Вирусы

Описание: Это программы, которые могут заразить ваш компьютер и повредить файлы.

Контрмеры:
Установите антивирусное программное обеспечение и обновляйте его регулярно.
Не скачивайте файлы с ненадежных источников.
Постоянно обновляйте операционную систему и приложения.

Фишинг

Описание: Злоумышленники пытаются получить вашу личную информацию, представляясь как доверенные источники.

Контрмеры:
Будьте осторожными с электронными письмами и ссылками от незнакомых отправителей.
Проверьте адрес веб-сайта перед вводом личных данных.
Используйте антифишинговые расширения для браузера.

Социальная Инженерия

Описание: Злоумышленники могут использовать манипуляции и обман, чтобы получить доступ к вашей информации.

Контрмеры:
Не давайте личную информацию незнакомым людям в интернете.
Остерегайтесь запросов на восстановление паролей или секретных вопросов.
Проверяйте подлинность запросов на предоставление информации.

Утечка личных данных

Описание: Ваша личная информация может быть украдена или раскрыта без вашего согласия.

Контрмеры:
Используйте сложные и уникальные пароли для каждого аккаунта.
Шифруйте важные файлы и данные.
Периодически проверяйте политику конфиденциальности онлайн-сервисов.

Доступ к учетным данным

Описание: Злоумышленники могут попытаться получить доступ к вашим аккаунтам, используя ваши учетные данные.

Контрмеры:
Включите двухфакторную аутентификацию для аккаунтов.
Регулярно меняйте пароли и следуйте рекомендациям по безопасности паролей.
Мониторьте активность на своих аккаунтах и реагируйте на подозрительную активность.

Спам

Описание: Навязчивые и нежелательные сообщения и реклама, которые могут быть раздражающими и опасными.

Контрмеры:
Используйте фильтры спама в вашей электронной почте.
Не открывайте сообщения от незнакомых отправителей.
Не кликайте на подозрительные ссылки или приложения в сообщениях.

Онлайн-мошенничество

Описание: Злоумышленники могут пытаться обмануть вас с целью получения денег или личной информации.

Контрмеры:
Будьте осторожными с онлайн-покупками и предоставлением финансовой информации.
Проверяйте подлинность продавцов и веб-сайтов перед совершением покупок.
Не давайте свои финансовые данные незнакомцам в интернете.

Кибербуллинг

Описание: Злоумышленники могут наносить вред вашей репутации и моральному состоянию, используя интернет.

Контрмеры:
Не участвуйте в онлайн-конфликтах и не разжигайте споры.
Блокируйте и сообщайте о нежелательных контактах.
Обсуждайте с родителями или взрослыми случаи кибербуллинга.

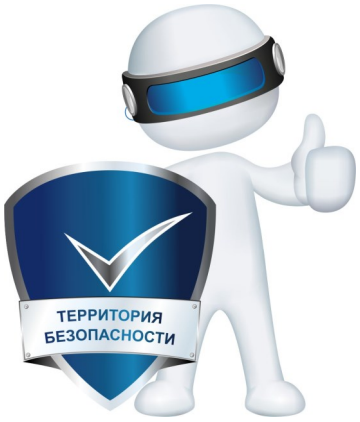
Недостаточная безопасность паролей

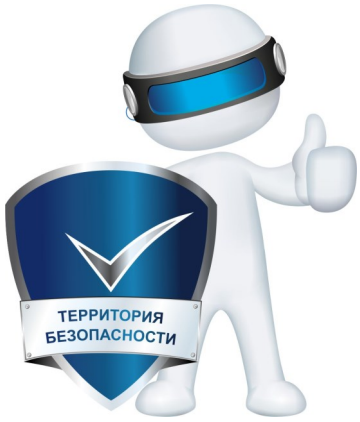
Описание: Использование слабых паролей и повторение их для разных аккаунтов может сделать вас уязвимыми.

Контрмеры:
Создавайте уникальные и сложные пароли для каждого аккаунта.
Используйте менеджеры паролей для хранения и управления вашими паролями.
Не передавайте пароли или не делитесь ими с другими людьми.

