



Безопасность в Интернете

Для школьников 5-11 классов



Защита данных



Без кибербуллинга



Критическое мышление

Уважай себя и других в сети!



КИБЕРБУЛЛИНГ

Травля в интернете



Что это?

Оскорбления, угрозы, распространение слухов и унижение чести в интернете.

Как распознать?

- Агрессивные комментарии
- Создание фейковых страниц
- Отправка оскорбительных картинок

Как защититься?

- | | |
|---|---|
| 1 Не отвечай на агрессию
Игнорируй провокаторов | 2 Блокируй обидчиков
Используй функции блокировки |
| 3 Сохраняй доказательства
Делай скриншоты | 4 Обратись к взрослым
Родители и учителя помогут |

 **8-800-250-00-15** Линия помощи «Дети Онлайн».
Звонок абсолютно бесплатный. Профессиональные советы экспертов и психологов по борьбе с кибербуллингом.

Помни: Ты не один! Останови травлю!



ОПАСНЫЕ НЕЗНАКОМЦЫ

Онлайн-груминг



Что это?

Взрослые, которые заводят знакомства с детьми в интернете для их эксплуатации.

Как распознать?

- Задают слишком личные вопросы
- Предлагают подарки или деньги
- Просят хранить общение в секрете

Как защититься?

1 Не добавляй незнакомцев

В друзья и контакты

2 Не делись личной информацией

Адрес, телефон, школа

3 Не назначай встреч

Без родителей не ходи

4 Расскажи взрослым

Если чувствуешь опасность

 **8-800-2000-122** Единый телефон доверия для детей, подростков и их родителей при любых сложных жизненных ситуациях.

Помни: Настоящий друг не просит хранить секреты от родителей!



КРАЖА ПЕРСОНАЛЬНЫХ ДАННЫХ

Защита личной информации



Что это?

Похищение личной информации (адрес, пароли, фото) для мошенничества и шантажа.

Никогда не делись:

- Паролями от аккаунтов
- Домашним адресом и телефоном
- Данными банковских карт



Как защитить свои данные?

1

Используй сложные пароли

Разные для каждого сайта

2

Не переходи по подозрительным ссылкам

Они могут вести на фишинговые сайты

3

Проверяй настройки приватности

Ограничь доступ к профилю

4

Включи двухфакторную аутентификацию

Дополнительная защита аккаунта

Твои данные — твоя безопасность!



НЕЖЕЛАТЕЛЬНЫЙ КОНТЕНТ

Как избежать опасного контента



Что это?

Информация, которая может навредить: насилие, жестокость, сцены терроризма, порнография, пропаганда наркотиков.

Как распознать?

- Пугающие и агрессивные картинки
- Предложения перейти по сомнительным ссылкам
- Реклама запрещенных товаров

Как защититься?

1 Не открывай подозрительные ссылки

Особенно от незнакомцев

2 Используй родительский контроль

Настрой фильтры в браузере

3 Закрывай вкладки с нежелательным контентом

Не продолжай просмотр

4 Расскажи родителям

Если увидел что-то страшное

Если контент вызывает тревогу — немедленно закрой его!



ФИШИНГ И МОШЕННИЧЕСТВО

Как не попасть на удочку мошенников



Что это?

Мошенничество, при котором злоумышленники пытаются получить твои личные данные или деньги через поддельные сайты и сообщения.

Признаки мошенничества

- Сообщения о "выигрыше" или "блокировке аккаунта"
- Просьба перейти по ссылке и ввести пароль
- Требование оплатить "услуги" или "штрафы"

Как защититься?

1

Проверяй адрес сайта

Мошенники используют похожие адреса

2

Не вводи пароли на подозрительных сайтах

Официальные сервисы не просят пароль по почте

3

Не переводи деньги незнакомцам

Даже если обещают вернуть в двойном размере

4

Сообщай о мошенниках

Расскажи родителям и заблокируй отправителя

Бесплатный сыр бывает только в мышеловке!



ВРЕДОНОСНЫЕ ПРОГРАММЫ И ВИРУСЫ

Защита твоих устройств



Что это?

Программы, которые тайно проникают на устройство, чтобы украсть данные, навредить системе или показать рекламу.



Признаки заражения

- Устройство работает медленно
- Появляется непонятная реклама
- Программы открываются сами по себе



Как защититься?

1

Установи антивирус

Обновляй его регулярно

2

Не скачивай файлы с непроверенных сайтов

Особенно программы и игры

3

Обновляй операционную систему

Обновления закрывают уязвимости

4

Проверяй флешки перед открытием

На них могут быть вирусы

Если устройство заражено — обратиться к родителям!



ЦИФРОВОЙ СЛЕД И РЕПУТАЦИЯ

Что остается после тебя в интернете



Что это?

Все данные, которые ты оставляешь в интернете: посты, фото, комментарии, лайки. Они формируют твою цифровую репутацию.

Последствия негативного следа

- Отказ при поступлении в вуз или приеме на работу
- Проблемы с друзьями и семьей
- Использование данных мошенниками

Как управлять репутацией?

1 **Думай перед публикацией**

Представь, что это увидят все

2 **Не публикуй личные данные**

Адрес, телефон, название школы

3 **Настрой приватность**

Ограничь доступ к своим страницам

4 **Удаляй старые ненужные посты**

Регулярно проверяй свои аккаунты

Интернет помнит всё! Создавай положительный цифровой след.



ЗАВИСИМОСТЬ ОТ ИНТЕРНЕТА

Как найти баланс между онлайн и офлайн



Признаки зависимости

Постоянное желание проверять соцсети, тревога без телефона, потеря счет времени онлайн, замена реального общения виртуальным.

Чем опасна?

- Проблемы со сном и здоровьем
- Ухудшение успеваемости
- Одиночество и депрессия



Как контролировать время?

1

Установи лимиты времени

Используй таймеры и приложения контроля

2

Отключай уведомления

Не отвлекайся на каждое сообщение

3

Чередуй онлайн и офлайн

Найди хобби вне интернета

4

Общайся в реальной жизни

Встречайся с друзьями офлайн

Интернет — это инструмент, а не вся жизнь!



ФЕЙКИ И ДЕЗИНФОРМАЦИЯ

Как отличить правду от лжи в интернете



Что такое фейк?

Намеренно ложная информация, которая создается для обмана, манипуляции или привлечения внимания.

Признаки фейка

- Слишком сенсационные заголовки
- Отсутствие ссылок на источники
- Ошибки и опечатки в тексте



Как проверять информацию?

1

Ищи первоисточник

Проверяй, кто изначально опубликовал информацию

2

Сравнивай с другими источниками

Не доверяй только одному сайту

3

Проверяй дату публикации

Старые новости могут выдавать за новые

4

Не пересылай без проверки

Прежде чем делиться — убедись в правдивости

Доверяй, но проверяй! Не становись распространителем фейков.