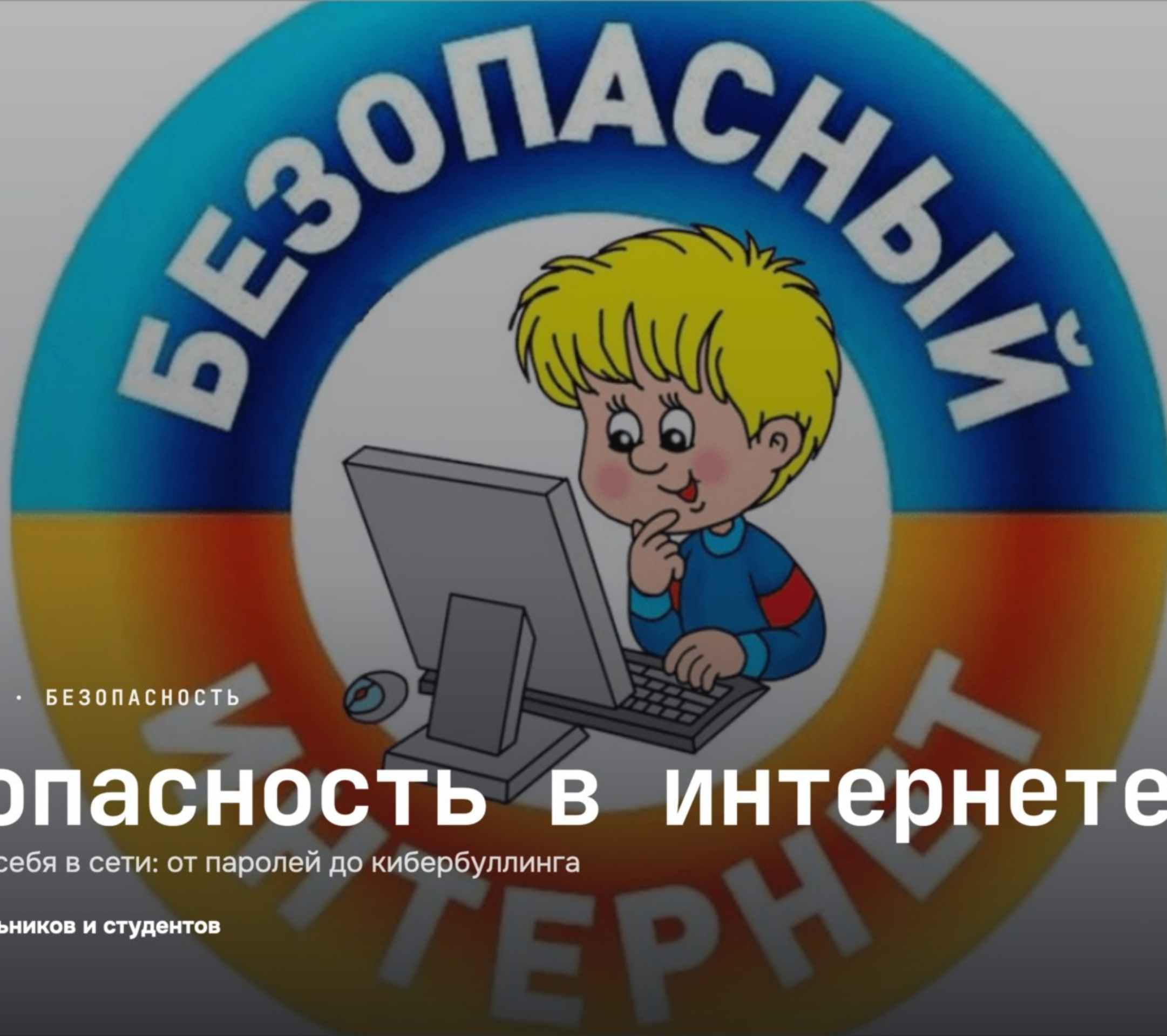




КЛАССНЫЙ ЧАС • БЕЗОПАСНОСТЬ

Безопасность в интернете

Как защитить себя в сети: от паролей до кибербуллинга

Доклад для школьников и студентов

Какие угрозы есть в сети

01

Вредоносные программы

Вирусы, трояны и шпионское ПО могут украсть данные, повредить устройство или следить за вами.

02

Фишинг

Поддельные сайты и письма, маскирующиеся под официальные, чтобы выманить пароли и личную информацию.

03

Кибербуллинг

Травля, оскорбления и угрозы в соцсетях и мессенджерах — серьёзная проблема среди подростков.

04

Мошенничество

Звонки от «банков», предложения лёгкого заработка и другие уловки для кражи денег.

05

Утечка данных

Раскрытие персональной информации (адрес, фото, пароли) без вашего ведома — потеря приватности.

