

Словарь интернет угроз

- **Фишинг.** Атаки, при которых мошенники выдают себя за надежные организации, чтобы выманить у пользователей конфиденциальные данные (логины, пароли, банковские данные).
- **Вредоносное ПО.** Программы (вирусы, черви, трояны, программы-вымогатели), которые наносят вред устройству, шифруют данные или крадут информацию.
- **Социальная инженерия:** Манипулирование пользователями с целью получения от них доступа к информации или системам.
- **DDoS-атаки.** Атаки, направленные на отказ в обслуживании, когда злоумышленники перегружают серверы огромным количеством запросов, делая сервис недоступным.
- **Кибермошенничество.** Различные виды мошенничества в сети, включая мошеннические сайты, поддельные аккаунты и фишинговые рассылки.
- **Кража данных.** Умышленные действия, направленные на получение доступа к конфиденциальной информации пользователя или организации.
- **Кибербуллинг.** Травля и оскорбления в интернете, которые могут нанести психологический вред жертве.



На ресурсе **kids.pomogut.by** вы узнаете, как противостоять кибербуллингу, как распознать мошенников, защитить личные данные: есть адаптированная информация как для детей и подростков, так и для родителей и учителей.

Если вы уже столкнулись с угрозой или насилием, всегда можно написать об этом специалистам в онлайн-чат на сайте или позвонить по телефонам, указанным ниже.

Эксперты дадут совет и поддержат.



Никакая проблема не является слишком большой или слишком маленькой. Мы здесь для вас. Звонок анонимный 24/7!

8 801 100 16 11 *звонок бесплатный

8 (029) 367 32 32 *согласно тарифу оператора

Государственное учреждение образования
«Средняя школа №9 г.Мозыря»



**«10 правил безопасности
для детей в сети
Интернет»**

Мозырь, 2025

Правила безопасного использования сети Интернет



Не делитесь личной информацией: Не публикуйте свой адрес, номер телефона, домашний адрес, фотографии или видео без разрешения

родителей.

Будьте осторожны с незнакомцами:

Виртуальные знакомые могут не быть теми, за кого себя выдают. Не встречайтесь с незнакомцами из Интернета в реальной жизни без родителей.



Не открывайте неизвестные файлы: Не открывайте файлы из писем от незнакомых людей, так как они могут содержать вирусы или "агрессивный" контент.

Думайте, прежде чем писать: Вежливое и

уважительное общение в сети важно. Прежде чем что-то опубликовать, подумайте, не навредит ли это вам или другим.



Не отвечайте на спам: Игнорируйте нежелательные электронные письма и сообщения.

Не используйте веб-камеру для общения с незнакомцами:

Используйте веб-камеру только для общения с проверенными друзьями.



Рассказывайте взрослым о проблемах: Если кто-то в Интернете обидел вас или заставил почувствовать себя некомфортно, обязательно расскажите родителям или учителю.

Проверяйте сайты на безопасность: Используйте надежные антивирусные программы и проверяйте сайты на безопасность перед использованием.



Не указывайте месторасположение:

Будьте осторожны с приложениями и функциями, которые могут раскрывать ваше местоположение.

Меняйте пароли: Регулярно меняйте пароли от своих аккаунтов и не используйте простые пароли, которые легко угадать.

