Universidade São Judas Tadeu

Arthur Frederico Piasse Pereira – 824219186

Guilherme Pereira da Silva – 825129559

Jhonatan de lima Alves – 824215769

Matheus Fideles da Silva – 825144599

Sophia Grave Silva – 824213875

Thiago Carvalho Passos – 825117520

Sistemas Computacionais e Soluções

São Paulo

2025

Sistemas Computacionais e Segurança

Trabalho apresentado á

UC Sistemas Computacionais e Segurança do curso de T.I da Universidade São Judas Tadeu – Campus Mooca, como requisito parcial para a obtenção de nota.

Orientador: Prof. Robson Calvetti

São Paulo

2025

Resumo

A segurança digital é essencial no uso da internet, abrangendo práticas como atualizações automáticas de software, segurança em compras online, uso de VPNs, controle de privacidade nas redes sociais e cuidados ao utilizar redes Wi-Fi públicas. As atualizações automáticas garantem que sistemas e aplicativos recebam correções de segurança e melhorias, protegendo contra vulnerabilidades exploradas por cibercriminosos. A segurança em compras online envolve utilizar sites confiáveis, métodos de pagamento seguros e evitar redes públicas para transações sensíveis. As VPNs (Redes Privadas Virtuais) criam conexões criptografadas, oferecendo mais privacidade e proteção, especialmente em redes abertas. O controle de privacidade nas redes sociais ajuda a limitar o acesso a informações pessoais e evitar o compartilhamento excessivo de dados. Já o uso de Wi-Fi público para transações sensíveis representa riscos, sendo recomendável evitar esse tipo de atividade ou usar uma VPN para proteger os dados. Adotar essas práticas contribui para uma navegação mais segura e resguarda informações pessoais e financeiras.

Sumario

Tópicos a serem apresentados:

1. Atualizações Automáticas de Software;
2. Segurança em Compras Online;
3. VPN (Rede Privada Virtual);
4. Controle de Privacidade nas Redes Sociais;
5. Uso de Wifi Publico para Translações Sensíveis;

1. # Atualizações Automáticas de Software

Definição

As atualizações automáticas de software são processos que permitem que sistemas operacionais e aplicativos sejam corrigidos ou aprimorados sem a necessidade de ação manual do usuário. Esse recurso é fundamental para a segurança digital, pois garante que falhas e vulnerabilidades sejam corrigidas rapidamente, reduzindo o risco de ataques cibernéticos.

Explicação

A principal função das atualizações automáticas é manter os softwares protegidos contra novas ameaças. Quando uma falha de segurança é descoberta, desenvolvedores lançam rapidamente patches (correções) para impedir que hackers explorem essa vulnerabilidade. Sem essas atualizações, o sistema fica exposto a ataques, como invasões, roubo de dados e infecção por malwares.

Apesar de serem essenciais para a segurança, as atualizações automáticas também apresentam riscos. Algumas atualizações podem conter erros que causam instabilidade no sistema ou falhas de compatibilidade com outros softwares. Além disso, hackers podem explorar brechas no próprio processo de atualização, forçando a instalação de versões maliciosas. Por isso, é fundamental que as empresas adotem protocolos de verificação para garantir a autenticidade e confiabilidade das atualizações.

Exemplo Prático

Um caso real foi o ataque pelo malware NotPetya em 2017. Hackers exploraram uma atualização maliciosa de um software amplamente utilizado na Ucrânia, infectando milhares de computadores ao redor do mundo. O malware se espalhou rapidamente, causando prejuízos bilionários a empresas e governos. Esse exemplo mostra que, se

não houver um controle rigoroso sobre a origem e a segurança das atualizações automáticas, elas podem se tornar um risco ao invés de uma proteção.

Resoluções

Para garantir a segurança das atualizações automáticas, algumas medidas devem ser adotadas:

-Verificação de autenticidade: Sistemas devem validar se as atualizações vêm de fontes confiáveis antes de serem aplicadas.

