4. Правила безопасного поведения в интернете

Теория:

Интернет — это потрясающий ресурс, который предоставляет огромное количество информации, образовательных материалов и возможностей для общения.

Однако при использовании **сети Интернет** необходимо соблюдать определённые правила безопасности, чтобы избежать негативных последствий.

1. Не доверяй свои личные данные незнакомым лицам. Никогда не сообщай пароли, номера кредитных карт, адреса и другую конфиденциальную информацию.
2. Будь осторожен при открывании вложений в письмах или сообщениях, особенно если они пришли от незнакомых отправителей. Вложения могут содержать вирусы.

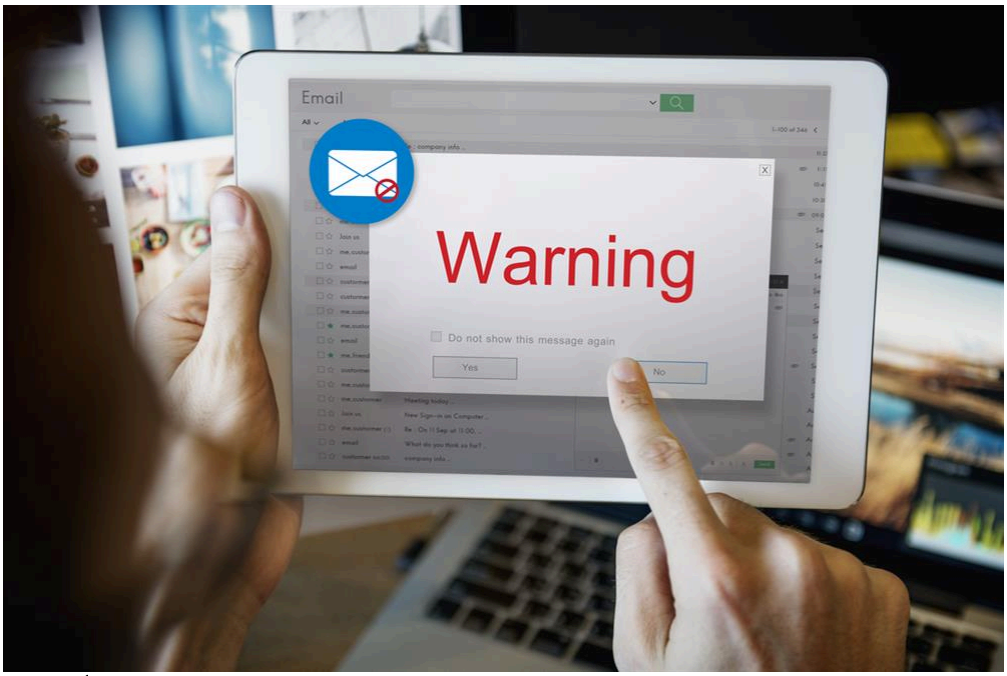

Рис. 1. Вирусные программы в письмах электронной почты

3. Используй сложные и уникальные пароли для своих аккаунтов.

Сложный пароль содержит заглавные и прописные символы, цифры и специальные символы. Старайся создавать пароли не менее 10–12 символов (можно и длиннее), избегай простые распространённые комбинации.

Рис. 2. Пример сложного пароля

4. Обращай внимание на защищённое соединение (**https**) при передаче конфиденциальной информации.

Протокол HTTPS (HyperText Transfer Protocol Secure) — это защищённая версия протокола HTTP, используемая для обеспечения безопасной передачи данных через интернет.

Протокол HTTPS помогает подтверждать подлинность веб-сайтов и защищает пользователя.

