



SEGURANÇA DA INFORMAÇÃO

DISPOSITIVOS MÓVEIS

SOBRE O QUE FALAREMOS?

- SEGURANÇA EM MOBILE
- BOAS PRÁTICAS
- CASOS REAIS
- LEIS RELACIONADAS
- PENALIZAÇÃO, LIMITES E 'PROBLEMAS'
- CONCLUSÃO

SEGURANÇA EM MOBILE?

1. CONCEITO

A segurança da informação em dispositivos móveis refere-se ao conjunto de práticas e tecnologias que protegem os dados armazenados, processados ou transmitidos por aparelhos como smartphones e tablets.

2. IMPORTÂNCIA DE DADOS PESSOAIS E EMPRESARIAIS

A proteção de dados nesses dispositivos é fundamental, pois eles armazenam desde fotos pessoais e senhas bancárias até documentos empresariais sensíveis.

3. PRINCIPAIS AMEAÇAS

Malware, Phishing, Vazamento de dados, engenharia social etc...

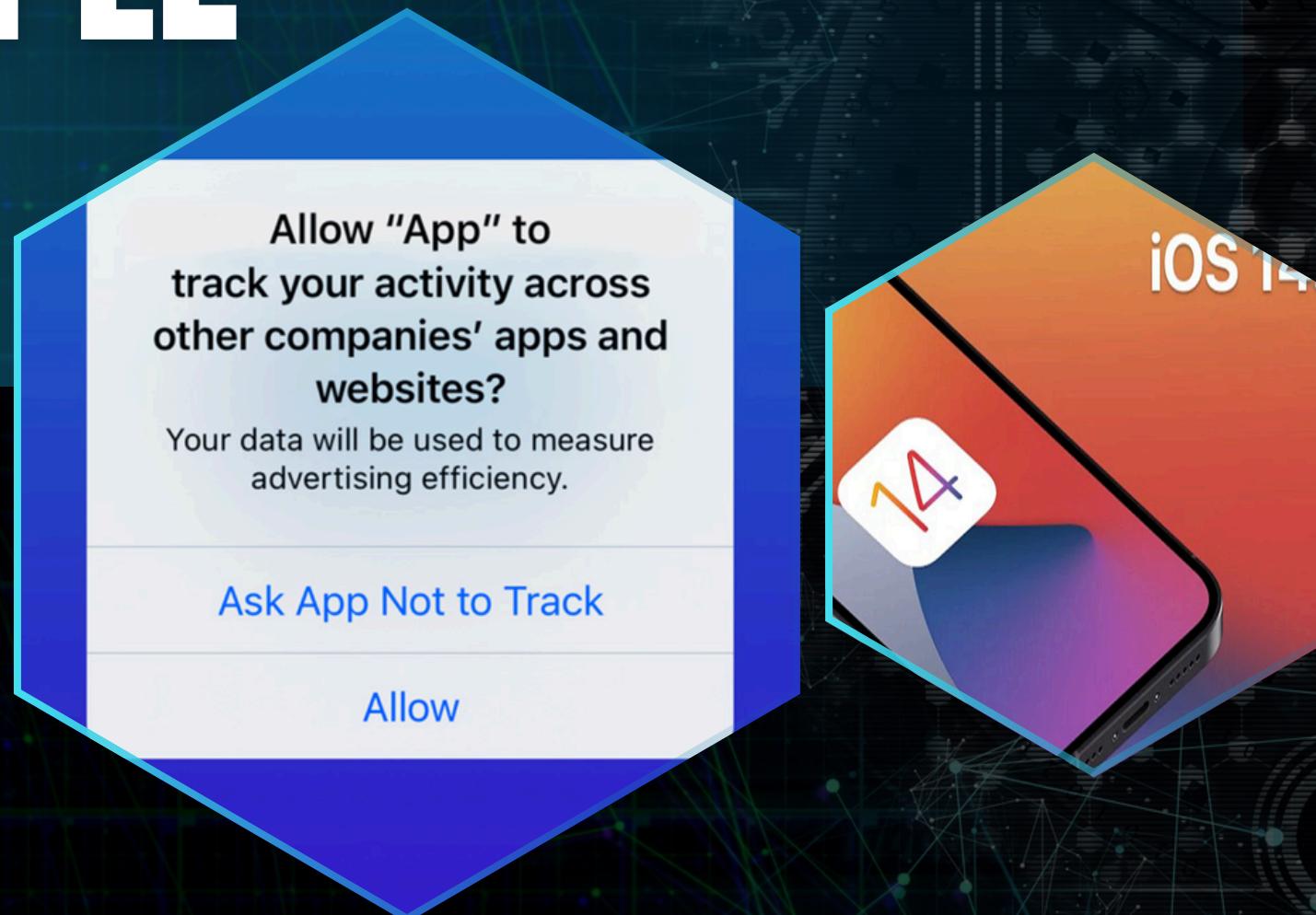


BOAS PRÁTICAS?



1. AUTENTICAÇÃO EM DOIS FATORES
2. USO DE SENHAS FORTES E ÚNICAS
3. ATUALIZAÇÃO CONSTANTE DO SISTEMA E APPS
4. USO DE ANTIVÍRUS CONFIÁVEL
5. EVITAR REDES WI-FI PÚBLICAS SEM VPN

IOS MELHORADO APPLE



1. QUANDO ACONTECEU?

O recurso App Tracking Transparency (ATT) foi implementado oficialmente no iOS 14.5, lançado em 26 de abril de 2021.

2. O QUE É O APP TRACKING TRANSPARENCY?