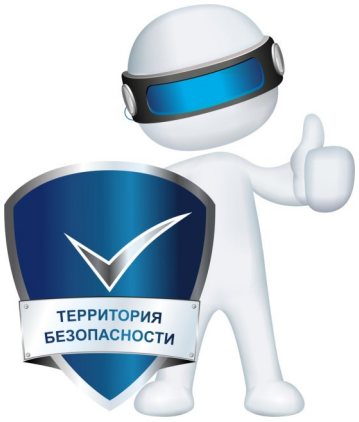
Поддельные новости **Описание**: Манипуляция информацией и распространение ложных новостей может привести к недовольству и панике. **Контрмеры**: Проверяйте достоверность источников новостей и информации. Обучайтесь критическому мышлению и анализу информации. Не распространяйте информацию, которую вы не проверили.	**Онлайн-гонения** **Описание**: Онлайн-гонения могут разрушить вашу приватность и безопасность, а также нарушить законы. **Контрмеры**: Не участвуйте в онлайн-гонениях и не поддерживайте их. Сообщайте об онлайн-гонениях в социальных сетях и интернет-сервисах. Защищайте свою личную информацию и аккаунты от злоумышленников.	**Нарушение Конфиденциальности** **Описание**: Незаконное доступ к чужим личным данным или коммуникациям. **Контрмеры**: Использование средств шифрования для личных сообщений. Защита устройства паролем или биометрией. Проверка правил конфиденциальности на вебсайтах и социальных сетях.
Физические атаки **Описание**: Попытки физически повредить или украсть устройства или данные. **Контрмеры**: Сохранение устройств в надежных местах. Использование защитных чехлов и замков. Внимательность при использовании общественных устройств.	**Кража учетных данных** **Описание**: Поиск и использование чужих учетных данных для несанкционированного доступа. **Контрмеры**: Использование уникальных паролей для каждого аккаунта. Двухфакторная аутентификация. Мониторинг активности на аккаунтах.	**Нарушение авторских прав** **Описание**: Использование чужого интеллектуального собственности без разрешения. **Контрмеры**: Соблюдение авторских прав при использовании контента. Проверка лицензий и разрешений.
Оскорбления и угрозы **Описание**: Нежелательные комментарии, угрозы или оскорбления в онлайн-среде. **Контрмеры**: Игнорирование и блокировка агрессивных пользователей. Сообщение о нарушениях администраторам платформы.	**Сетевые боты** **Описание**: Автоматизированные программы, которые могут использоваться для вредоносных целей. **Контрмеры**: Использование антивирусного ПО. Регулярное обновление программ и системы. Осторожность при скачивании и клике на неизвестные ссылки.	**Кража идентификационных данных** **Описание**: Поиск и использование чужих личных идентификационных данных. **Контрмеры**: Соблюдение осторожности при предоставлении личных данных онлайн. Использование средств шифрования при обмене конфиденциальными данными.

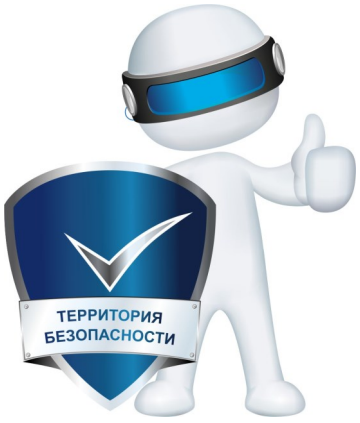
Файлы с вредоносным ПО **Описание**: Загрузка и запуск файлов, которые содержат вредоносные программы. **Контрмеры**: Не скачивать файлы с ненадежных источников. Использовать антивирусное ПО для сканирования скачанных файлов. Регулярное обновление антивирусных баз данных.	**Незащищенные Wi-Fi сети** **Описание**: Подключение к ненадежным и незащищенным Wi-Fi сетям, которые могут быть использованы для кражи данных. **Контрмеры**: Использование только защищенных сетей с паролем. Осторожность при подключении к общественным Wi-Fi сетям.	**Сбор информации о пользователе** **Описание**: Сбор личной информации о пользователях без их согласия. **Контрмеры**: Ограничение доступа к личной информации на социальных сетях. Проверка правил конфиденциальности на веб-сайтах и приложениях.
Кибершантаж **Описание**: Угрозы и попытки вымогательства в онлайн-среде. **Контрмеры**: Не отвечать на угрозы и не платить вымогателям. Сообщать о случаях кибершантажа в полицию или администрацию платформы.	**Распространение Дезинформации** **Описание**: Распространение ложных или вводящих в заблуждение сведений. **Контрмеры**: Проверка информации перед её распространением. Повышенная осведомленность о фейковых новостях и дезинформации.	**Неавторизованный Доступ** **Описание**: Попытки получить доступ к системам или данным без разрешения. **Контрмеры**: Использование сильных паролей и двухфакторной аутентификации. Постоянное обновление паролей.

