ЧЕМ ГРОЗИТ УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ?

Завладев персональными данными, мошенники могут:

- *оформить кредит в банке;*
- *«повесить» долги или фирму;*
- *совершить незаконные действия с вашей недвижимостью;*
- *распорядиться средствами с банковских карт;*
- *открыть электронный кошелек;*
- *зарегистрироваться на сайтах знакомств, онлайн-игр и казино;*
- *шантажировать вас или ваших родственников;*
- *использовать вашу личность как «подменную» для мошеннических действий;*
- *устроить кибербуллинг;*
- *использовать ваши данные в собственных интересах, например, навязывать услуги, распространять противоправный контент.*

Поговорим о цифрах

47% россиян зарегистрированы в социальных сетях;

6,5 часов в сутки — средняя продолжительность времяпрепровождения в сети «Интернет»;

46% наших соотечественников постоянно совершают онлайн-покупки.

Отчет «Global Digital 2018», подготовленный аналитическим агентством «We Are Social» и SMM-платформой «Hootsuite

Больше полезной информации: http://персональныеданныедети/

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ЗЛОУМЫШЛЕННИКОВ В СЕТИ ИНТЕРНЕТ

Авторы :
Алиев А.М, Жученко В.С, Саенко Д.А.

НЕ ПОНИМАЕТЕ О ЧЕМ ГОВОРИТ ВАШ РЕБЕНОК?

Кринж - это отвращение, например отвратительные бессмысленные ролики вызывают много кринжа.

Краш - человек, который нравится.

Изи используется в играх и иногда в жизни, что-то легкое и простое, даже слишком!

Хайповый означает модный, в теме, шарит что происходит в мире моды. **Хайп** это то, что сейчас модно. **Хайпим** означает тусим, развлекаемся, зажигаем.

Трэш - вещь, которая уже не актуальна. **Трэшиться** - то есть прикалываться, делать что-то не всерьёз.

Шер - поделиться чем-то в социальной сети.

КОНТАКТЫ

НЦПТИ

ИНТЕРНЕТ БЕЗ УГРОЗ

Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет

Веб-сайт: НЦПТИ.РФ
Телефон: (863) 201-28-22
E-mail: info@ncpti.ru

Министерство общего и профессионального образования Ростовской области

Веб-сайт: http://www.rostobr.ru
Телефон: (863) 240-34-97
E-mail: min@rostobr.ru

Безопасность детей в интернете

ОСТОРОЖНО:

ВИРУСЫ И ДРУГИЕ ВРЕДОНОСНЫЕ ПРОГРАММЫ (ЧЕРВИ, ТРОЯНЫ)

В Интернет ты заходишь через компьютер. Это может быть школьный или библиотечный компьютер, твой личный или тот, которым пользуется вся семья.

Любому компьютеру могут повредить вирусы, их еще иногда называют вредоносными программами. Они могут **уничтожить** важную информацию **или украсть** деньги через Интернет.

- **Для защиты компьютера** на нём установлены специальные защитные программы и фильтры. Не меняй ничего в их настройках!
- **Не сохраняй подозрительные файлы** и не открывай их.
- Если антивирусная защита компьютера не рекомендует, **не заходи на сайт, который считается «подозрительным».**
- Никому **не сообщай свой логин с паролем** и не выкладывай их в Интернете – относись к ним так же бережно, как к ключам от квартиры.

ВИРТУАЛЬНЫЕ МОШЕННИКИ (ВОРЫ) И ДРУГИЕ ПРЕСТУПНИКИ ИНТЕРНЕТА

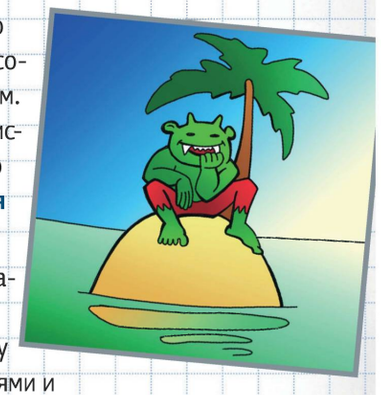
Ты знаешь, что вне дома и школы есть вероятность столкнуться с людьми, которые могут причинить тебе вред или ограбить. В Интернете также есть злоумышленники – ты должен помнить об этом и вести себя так же осторожно, как и на улице или в незнакомых местах.

- **Не сообщай свой адрес или телефон** незнакомым людям и никогда не выкладывай в Интернете. Никогда **не высылай свои фотографии** без родительского разрешения. Помни, что **преступники могут использовать эту информацию** против тебя или твоих родных.
- **Если ты хочешь поучаствовать** в каком-нибудь конкурсе, где нужно указывать свои данные, посоветуйся с родителями.
- Никогда **не соглашайся прийти в гости к человеку, с которым ты познакомился в Интернете.** Если назначается встреча, она должна проходить в людном месте и желательно с присутствием родителей. Помни, что под маской твоего ровесника **может скрываться взрослый человек с преступными намерениями.**

ГРУБИЯНЫ И ХУЛИГАНЫ (ТРОЛЛЬ, ПРОВОКАТОР) В ИНТЕРНЕТЕ: КАК СЕБЯ ВЕСТИ?

