МОБИЛЬНАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА СМАРТФОНОВ — ОСНОВНЫЕ УГРОЗЫ МОБИЛЬНОМУ УСТРОЙСТВУ И СПОСОБЫ ИХ ПРЕДОТВРАЩЕНИЯ

Сычёв Владимир

ОЗНАКОМЛЕНИЕ

В презентации мы рассмотрим основные угрозы для мобильных устройств, включая вирусы, фишинговые атаки и кражу данных через публичные сети. Вы узнаете о методах защиты, таких как установка антивирусного ПО, настройка параметров конфиденциальности и использование VPN. Также мы поделимся практическими советами по защите вашего устройства.

ОСНОВНЫЕ УГРОЗЫ МОБИЛЬНЫМ УСТРОЙСТВАМ

- Мобильные устройства уязвимы для вирусов и вредоносного ПО, которые могут украсть личные данные или заблокировать устройство.
- Также существует риск фишинговых атак и мошенничества через поддельные приложения, которые могут получить доступ к конфиденциальной информации. Небезопасные публичные сети могут стать путём для злоумышленников, чтобы перехватить данные пользователя.

ВИРУСЫ И ВРЕДОНОСНЫЕ ПРОГРАММЫ

- Вирусы и вредоносные программы представляют серьёзную угрозу для смартфонов, так как могут украсть личные данные, заблокировать устройство или повредить его работу.
- Они могут попасть в систему через загрузки из ненадёжных источников или через уязвимости в системе безопасности.
- Регулярное обновление программного обеспечения и использование антивирусных приложений помогут минимизировать риски и защитить ваш смартфон.

ФИШИНГОВЫЕ АТАКИ

1 Фишинговые атаки — это вид мошенничества, при котором злоумышленники пытаются получить доступ к личным данным пользователей, маскируясь под доверенные источники.

2 Они могут приходить в виде подозрительных сообщений, ссылок или вложений в электронных письмах, а также через поддельные веб-сайты. Будьте бдительны и не предоставляйте личную информацию в ответ на неожиданные запросы.

КРАЖА ДАННЫХ ЧЕРЕЗ ПУБЛИЧНЫЕ СЕТ

Публичные сети Wi-Fi могут быть небезопасными, и злоумышленники используют их для кражи данных. Они могут перехватывать незашифрованные соединения и получать доступ к личной информации, такой как пароли и банковские данные. Поэтому важно использовать VPN и избегать ввода конфиденциальных данных в общественных местах.

МЕТОДЫ ЗАЩИТЫ СМАРТФОНОВ

1 Использование сложных паролей и двухфакторной аутентификации значительно повышает уровень защиты смартфона.

2 Регулярное обновление программного обеспечения закрывает уязвимости и предотвращает несанкционированный доступ.

3 Также важно установить антивирусное приложение для обнаружения и удаления вредоносных программ.

УСТАНОВКА АНТИВИРУСНОГО ПО

Антивирусное ПО помогает защитить смартфон от вредоносных программ и хакерских атак. Установка такого ПО — важный шаг для обеспечения безопасности вашего устройства. Выбирайте проверенные антивирусные программы и регулярно обновляйте их для максимальной защиты.

НАСТРОЙКА ПАРАМЕТРОВ КОНФИДЕНЦИАЛЬНОСТИ

Настройте параметры конфиденциальности в настройках вашего смартфона, чтобы защитить личные данные от несанкционированного доступа. Убедитесь, что приложения имеют минимальные необходимые разрешения, и регулярно обновляйте настройки безопасности для предотвращения утечек информации. Используйте встроенные функции блокировки экрана и шифрования данных для дополнительной защиты вашего устройства.

ИСПОЛЬЗОВАНИЕ VPN

- VPN помогает предотвратить перехват данных злоумышленниками и обеспечивает анонимность в интернете. Рекомендуется использовать проверенные сервисы VPN для максимальной защиты вашего мобильного устройства.

- VPN обеспечивает шифрование данных и скрывает ваш IP-адрес, что защищает личную информацию при использовании общественных Wi-Fi сетей. Использование

ПРАКТИЧЕСКИЕ СОВЕТЫ ПО ЗАЩИТЕ УСТРОЙСТВА

Регулярно обновляйте операционную систему и приложения, чтобы устранить уязвимости. Используйте сложные пароли и двухфакторную аутентификацию для повышения уровня защиты. Избегайте загрузки файлов из ненадёжных источников, чтобы не допустить установки вредоносного ПО.

СПАСИБО ЗА ВНИМАНИЕ!