rules/zashhishhaem-rebenka-nastrojki-bezopasnosti-v-sotsialnyh-setyah-i-servisah>).