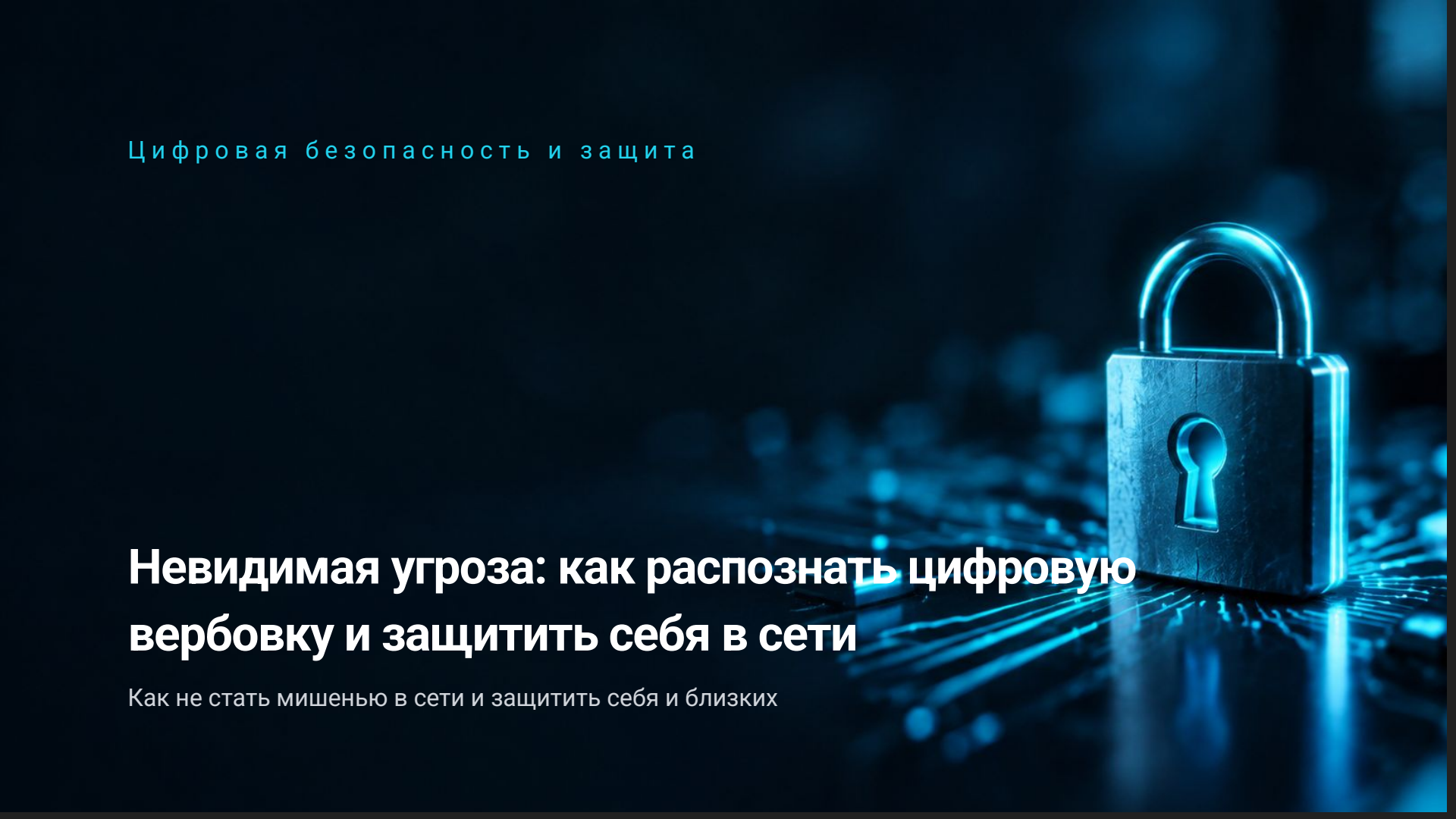
Цифровая безопасность и защита



Невидимая угроза: как распознать цифровую вербовку и защитить себя в сети

Как не стать мишенью в сети и защитить себя и близких

Интернет — главное пространство, где нас ищут

Социальные сети, мессенджеры и онлайн-игры стали основным полем для скрытого воздействия на молодежь.

Основные каналы: Соцсети, мессенджеры и онлайн-игры — ключевые пространства ежедневного общения молодежи.

Удаленная атака: Вербовщикам не нужно выходить из дома, чтобы найти и вовлечь жертву.

Незаметность угрозы: Полная анонимность в сети и искусственно сформированное доверие к «своим» делают любые атаки не

Цифровая безопасность

Нейросети, дипфейки и фейковые аккаунты

Современные технологии позволяют создавать убедительные подделки для обмана пользователей.

- **Нейросети**

  Генерируют тексты, полностью неотличимые от живого, эмоционального человеческого общения.
- **Дипфейки**

  Подделывают голос и видеозаписи знакомых, друзей или «авторитетных» лидеров мнения.
- **Фейковые аккаунты**

  Обладают тщательно проработанной «идеальной» историей, выглядя как реальные люди.

Главное правило

Всегда проверяйте реальное поведение и поступки собеседника, а не красивую цифровую картинку.

Психологическая обработка

Как начинается общение: четыре типичных крючка

Суть стратегии

Вербовка начинается с психологической обработки через комплименты, ложные перспективы и эксплуатацию уязвимостей.

Воронка воздействия

От этапа внимания через доверие и выгоду к полной изоляции жертвы.

01

Внимание

Обильные комплименты и демонстрация «особого» понимания.

02

Доверие

Постепенное сближение и стирание личных границ.

03

Выгода

Заманчивые предложения лёгкого заработка за простые действия.

04

Изоляция

Игра на одиночестве, чувстве несправедливости и отчуждение от близких.

Информационная безопасность

Красные флаги в переписке: когда пора насторожиться

Четкие индикаторы в переписке, указывающие на попытку манипуляции и вербовки.

Секретность

Прямые просьбы хранить общение в секрете от родителей, друзей и близких.

Лёгкие деньги

Предложения быстрого и крупного заработка за минимальные усилия.

Закрытые контуры

Настойчивый перевод общения в зашифрованные или закрытые чаты.

Личные данные

Требования отправить интимные фото, видео или конфиденциальные личные данные.

Инструкция безопасности

Что делать, если вас или друга пытаются вовлечь

Главный принцип

Соблюдение четкого алгоритма безопасности помогает пресечь угрозу на раннем этапе.

01

Стоп-реакция

Категорически не отвечать на подозрительные сообщения, не переводить деньги и не отправлять личные данные.

02

Фиксация

Сделать цифровые следы улик — скриншоты переписок, ссылки, никнеймы и точное время.

03

Блокировка

Заблокировать злоумышленника, пожаловаться на аккаунт в системе.

04

Огласка

Незамедлительно рассказать родителям, учителям или взрослым, которым доверяете. Главное — не молчать!

Информационная безопасностьБезопасная среда

Цифровая гигиена — это личная безопасность

112

Единый номер экстренных служб: **112**

☎

Детский телефон доверия:

8-800-2000-122

бесплатно, круглосуточно

✦

Школьный психолог или классный руководитель