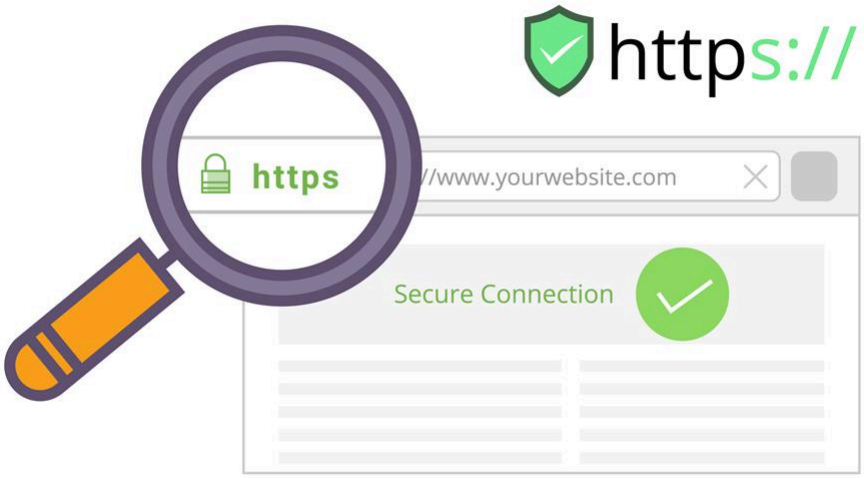

Рис. 3. Протокол HTTPS

5. Используй антивирусы для защиты от вредоносных программ.

Антивирусные программы — это специальные программы, предназначенные для защиты компьютера от вредоносных программ, для их обнаружения и удаления.

Необходимо регулярно обновлять антивирусное программное обеспечение и проводить сканирование компьютера, чтобы обеспечить его безопасность.

Обрати внимание!

Рекомендуется выполнять антивирусную проверку не реже одного раза в неделю для повышения защиты компьютера.

Вот некоторые примеры популярных антивирусных программ.

Значок	Характеристика

 *Рис. 4. Kaspersky Anti-Virus*	Kaspersky Anti-Virus — это надёжный и лёгкий в использовании антивирус, предлагающий защиту от вирусов, шпионских программ, фишинговых сайтов и других угроз. Разразработан компанией «Лаборатория Касперского», основанной российским программистом Е. В. Касперским.
 *Рис. 5. Avast Free Antivirus*	Avast Free Antivirus — это бесплатная антивирусная программа с хорошей репутацией и широким спектром функций для обеспечения безопасности компьютера
 *Рис. 6. Dr.Web Antivirus*	Dr.Web Antivirus — это антивирусная программа, которая предназначена для защиты устройств от вредоносных программ, вредоносных сайтов и других угроз безопасности
 *Рис. 7. Брандмауэр Windows*	Брандмауэр Windows — это встроенная антивирусная программа в операционной системе Windows, которая обеспечивает базовую защиту компьютера от вредоносных программ

Аутентификация — это процесс, который помогает убедиться, что человек является тем, за кого себя выдаёт.

Важно помнить, что аутентификация помогает защищать важные данные, такие как фотографии, сообщения или личные сведения.

Существует несколько видов аутентификации, каждый из которых имеет свои особенности и уровни защиты.

Первый вид — это **аутентификация по паролю**. Это самый распространённый метод, который требует от пользователя ввода уникального пароля для доступа к системе. Однако данный способ может быть уязвим для атак, если пароли недостаточно надёжны или используются повторно на различных платформах.

Второй вид — **биометрическая аутентификация**. Этот метод использует уникальные физические характеристики пользователя, такие как отпечатки пальцев, радужная оболочка глаза или черты лица. Хотя биометрическая аутентификация предлагает более высокий уровень безопасности, она требует специализированного оборудования и может вызывать опасения по поводу конфиденциальности данных.

Третий вид — **многослойная аутентификация**, или **многофакторная аутентификация** (MFA). Этот подход сочетает в себе два и более метода, например пароль и текстовое сообщение с кодом. Такой уровень защиты значительно уменьшает риски несанкционированного доступа и становится всё более популярным в современных системах.

Аутентификация, которая требует предоставления достоверной информации, является важным инструментом борьбы с таким явлением, как кибербуллинг.

Кибербуллинг — это когда кто-то обижает или унижает другого человека с помощью интернета. Подобное может происходить в социальных сетях, играх или чатах. Например, если кто-то пишет злые комментарии под фотографиями другого человека или отправляет угрозы в личных сообщениях, это и есть кибербуллинг.

Рис. 8. Кибербуллинг

Если ты стал свидетелем кибербуллинга или сам его переживаешь, важно не молчать. Расскажи об этом взрослым, которым доверяешь, будь то родители, учителя или друзья. Более подробную информацию о кибербуллинге и способам борьбы с ним можно найти в статье.