Кроме преступников в Интернете есть просто злые и невоспитанные люди. Ради собственного развлечения они могут обидеть тебя, прислать неприятную картинку или устроить травлю. Ты можешь столкнуться с такими людьми на самых разных сайтах, форумах и чатах.

- Помни: **ты не виноват**, если получил оскорбительное сообщение. Не нужно реагировать на грубых людей – просто прекрати общение.
- **Если тебе угрожают** по Интернету, не стесняйся сообщить об этом родителям. Помни, что цель угроз – испугать тебя и обидеть. Но **подобные люди боятся ответственности.**



- Коллективное преследование – это крайнее проявление жестокости. Жертву забрасывают оскорблениями и угрозами, его фотографию искажают и все данные публикуют. **Никогда не участвуй в травле и не общайся с людьми, которые обижают других.**
- Всегда **советуйся с родителями** во всех указанных случаях.

КАКИЕ УГРОЗЫ СУЩЕСТВУЮТ В СЕТИ ИНТЕРНЕТ?

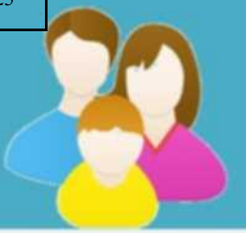
КИБЕРБУЛЛИНГ

Интернет - мошенничество

ПРОПАГАНДА НАРКОТИКОВ И АЛКОГОЛЯ

ИГРОМАНИЯ

ЧТО ДЕЛАТЬ РОДИТЕЛЯМ?



Не пытайтесь насильно ограничивать ребенка в использовании сети Интернет

Частая ошибка родителей: мы пытаемся сократить время пребывания ребенка в сети, вместо того, чтобы работать над качеством. Ребенок может провести час на сайте с опасным контентом и два часа на образовательном канале. Работайте НЕ над временем.

Будьте друзьями

В 13-17 лет нужно быть максимально лояльными с детьми, вряд ли они будут доверять тирану.

Не забывайте беседовать с детьми об их друзьях в интернете, о том, чем они заняты, таким образом, будто речь идет о друзьях в реальной жизни. Делайте беседу непринужденной. Помните, допросы только оттолкнут.

Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с интернетом

Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

ЧТО ДЕЛАТЬ РОДИТЕЛЯМ?

Приучите себя знакомиться с сайтами, которые посещают подростки

Делайте это аккуратно, чтобы у ребенка не возникало чувство излишнего контроля над ним. Регистрируйтесь во ВКонтакте, Instagram, обычно именно там подростки делятся своими новостями и мыслями.

Объясните детям, что ни в коем случае нельзя использовать сеть для хулиганства, распространения сплетен или угроз другим людям. Напомните, что это противоречит не только морали, но и закону.

Обсудите с ребенком его новости в социальных сетях. Предупредите о том, что любая фотография, текст навсегда остаются в интернете, независимо от того, удалили ее с личной страницы или нет. Прежде чем что-то публиковать - пусть ребенок подумает: не отразится ли это на его будущем?

НЕ ПОНИМАЕТЕ О ЧЕМ ГОВОРИТ ВАШ РЕБЕНОК?

Кринж - это отвращение, например отвратительные бессмысленные ролики вызывают много кринжа.

Краш - человек, который нравится.

Изи используется в играх и иногда в жизни, что-то легкое и простое, даже слишком!

Хайповый означает модный, в теме, шарит что происходит в мире моды. **Хайп** это то, что сейчас модно. **Хайпим** означает тусим, развлекаемся, зажигаем.

Трэш - вещь, которая уже не актуальна. **Трэшиться** - то есть прикалываться, делать что-то не всерьёз.

Шер - поделиться чем-то в социальной сети.

КОНТАКТЫ

НЦПТИ

ИНТЕРНЕТ БЕЗ УГРОЗ

Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет

Веб-сайт: НЦПТИ.РФ
Телефон: (863) 201-28-22
E-mail: info@ncpti.ru

Министерство общего и профессионального образования Ростовской области

Веб-сайт: http://www.rostobr.ru
Телефон: (863) 240-34-97
E-mail: min@rostobr.ru

Безопасность детей в интернете

СЭД МВД
№1-534 от 12.02.2025

Что включают в себя персональные данные?

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

фамилия, имя и отчество, дата и место рождения, адрес, семейное положение, паспортные данные, номер телефона, профессия, доходы, ИНН,

Нормативно-правовая база по защите персональных данных:

Где существует наибольший риск потери персональных данных ?

Социальные сети и мессенджеры

Аккаунт Google или Apple ID

Электронная почта

Банковские данные

Аккаунты в игровых сервисах

Незащищённая Wi-Fi-точка

Мобильные приложения

ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ ОБНАРУЖИЛИ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ В ИНТЕРНЕТЕ?

Написать жалобу →

Владелец аккаунта

Тех.поддержка

Администрация сайта

Когда невозможно установить источник распространения персональных данных или связаться с ним? напрямую ?

Нужно обратится в **Прокурату** или Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (**Роскомнадзор**).

ТОП-5 ОСНОВНЫХ СПОСОБОВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1

Используйте двухфакторную аутентификацию

2

Контролируйте доступ приложений к вашим данным

3

Пользуйтесь менеджерами паролей

4

Используйте только защищённое соединение

5

Пользуйтесь VPN, работая с публичными Wi-Fi-точками