


ТВОЯ БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ.

(ПАМЯТКА ДЛЯ УЧАЩЕГОСЯ)




Интернет – мир широких возможностей. Он позволяет нам

	<ul style="list-style-type: none">✚ общаться с друзьями и семьёй;✚ получать доступ к информации и развлечениям;✚ учиться, встречаться с людьми, узнавать новое.
---	---






Чтобы делать всё это без последствий, нужна специальная защита.

Современные технологии защищают наши компьютеры так, как это делает дверной замок в квартире. Но наше поведение тоже должно защищать нас. Как? От кого и чего? Зачем?





Основные угрозы безопасности компьютера:

	<p>Вирусы и программы-черви. Проникают в компьютер для копирования, повреждения или уничтожения данных.</p>
	<p>Программы-трояны. Имитируют полезные программы для уничтожения данных, повреждения компьютера, похищения личных сведений.</p>
	<p>Программы-шпионы. Отслеживают твои действия в Интернете, транслируют навязчивую рекламу.</p>

Основные угрозы твоей безопасности в Интернете:

	Киберхулиганы. 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 заражение вредоносными программами.
	Неприличный контент. Если ты используешь компьютер с доступом к сети без присмотра взрослых, ты можешь столкнуться с информацией неприличного содержания.
	Хищники. Преступники. Эти люди могут использовать Интернет для того, чтобы заманить тебя на личную встречу.
	Вторжение в частную жизнь. Заполняя различные формы регистрации, ты можешь выдать личные, конфиденциальные сведения о себе и своей семье.

Что может подстергать тебя и твоих близких в Интернете? Виртуальные угрозы иногда бывают реальными.

	Фишинг. Сообщения электронной почты, отправленные преступниками, чтобы обманом вынудить пользователя посетить поддельные сайты и предоставить там личные сведения (логин, пароль).
	Кража идентификационных сведений. Преступление, связанное с похищением личных сведений и получением доступа к наличным деньгам или кредиту.
	Нежелательная почта. Нежелательные, часто рекламные сообщения электронной почты, служб мгновенных сообщений и других видов коммуникаций (спам).
	Мистификация. Сообщения электронной почты (часто – о крупном выигрыше), отправленные, чтобы обманом вынудить пользователя отдать деньги.

Что можно предпринять?

Твой компьютер:

- ✚ включить брандмауэр;
- ✚ использовать обновления операционной системы;
- ✚ загрузить и обновлять антивирусные программы.

Твоя семья:

- ✚ посоветуйся с родителями, узнай у них (или поясни им), какие вредоносные сайты и угрозы существуют в Интернете;
- ✚ держи личные сведения в секрете;
- ✚ используй настройки семейной безопасности.

Дополнительные способы защиты компьютера:

- ✚ архивируй данные своего компьютера;
- ✚ не ленись читать заявления о конфиденциальности на веб-узлах;
- ✚ закрывай всплывающие окна при помощи кнопки «X»;
- ✚ думай, прежде чем щёлкать по ссылке;
- ✚ не открывай подозрительные письма.

ПОМНИ ПРОСТЫЕ ПРАВИЛА:

Относись к другим так, как ты хочешь, чтобы относились к тебе.

Защищай себя.

Уважай собственность других людей.

Никогда не отправляйся в одиночку на личную встречу с «другом» из Интернета.

**Подготовила
Колесникова
Татьяна Владимировна,
МБУДО ДОО(сп)Ц**