

Правовая ответственность

1. Федеральный закон от 28.07.2012 № 139-ФЗ "О внесении изменений в федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации.
2. Федеральный закон "О рекламе" от 13.03.2006 N 38-ФЗ
3. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ред. от 19.02.2018)
4. Статья 137. Нарушение неприкосновенности частной жизни;
5. Статья 242. Незаконные изготовление и оборот порнографических материалов или предметов;
6. Постановление Правительства РФ от 26 октября 2012 г. N 1101 "О единой автоматизированной информационной системе "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено"

Где находятся источники угроз, которые несет всемирная сеть?

Личная безопасность в сети предполагает, прежде всего, знакомство с основными источниками, которые могут нести угрозу. Существует много способов взлома ПК с целью кражи личных данных и паролей пользователей.

Самыми распространенными из них являются:

- социальная инженерия, основанная на определенных психологических уловках и рассчитанная на доверчивых пользователей. Например, на электронную почту присылается письмо от имени какого-нибудь сайта с просьбой выслать данные для подтверждения пароля, а на самом деле содержащее вирусный файл;
- большинство вирусов скрытано в различных бесплатных программах для скачивания;
- заражение компьютера может происходить через так называемые дыры в программном обеспечении, которые умело используют хакеры;
- зачастую вирусы внедряются посредством фишинга (организации поддельных сайтов, которые копируют странички популярных фирм). Следует помнить, что все так называемые грязные сайты являются первыми распространителями вредоносных программ.



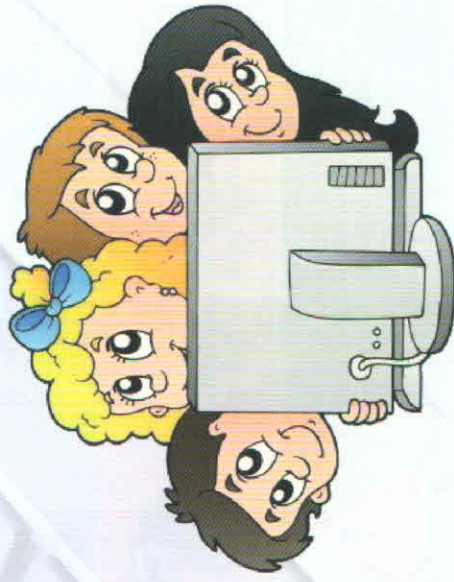
Учебно-методический центр по гражданской обороне, чрезвычайным ситуациям и пожарной безопасности Удмуртской Республики



«ИНТЕРНЕТ» Территория безопасности

| | |
|---|---------------------------|
| Приемная Главного управления МЧС России по УР | (3412) 72-81-75; 72-72-08 |
| Единый телефон спасения | 112 |
| Единый телефон пожарных и спасителей | 101; 011 |
| Полиция | 102; 022 |
| Скорая помощь | 103; 033 |
| Аварийная газовая служба | 104; 044 |
| Телефон доверия | (3412) 51-99-99 |
| Телефон ЦЭПП (приемная) | (495) 989-50-53 |
| (горячая линия) | (495) 216-50-50 |
| УМЦ по ГО и ЧС УР | (3412) 74-14-54 |

426019, г. Ижевск
ул. Областная, 6



г. Ижевск, 2018 г.

Советы по безопасной работе в сети Интернет: для родителей

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.

ЛИЧНАЯ ИНФОРМАЦИЯ

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

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 посмотреть твою личную информацию.

БЕСПЛАТНЫЙ Wi-Fi

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

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.

НЕ ОТПРАВЛЯЙ SMS

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

ОСТОРОЖНО, НЕЗНАКОМЕЦ

Никогда не отвечай на сообщения от незнакомцев в Интернете и не отправляй им SMS. 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!

ЗАЩИТИ КОМПЬЮТЕР

Попроси родителей или сам установи систему фильтрации (антивирус). Она защитит тебя от потери денег и кражи паролей, а также будет блокировать большую часть рекламы, ускоряя загрузку страниц в Интернете.

1. Не запрещайте ребенку заводить свою страничку в социальной сети, если он об этом просит. Наверняка это уже сделал многие из его друзей, и он тоже хочет, не делайте его изгоем среди них и не заставляйте делать себе тайный аккаунт.

Наоборот - сядьте вместе, вместе сделайте страничку, походите по сети, посмотрите разные опции, группы, паблики, объясните ему, какие есть возможности, что такое тэги, покажите, что делать с неприличными картинками, рекламой и спамом, своим примером покажите грамотную реакцию на все это.

2. Научите ребенка правилам безопасности в интернете: не вывешивать в открытом доступе свои фотографии и контакты, не реагировать на «привлекательные» предложения от чужих людей, помнить, что он никогда не знает, кто на самом деле незнакомый человек, который представляется, например, его ровесником. Объясните, какие существуют опасности.

3. Время от времени просматривайте список «друзей» вашего ребенка, обращайтесь внимание на взрослых людей, если это не учителя, смотрите, какие группы он читает и на какие паблики подписан. В интернете на ребенка посыплется масса привлекательно преподносимой информации о наркотиках, самоубийствах и прочих вещах.

4. И да, «группы про китов» действительно существуют и действительно несут угрозу для ребенка. Объясните ребенку бессмысленность участия в этом и то, что за этим стоят взрослые люди, которые ищут управляемых детей для своих целей.

Если что-то непонятно,
Страшно или неприятно -
Быстро к взрослым поспешите,
Расскажите и покажите.
Есть проблемы в Интернете?
**Вместе взрослые и дети
Могут все решить всегда
Без особого труда.**



Советы по безопасной работе в сети Интернет: для школьников

1. Проводи больше времени с реальными друзьями, чем с виртуальными.

2. Сразу прекращай контакт с любым, кто пытается давить для получения информации о тебе (имени, возраста, роста и размера, фотографий, адреса, информации о семье).

3. Будь очень осторожен с незнакомцами, которые пытаются настроить тебя против твоей семьи, обещая быть твоим лучшим другом (они могут послать тебе подарки и говорить много комплиментов, но в то же время они распускаются твоим временем и критикуют твоих родителей).

4. Не обменивайся с незнакомцами фотографиями через Интернет.

5. Не открывай электронные сообщения от незнакомых людей и не загружай вложенные в них файлы.

6. Не сообщай информацию о себе для того, чтобы получить что-то бесплатно.

7. Не соглашайся на встречу с теми, кого ты не знаешь в реальной жизни.

С незнакомыми людьми

Ты на встречу не иди!

С грубиянами в сети

Разговор не заводи.

Ну и сам не оплошай -

Никого не обижай.

Кто грубит в эфире - скверно

Поступает он не верно!

«Троллями» таких зовут,
Дружку с ними не ведут.
Ничего глупей нет более.
Игнорируйте таких -
Покидайте сайты их.

