

**БЕЗОПАСНОСТЬ**



**В СЕТИ ИНТЕРНЕТ**



# Недетские угрозы: Что угрожает нам в интернете?



**Компьютерный вирус** – это вид вредоносных программ. Вирусы могут повредить или даже уничтожить операционную систему со всеми файлами в целом. Вирусы распространяются через интернет.

## Методы защиты от вредоносных программ:



Используйте антивирусные программы



Не открывайте компьютерные файлы, полученные из ненадёжных источников



# Кибербуллинг

- это использование интернет-технологий с целью преследования, запугивания, унижения, оскорбления другого человека.



Травля по интернету — это угрозы и оскорбления от агрессивных пользователей в адрес другого пользователя.

## Кибербуллинг (кибертроллинг)

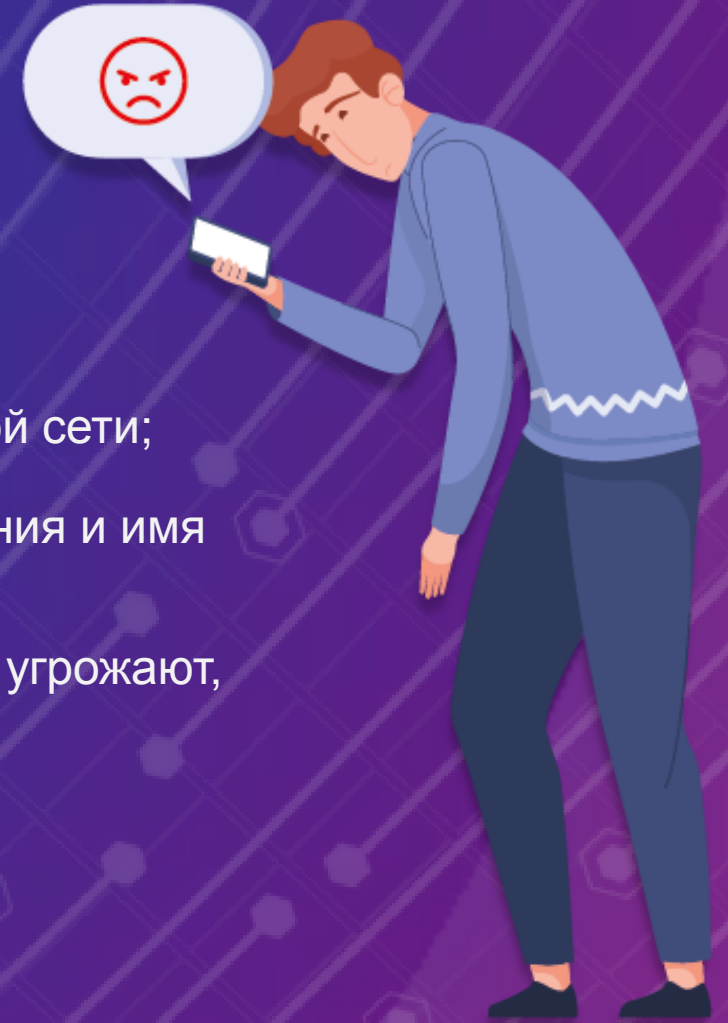
- Насмешливые фотографии, видео, которые могут опозорить человека;
- Поддельные учетные записи с использованием чужих фотографий;
- Издевательство и преследование в интернете;
- Публикация фотографий другого человека без его согласия;
- Преследование человека в соцсетях или онлайн-играх.



# Меня троллят, что делать?

Чтобы не пострадать от подобной травли, соблюдайте несколько правил:

1. **Не отвечайте** на агрессивные сообщения;
2. Занесите пользователей в **чёрный список**;
3. **Сообщите** о происходящем **технической поддержке** социальной сети;
4. **Делайте скриншоты переписки**, в котором виден текст сообщения и имя отправителя;
5. **Расскажите о происходящем взрослым**. Если вас запугивают, угрожают, то расскажите об этом родителям.





**Фишинг-атаки**— это рассылки мошеннических электронных писем и попытка обманом заставить получателей нажать на вредоносную ссылку или скачать зараженный файл, чтобы украсть их личную информацию.



Нельзя кликать на подозрительные ссылки, которые приходят по электронной почте или в сообщениях!