Статистика кибермошенничества в цифрах

\$10,5 трлн

Глобальный ущерб от киберпреступности

Прогноз Cybersecurity Ventures на 2025 год

69%

Кибербуллинг среди школьников (Россия)

Рост на 14% в 2025 г. (данные ВЦИОМ)

Надёжные пароли: правила безопасности

- ◆ **Длина и сложность** Используйте не менее 12 символов: буквы разного регистра, цифры, спецсимволы.
- ◆ **Уникальность паролей** Никогда не используйте один и тот же пароль для разных сайтов и сервисов.
- ◆ **Менеджер паролей** Доверьте запоминание паролей специальным приложениям — это безопасно и удобно.
- ◆ **Никому не сообщайте пароль** Даже друзьям: многие взломы происходят из-за небрежности.

Помните: надёжный пароль — залог вашей безопасности в сети

Защита персональных данных

01

Что такое персональные данные

Информация, позволяющая идентифицировать человека: имя, адрес, телефон, фото, паспорт.

02

Не делитесь лишним

Не публикуйте в соцсетях свой адрес, номер телефона, паспортные данные и другую личную информацию.

03

Настройте приватность

Проверьте настройки конфиденциальности в соцсетях и мессенджерах: ограничьте доступ к вашим данным.

04

Осторожно: запросы!

Не отвечайте на подозрительные сообщения, просьбы прислать пароль, код или фото документов.

Как проявляется кибербуллинг



Не соглашайтесь на встречи с незнакомцами, не отправляйте личные фото — это снизит риск.

Мошеннические схемы и как их распознать



Фишинг

Поддельные письма от банков. Просят ввести данные по ссылке.
Признак: срочность и необычный адрес.



Фальшивые магазины

Товары по низким ценам, требуют предоплату. После оплаты сайт исчезает. Проверяйте отзывы и адрес.



Лотереи и выигрыши

Сообщают о выигрыше, просят перевести налог. Помните:
бесплатный сыр — в мышеловке.



Звонки из банка

Якобы из службы безопасности банка. Просят назвать код из СМС.
Перезвоните в банк сами.

Правила безопасного поведения в сети



Используй антивирус

Установи защитное ПО на все устройства и регулярно обновляй его для предотвращения заражения вирусами.



Обновляй программы

Своевременно устанавливай обновления операционной системы и приложений — они закрывают уязвимости.



Проверяй ссылки перед кликом

Перед переходом проверяй адрес ссылки, особенно в письмах и сообщениях от незнакомцев.



Не скачивай сомнительные файлы

Загружай файлы только с официальных сайтов и доверенных платформ, избегая торрентов и сомнительных ресурсов.



Включи двухфакторный вход

Добавь дополнительный уровень защиты к своим аккаунтам — это сильно усложнит взлом.

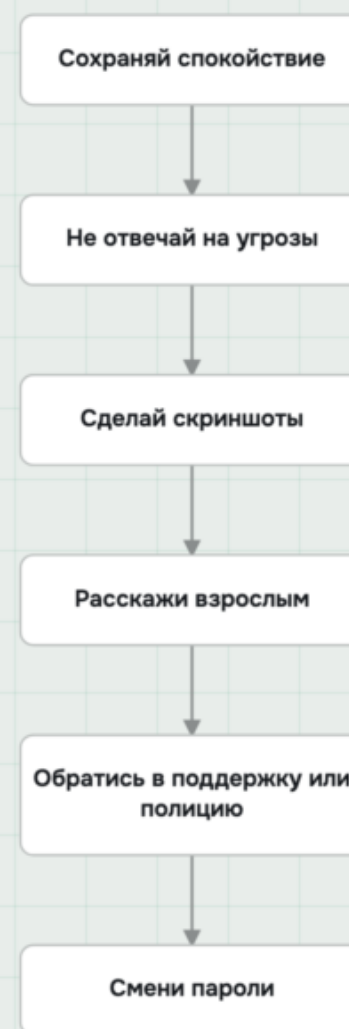


Не сообщай данные незнакомцам

Никому не передавай пароли, номера карт, адреса и другую личную информацию в сети.

ИНСТРУКЦИЯ

Что делать, если столкнулся с угрозой в интернете



Запомни: всегда обращай за помощью к взрослым!

Памятка-чеклист: 5 шагов к безопасности

01

Используй надёжные пароли

Создавай пароли длиной не менее 12 символов из букв, цифр и символов. Не используй одинаковые пароли для разных сервисов.

02

Не делись личной информацией

Не сообщай в сети адрес, телефон, номер школы, фото документов. Личные данные — твоя главная ценность.

03

Проверяй ссылки

Перед переходом наводи курсор и смотри настоящий адрес. Не кликай на подозрительные ссылки — они могут вести на фишинг.

04

Обновляй ПО

Регулярно обновляй операционную систему, браузер и антивирус — это закрывает уязвимости, которыми пользуются хакеры.

05

Сообщай о подозрительном

Если кто-то угрожает, просит деньги или присылает странные ссылки — сразу скажи родителям или учителю. Не пытайся разобраться сам.

ИТОГ

Будьте в безопасности!

Помните главные правила: не делитесь личными данными, используйте сложные пароли, не общайтесь с незнакомцами. Ваша безопасность в ваших руках!

ТЕЛЕФОН ДОВЕРИЯ

8-800-2000-122