**Logotipo

Descrição gerada automaticamente**

Serviço Nacional de Aprendizagem Industrial

SENAI “Gaspar Ricardo Junior”

Curso

TÉCNICO EM DESENVOLVIMENTODE SISTEMAS

**Segurança em Dispositivos Móveis**

Isabele Agapito

Juliana Karla

Mateus Oliveira

Nícolas Oliveira

Leandro rosa

vedilson prado

Sorocaba

Abril – 2024

1. Introdução
2. Desenvolvimento
3. Tecnologias relacionadas
4. Ferramentas e soluções
   1. atualizações de software
   2. senhas fortes
   3. conexões Wi-Fi pública

4.4 antivírus

1. Conclusão

**1- Introdução**

A segurança em dispositivos móveis refere-se a práticas e medidas que procuram proteger os dados e a privacidade armazenados e transmitidos por dos dispositivos móveis. Isso inclui tanto a segurança dos dispositivos quanto a proteção contra ameaças virtuais, como malware e ataques cibernéticos.

**2- Desenvolvimento**

A segurança do dispositivo móvel é a proteção total dos dados nos dispositivos moveis e da rede conectada aos dispositivos. A segurança de dispositivos móveis se refere às medidas feitas para proteger informações armazenadas e transmitidas pelos dispositivos. Na fonte da segurança dos dispositivos está o objetivo de impedir que usuários não autorizados acessem a rede corporativa. A segurança dos dispositivos móveis é importante porque hoje mais da metade dos computadores corporativos são móveis. Além disso, a flexibilização do local de trabalho tem permitido aos funcionários a possibilidade de realizar tarefas por tablets ou smartphones, de onde estiverem. As possíveis ameaças aos dispositivos incluem aplicativos móveis maliciosos, golpes de phishing, vazamento de dados, spyware e redes Wi-Fi não seguras. Além disso, as empresas precisam levar em consideração a possibilidade de um funcionário perder um dispositivo móvel ou o dispositivo ser roubado.

**3- Tecnologias relacionadas**

Ao tomar as medidas básicas para proteger seu dispositivo, você pode ajudar a se proteger de várias ameaças. Uma das maneiras de garantir a segurança dos seu dispositivo são, os softwares antivírus.

Um antivírus é um programa usado para detectar, prevenir e remover um software malicioso, também conhecido como malware, de um dispositivo com o objetivo proteger o sistema contra vírus ou outros tipos de ameaças. Um software malicioso pode causar diversos tipos de prejuízos ao sistema, como danos ou roubo de informações. Isso varia de acordo com o vírus e objetivo do invasor.

Esses softwares funcionam escaneando o sistema em busca de arquivos ou atividades suspeitas e comparando-os com uma base de dados de assinaturas conhecidas de malware. Além disso, os antivírus geralmente incluem recursos adicionais de segurança, como proteção contra phishing, firewall e proteção de privacidade.

**4- Ferramentas e soluções**

Os ataques cibernéticos estão se tornando cada vez mais recorrentes, e as ameaças se tornaram mais avançadas, o que torna mais difícil proteger os dispositivos móveis contra eles. Hoje em dia, os celulares e tablets contêm muita informação pessoal e confidencial, o que torna essencial protegê-los contra os hackers.

**4.1- Atualize seu software regularmente**

Uma maneira de proteger seus dispositivos móveis contra-ataques cibernéticos é manter seus softwares atualizados. Muitas vezes, as atualizações de software arrumam falhas de segurança que poderiam ser usadas pelos hackers.

**4.2 - Use senhas fortes**

As senhas fortes são uma defesa importante contra-ataques cibernéticos. Lembre-se de utilizar senhas exclusivas para cada conta e dispositivo, e use senhas que contenham letras maiúsculas e minúsculas, números e símbolos. Além disso, evite usar senhas óbvias (data de nascimento ou nome de animal de estimação.)

**4.3- Evite conexões Wi-Fi públicas**

As conexões Wi-Fi públicas podem ser perigosas, pois os hackers podem interceptar seus dados pessoais e confidenciais enquanto você está conectado à rede. Portanto, evite fazer transações financeiras ou acessar informações confidenciais enquanto estiver conectado à rede Wi-Fi pública. Caso seja necessário usar Wi-Fi pública, lembre-se de usar uma VPN para proteger seus dados.

**4.4- Instale um antivírus**

Instalar um antivírus confiável em seu dispositivo é uma das maneiras mais eficaz de protegê-lo contra ameaças cibernéticas. Os antivírus detectam e removem malware e outras ameaças antes que elas possam causar danos ao seu dispositivo ou roubar suas informações pessoais.

**5- Conclusão**

A segurança em dispositivos móveis é uma necessidade cada vez mais. Com a evolução constante das tecnologias, surgem também novas ameaças cibernéticas que comprometem a integridade dos dados e a privacidade dos usuários.

A adoção de práticas seguras, como a atualização regular de softwares, a utilização de senhas fortes e o cuidado ao se conectar a redes Wi-Fi públicas, desempenham, uma função na segurança digital.

Porém, os softwares antivírus se destacam como uma ferramenta ótima para a segurança dos dispositivos, oferecendo não apenas a detecção e remoção de malware, mas também, proteção contra diversas ameaças cibernéticas.

Portanto, ao implementar as medidas de segurança correta, os usuários podem fortalecer a segurança de seus dispositivos móveis, protegendo assim seus dados e sua privacidade no ambiente digital.

Bibliografia

<https://www.cisco.com/c/pt_br/solutions/small-business/resource-center/security/mobile-device-security.html>

<https://4infra.com.br/seguranca-de-dados-em-dispositivos-moveis/>

<https://blog-pt.lac.tdsynnex.com/como-garantir-a-seguranca-em-dispositivos-moveis>

<https://www.kaspersky.com.br/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store>