-Testes antes da implementação: Empresas podem testar as atualizações antes de liberá-las para todos os dispositivos, evitando falhas inesperadas.

-Opção de adiamento: Permitir que os usuários escolham quando instalar atualizações pode prevenir problemas de compatibilidade ou erros críticos.

-Uso de redes seguras: Atualizações devem ser baixadas apenas em redes seguras, para evitar interceptação por hackers.

2. SEGURANÇA EM COMPRAS ONLINE

Definição

A segurança em compras online se trata a um conjunto de práticas, métodos e tecnologias com forte regularização, voltados a proteger os usuários de fraudes, golpes, roubos a dados pessoais e outros riscos associados a compras e vendas realizadas pela internet.

Explicação

Com o crescente avanço do consumismo online, a proteção aos usuários se tornou algo fundamental tanto para as empresas, quanto ao consumidor final. Proteger tais informações confidenciais, como dados pessoais, dados bancários e detalhes de cartões de credito e débito e credenciais de login. É de extrema importância prevenir práticas de fraudes e roubos de identidades, algumas medidas comuns incluem o uso da criptografia de dados, autenticação de dois fatores e certificados em segurança (SSL/TLS). Além disso, é importante para o usuário verificar a credibilidade dos vendedores e evitarem links maliciosos.

Exemplo prático

Um consumidor deseja comprar um notebook, porém decide entrar em um site desconhecido, pois dentro desse site este mesmo notebook está com um valor abaixo do valor de mercado. Antes de finalizar a compra, ele decide verificar a veracidade do site. Primeiro ele verifica se há algum certificado de segurança no site (um cadeado antes do endereço de link do site), procurou avaliações sobre outros consumidores que compraram o mesmo notebook e detectou diversas reclamações sobre aquele notebook, nas avaliações outros consumidores alegaram ser fraude pela falta da entrega do produto. Dessa maneira, ele evitou cair em uma possível fraude e optou por comprar em um site credenciado e verificado.

Resoluções

Para evitar que coisas desse tipo em compras online, existem alguns métodos que podem ser seguidas para prevenir ser afetado por alguma prática maliciosa:

- Utilizar métodos de pagamentos seguros para compras na internet, como cartões virtuais e carteiras digitais.
- Verificar se o site possui criptografia SSL/TLS.
- Verificar a reputação do vendedor em plataformas de avaliação de consumidores, como o reclame aqui por exemplo.
- Utilizar senhas fortes e autenticação de dois fatores.
- Verificar a veracidade dos links de lojas online recebidos tanto por e-mail, ou através das redes sociais.

Adotar essas práticas previnem significativamente o risco de cair em algum tipo de fraude ou roubo de dados, assim garantindo uma experiencia de compra mais tranquila para o usuário final.

3. # VPN (Rede Privada Virtual)

Definição

Uma VPN (Rede Privada Virtual) é uma ferramenta que ajuda a proteger sua conexão com a internet. Imagine que ela cria um "túnel" seguro entre o seu dispositivo e a rede, escondendo suas informações e mantendo tudo criptografado. Isso significa que, mesmo que alguém tente espionar o que você está fazendo online, não conseguirá entender nada, porque os dados estão protegidos.

Explicação

Como isso funciona?

1. Criptografia: Tudo o que você envia ou recebe pela internet passa por um processo de codificação, como se fosse um código secreto que só você e a VPN conseguem decifrar.

2. Túnel seguro: A VPN cria uma rota protegida entre você e um servidor remoto, impedindo que hackers ou curiosos acessem suas informações.

3. IP mascarado: Seu endereço IP real (uma espécie de "identificação" na internet) é escondido e substituído pelo IP do servidor VPN, dificultando que alguém descubra sua localização ou identidade.

Para que serve?