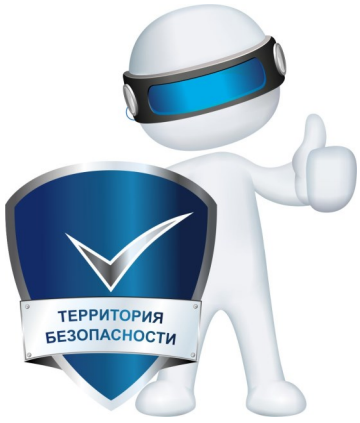

ТЕРРИТОРИЯ
БЕЗОПАСНОСТИ


ТЕРРИТОРИЯ
БЕЗОПАСНОСТИ

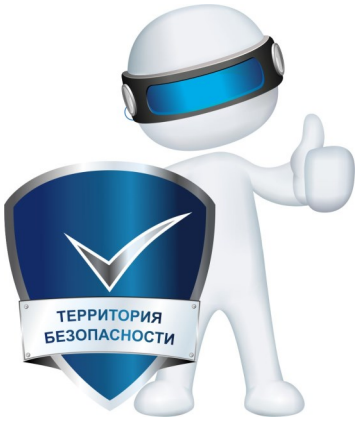
.

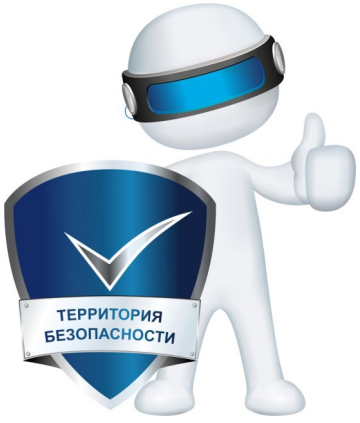

ТЕРРИТОРИЯ
БЕЗОПАСНОСТИ

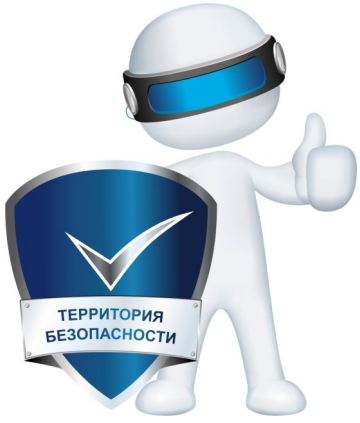

ТЕРРИТОРИЯ
БЕЗОПАСНОСТИ


ТЕРРИТОРИЯ
БЕЗОПАСНОСТИ

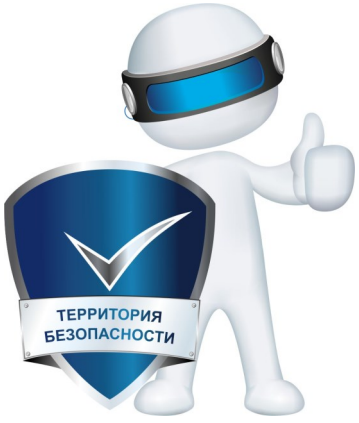
.


ТЕРРИТОРИЯ
БЕЗОПАСНОСТИ


ТЕРРИТОРИЯ
БЕЗОПАСНОСТИ


ТЕРРИТОРИЯ
БЕЗОПАСНОСТИ

.


ТЕРРИТОРИЯ
БЕЗОПАСНОСТИ