Например:

«Посмотри, что здесь о тебе говорят!»

«Ты стал обладателем нового iPhone — переходи по ссылке, чтобы забрать его»

Такие сообщения отправляют мошенники и при переходе по ссылке на компьютер попадает **опасный вирус**.



# Онлайн-груминг

Грумингом называют различные виды мошенничества в сети, когда преступники обманом втираются в доверие к пользователям и получают от них личные данные или деньги за несуществующие товары и услуги.



Если ваш друг или знакомый присылает сообщение с просьбой перечислить ему деньги на банковскую карту, обязательно позвоните другу по телефону и узнайте, нужны ли другу деньги или нет.



# Как защитить свой аккаунт?



Придумайте сложный пароль

Не используйте для паролей информацию, которую злоумышленники могут найти самостоятельно: дату рождения, номера документов, телефонов, имена ваших друзей и родственников, адрес;

Не используйте одинаковые пароли на разных сайтах;

Регулярно меняйте пароли;

Не храните информацию о паролях на компьютере. Если пароль слишком сложный, лучше записать его отдельно на лист бумаги или в блокнот, и хранить в надежном месте.





# Проводите чистку cookies

Файлы **cookies** — это временные файлы интернета, которые хранятся на вашем устройстве и содержат информацию о сайтах, которые вы посещаете.

Благодаря **cookies** сайты помнят ваши логины, пароли, электронную почту, историю интернет-заказов или состав корзины в интернет-магазине.

С их помощью также можно отслеживать вашу активность в интернете, ваши интересы и предпочтения.

С помощью **cookies** можно взломать почтовый ящик и получить доступ к личной информации.

Время от времени необходимо удалять файлы **cookies** на компьютере и в смартфоне.







# Не сообщайте свои персональные данные



**Персональные данные** - это ФИО, дата рождения, домашний адрес, номера телефона, банковских карточек, пароли.

Мошенники расспрашивают пользователей о работе родителей, о поездках, адреса, телефоны, номера машин. Вся эта информация может быть использована для совершения преступления.

Если в Сети у него кто-то попросит номер телефона или адрес, сначала нужно ответить: **«Спрошу разрешения у родителей»**.

Обычно после такого сообщения мошенники исчезают.



# Не скачивайте программы с подозрительных сайтов



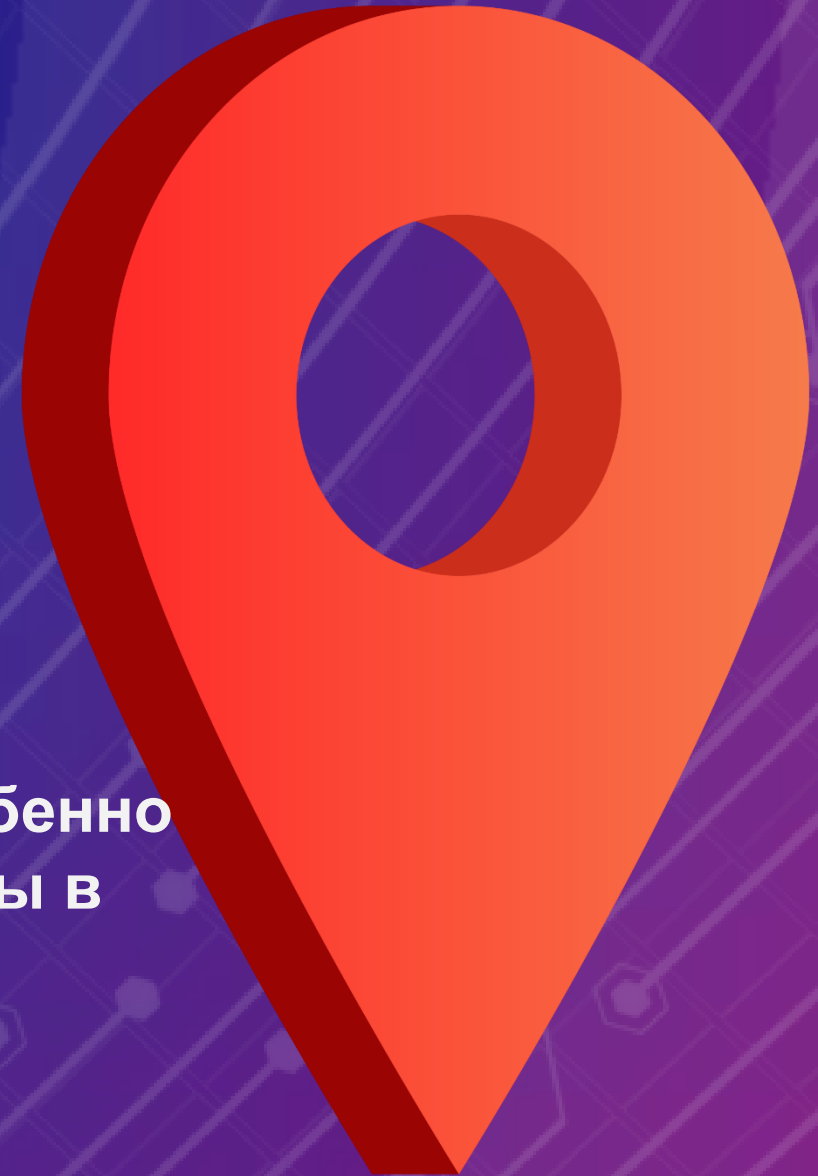
Скачав программу с непроверенного сайта, можно легко поймать вирус, из-за которого не только сломается техника, но и окажутся у злоумышленников номера банковских карт родителей.



