

2. Лента времени

“Visme”

История Интернета



3. Онлайн-доска

“Flip”

Правила безопасной работы в Интернете

Обновляйте операционную систему и приложения. Обновления содержат исправления уязвимостей, которые могут быть использованы злоумышленниками.

Обращайте внимание на настройки конфиденциальности. Настройте параметры конфиденциальности в социальных сетях и других сервисах, чтобы ограничить доступ к вашей информации.

Установите антивирусное программное обеспечение. Антивирус поможет обнаружить и удалить вирусы и другие вредоносные программы.

Избегайте общественных Wi-Fi сетей. В общественных местах используйте только защищенные сети, такие как VPN для HTTPS.

Не открывайте подозрительные письма и ссылки. Письма от неизвестных отправителей и подозрительные ссылки могут содержать вирусы или фишинг.

Будьте осторожны с личными данными. Не делитесь личной информацией, такой как адрес, номер телефона, паспортные данные и т.д., с неизвестными лицами. Проверьте сайты на надежность перед тем, как вводить свои данные.

Используйте сложные пароли. Пароль должен содержать буквы разного регистра, цифры и специальные символы. Регулярно меняйте пароли и не используйте один пароль для нескольких аккаунтов.

Включите двухфакторную аутентификацию. Это дополнительный уровень защиты, который требует подтверждения входа с помощью второго устройства или кода.

Источники информации

1. Официальные сайты государственных органов, таких как Роскомнадзор.

2. Сайты и блоги экспертов по кибербезопасности.

3. Специализированные ресурсы по защите персональных данных.

4. Рекомендации производителей программного обеспечения и оборудования.

4. Облако слов

“WordArt”



5. Инфографика

“Easelly”

