

## Преступления цифрового века:

**КИБЕРБУЛЛИНГ  
ТРОЛЛИНГ  
ФИШИНГ**

### *Как обезопасить себя в сети?*

*Помни, если тебе или  
твоим знакомым  
угрожают, то об этом  
обязательно нужно  
рассказать взрослым.*

- ⇒ К 4-6 годам у 54% детей есть свой девайс.
- ⇒ Доля детей, которые не могут обойтись без смартфонов составляет 85%. Несколько лет подряд.
- ⇒ У 46% детей в начальной школе есть свой аккаунт в социальных сетях.  
В основной школе этот показатель доходит до 95%.

Буклет подготовлен учителем информатики Тополевой Н.И.  
по материалам энциклопедии «[wikipedia.org](http://wikipedia.org)» и данным  
«Лаборатории Касперского».

## ПАМЯТКА – БУКЛЕТ

### «Уроки безопасности в сети Интернет»



## КИБЕРБУЛЛИНГ

**Кибертравля** — намеренные оскорбления, угрозы, диффамации и сообщение другим компрометирующих данных с помощью современных средств коммуникации, как правило, в течение продолжительного периода времени.

Дети, которые стали жертвами Интернет-травли, как правило, подвергались ей и в реальной жизни.

Наиболее частыми жертвами становятся дети в возрасте 11-16 лет. В этот период подростки наиболее чувствительные и закомплексованные.

### Что делать?

1. **Будьте на связи со старшими в соцсетях. Общие чаты, семейные и классные группы.**
2. **Помоги младшему братику или сестренке настроить аккаунт в социальной сети так, чтобы посторонние люди не могли писать малышам.**

Неизвестные люди мечтают украсть твоё хорошее настроение, аккаунты, виртуальные деньги и др.? Эта памятка для тебя!

## ФИШИНГ

**Фишинг** — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с ошибкой в адресе.

После того как пользователь попадает на поддельную страницу, мошенники пытаются побудить его ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Фишинг — одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности: в частности.

### Что делать?

**Обращайте внимание на адрес и наличие замочка слева в адресной строке, чтобы распознать сайт-подделку.**

## ТРОЛЛИНГ

**Троллинг** — форма социальной провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже

Основными местами осуществления троллинга могут выступать различные тематические форумы, конференции, социальные сети, порталы, чаты и новостные сайты.

### Что делать?

1. **Расскажите младшим о возможностях соцсетей по блокировке пользователей (о кнопке «Пожаловаться»).**
2. **Научитесь распознавать «троллей» и не реагировать на их сообщения. Блокируйте таких пользователей, удаляйте из друзей.**