



ВОЛГО-ДОНСКАЯ ТРАНСПОРТНАЯ ПРОКУРАТУРА

Основные угрозы личной безопасности в Интернете



Фишинг

Сообщения электронной почты, отправленные преступниками, чтобы обманом вынудить вас посетить поддельные веб-узлы и предоставить личные сведения

Мистификация

Сообщения электронной почты, отправленные, чтобы обманом вынудить пользователя отдать деньги



Кража идентификационных сведений

Преступление, связанное с похищением личных сведений и получением доступа к наличным деньгам или кредиту

Нежелательная почта

Нежелательные сообщения электронной почты, мгновенные сообщения и другие виды коммуникации



Основные угрозы безопасности компьютера



Вирусы и программы-черви

Программы, проникающие в компьютер для копирования, повреждения или уничтожения данных

Программы-трояны

Вирусы, имитирующие полезные программы для уничтожения данных, повреждения компьютера и похищения личных сведений



Программы-шпионы

Программы, отслеживающие ваши действия в Интернете или отображающие навязчивую рекламу

Защита. Необходимо защищать компьютеры при помощи современных технологий подобно тому, как мы защищаем двери в наших домах.

Безопасность. Наше поведение должно защищать от опасностей Интернета.

Основные угрозы безопасности детей в Интернете



Кибербуллинг

И дети, и взрослые могут использовать Интернет, чтобы изводить или запугивать других людей

Злоупотребление общим доступом к файлам

Несанкционированный обмен музыкой, видео и другими файлами может быть незаконным или повлечь загрузку вредоносных программ



грамм

Неприличный контент

Если дети используют Интернет без присмотра, они могут столкнуться с изображениями или информацией, от которой их желательно оградить



Хищники

Эти люди используют Интернет для того, чтобы заманить детей на личную встречу



Вторжение в частную жизнь

Заполняя различные формы в Интернете, дети могут оставить конфиденциальные сведения о себе или своей семье



Основные правила для школьников

Вы должны это знать:

- ✓ Всегда спрашивайте родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.
- ✓ Прежде чем начать дружить с кем-то в Интернете, спросите у родителей как безопасно общаться.
- ✓ Никогда не рассказывайте о себе незнакомым людям. Где вы живете, в какой школе учитесь, номер телефона должны знать только ваши друзья и семья.
- ✓ Не отправляйте фотографии людям, которых вы не знаете. Не надо чтобы незнакомые люди видели фотографии Вас, Ваших друзей или Вашей семьи.
- ✓ Не встречайтесь без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.
- ✓ Общаясь в Интернете, будьте дружелюбны с другими. Не пишите грубых слов, читать грубости так же неприятно, как и слышать. Вы можете нечаянно обидеть человека.
- ✓ Если вас кто-то расстроил или обидел, обязательно расскажите родителям.



Дорогой друг!



Интернет во многом похож на реальную жизнь.

Находить что-то новое, общаться с друзьями, возможно, заводить новые знакомства – здорово и интересно.

Но, как и в реальной жизни, в Интернете

нужно соблюдать простые правила безопасности.



Основные советы по безопасности в социальных сетях:

Ограничьте список друзей. У тебя в друзьях

не должно быть случайных и незнакомых людей;

- Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
- Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
- Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
- Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
- При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8
- Для социальной сети, почты и других сайтов необходимо использовать разные пароли.