O ATT é uma funcionalidade que obriga os aplicativos a obterem consentimento do usuário para rastrear suas atividades em outros aplicativos e sites de terceiros.

3. IMPACTO E REPERCUSSÃO

A introdução do ATT foi amplamente elogiada por defensores da privacidade, pois aumentou a transparência e o controle dos usuários sobre seus dados. No entanto, empresas que dependem de publicidade direcionada, como o Facebook, criticaram a mudança, alegando que ela afetaria negativamente seus modelos de negócios baseados em anúncios personalizados.

VAZAMENTO DE DADOS FACEBOOK



- O que aconteceu com o Facebook em 2019?
- Como eles conseguiram os dados?
- Impacto nos dispositivos móveis
- Consequências para a empresa

LEIS RELACIONADAS



1. LGPD (BRASIL)

A Lei Geral de Proteção de Dados estabelece regras claras para o tratamento de dados pessoais no Brasil, abrangendo coleta, armazenamento, uso e compartilhamento dessas informações.



2. MARCO CIVIL DA INTERNET

Essa lei brasileira define direitos e deveres para o uso da internet, garantindo a privacidade e a segurança das comunicações online.



3. NORMAS ISO/IEC

As normas internacionais ISO/IEC 27001 e 27002 definem um conjunto de boas práticas e controles para a gestão da segurança da informação.

PENALIZAÇÃO, LIMITES E “PROBLEMAS”

Penalidades:

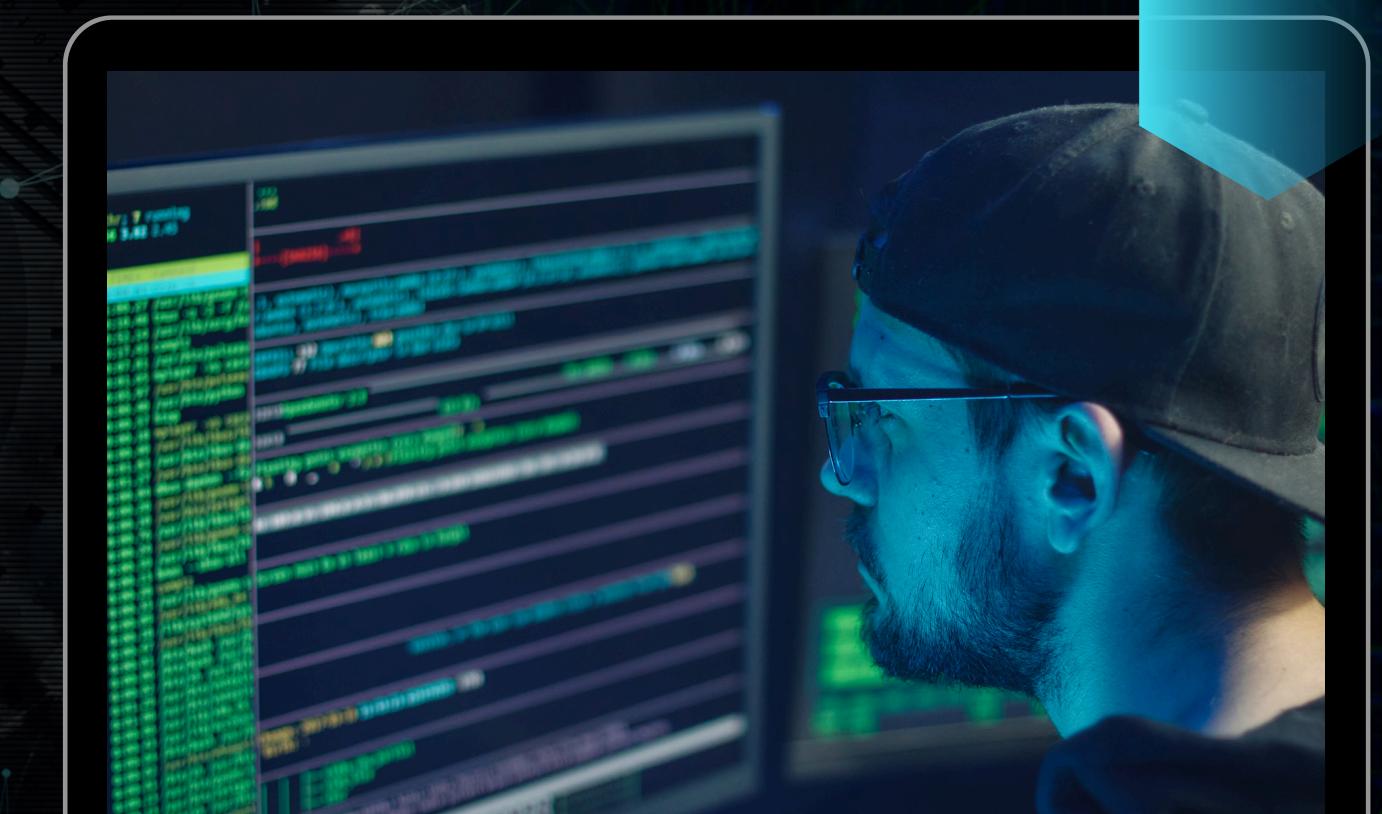
- Multas de até 2% do faturamento anual, limitadas a R\$ 50 milhões por infração.
- Possibilidade de suspensão de atividades de tratamento de dados.

Limites:

- Dificuldade em identificar responsáveis por ataques cibernéticos.
- Fiscalização ainda limitada, com estrutura da ANPD em desenvolvimento.

Críticas:

- Consentimento genérico permite coleta excessiva de dados.
- Multas brandas para grandes empresas podem não ser eficazes como punição.



CONCLUSÃO

A segurança da informação em dispositivos móveis é um desafio cada vez mais presente. Com tantos dados sensíveis nos nossos aparelhos, adotar boas práticas e exigir transparência no uso das informações é essencial. Avanços como o App Tracking Transparency da Apple mostram que a tecnologia pode proteger o usuário — mas falhas, como o vazamento de dados do Facebook, lembram que ainda há muito a melhorar.

Leis como a LGPD são um marco importante, mas sua força depende da aplicação efetiva e da postura ética das empresas. No fim, proteger os dados é uma responsabilidade compartilhada entre governos, empresas e usuários — e começa com escolhas conscientes no dia a dia.



MUITO OBRIGADO
ALGUMA PERGUNTA?