# Не ставьте геометки под фото

По ним злоумышленники легко узнают, где живёт и учится человек.

**Рассказывать о каждом своем перемещении и особенно указывать домашний адрес или номер своей школы в социальных сетях не стоит**





# Не верьте в быстрый и лёгкий заработок

Стремление найти подработку и самому заработать деньги — это похвально;

Помните, что порядочный работодатель не будет просить перевести деньги перед оформлением на работу;

И ещё — что нельзя верить предложениям заработать сразу много денег, практически ничего не делая.





# Не доверяйте сообщениям о крупном выигрыше



**ВЫ ВЫИГРАЛИ!**

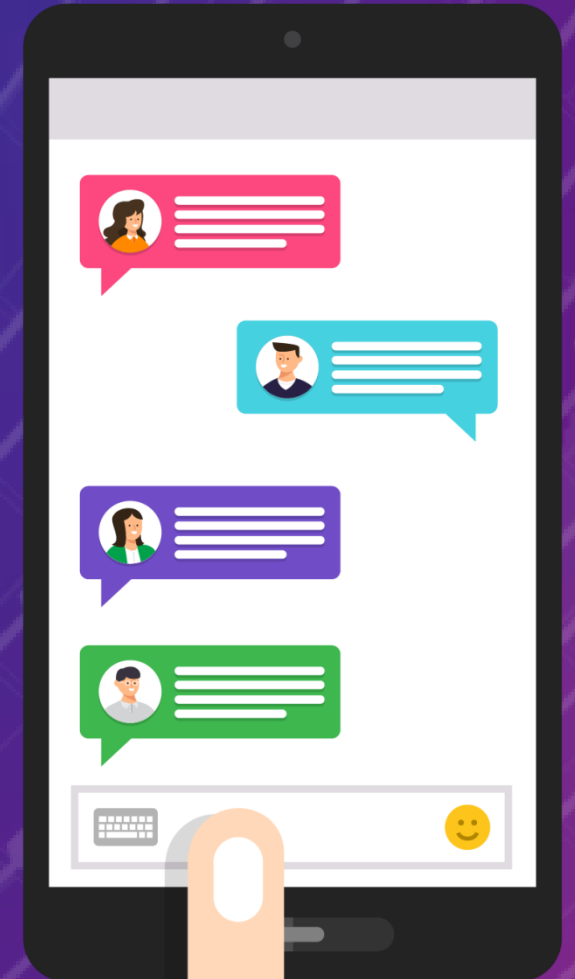
Неожиданное сообщение о крупном выигрыше, который можно получить после оплаты комиссии, тоже должно вызывать подозрение.



# Не верьте всему, что пишут в сообщениях

«Пополнял счёт и ошибся номером, верните, пожалуйста, деньги»

Если вы получили такое сообщение,  
расскажите об этом родителям.



**БЕЗОПАСНОСТЬ**



**В СЕТИ ИНТЕРНЕТ**



**СПАСИБО ЗА ВНИМАНИЕ!**