- Proteção em redes públicas: Se você usa Wi-Fi em aeroportos, cafés ou shoppings, a VPN ajuda a evitar que suas senhas ou dados sejam roubados.

- Acesso a conteúdo bloqueado: Com uma VPN, você pode acessar sites ou serviços que estão restritos em certos países.

- Privacidade: Ela impede que provedores de internet ou anunciantes rastreiem o que você faz online.

- Trabalho remoto: Muitas empresas usam VPNs para permitir que funcionários acessem arquivos e sistemas internos de forma segura, mesmo de casa.

Exemplo Pratico

Exemplo do dia a dia:

Imagine que você está em um hotel e precisa usar o Wi-Fi para fazer uma transferência bancária. Sem uma VPN, suas informações financeiras poderiam ser interceptadas por alguém mal-intencionado. Com a VPN, tudo fica criptografado, e você pode fazer isso com muito mais tranquilidade.

Resumo

Resumindo, uma VPN é como um escudo digital que protege sua privacidade e segurança na internet, especialmente quando você está conectado a redes que não são totalmente confiáveis.

4. # Controle de Privacidade nas Redes Sociais

Definição:

O controle de privacidade nas redes sociais refere-se ao conjunto de configurações e práticas que permitem aos usuários gerenciar quem pode acessar suas informações pessoais, postagens e interações dentro dessas plataformas.

Explicação:

Com o aumento da presença digital, garantir a privacidade online tornou-se essencial para proteger dados sensíveis, evitar exposição indesejada e reduzir riscos como golpes e vazamento de informações. As redes sociais oferecem opções de privacidade que permitem restringir o acesso ao perfil, ocultar publicações de certos usuários e impedir que terceiros utilizem dados pessoais para publicidade direcionada.

Exemplo Prático:

No Facebook, um usuário pode configurar suas postagens para serem vistas apenas por amigos, ocultando-as do público em geral. Além disso, a plataforma permite bloquear determinados perfis ou restringir o compartilhamento de informações, garantindo maior controle sobre quem pode interagir com suas publicações.

Resoluções:

Para manter a privacidade nas redes sociais, algumas práticas recomendadas incluem:

- Revisar e atualizar configurações de privacidade regularmente.
- Evitar compartilhar dados sensíveis, como endereço e número de telefone.
- Utilizar autenticação em dois fatores para aumentar a segurança da conta.

Manter um bom controle de privacidade é essencial para uma experiência segura nas redes sociais, garantindo que apenas as pessoas certas tenham acesso às informações compartilhadas.

5. # O Uso de Wi-Fi Público para Transações Sensíveis

Definição:

Se conectar em redes Wi-fi desconhecidas ou públicas para realizar compras online, acessar contas de banco e contas com dados pessoais, pode ser um risco para as suas informações. Essas redes geralmente são encontradas em restaurantes, padarias, aeroportos, sendo menos seguras que as redes privadas.

Explicação:

Ao se conectar em uma rede pública, as suas informações podem estar vulneráveis a ataques como Main-in-the-Middle ou escuta de rede.

Isso ocorre porque, em muitas redes não privadas, os dados não passam por criptografia, o que permite que um possível hacker entre na comunicação entre o seu dispositivo e o servidor acessado.

Esse tipo de ataque permite ao criminoso uma captura de informações como: senha, número de cartão de crédito ou dados bancários.

Exemplos Práticos:

Roubo de Senhas em Redes Wi-Fi Públicas:

Você precisa acessar uma rede Wi-fi para realizar o pagamento de uma conta, e acaba se conectando à rede do estabelecimento. E sem saber, um hacker que também está conectado em outro dispositivo à mesma rede, começa a monitorar seu tráfego de dados e faz uma captura da sua senha. Após isso, o hacker tem acesso a sua conta e pode realizar transações bancárias em seu nome.

Como Proteger suas Transações em Wi-Fi Público:

- Evite acessar dados sensíveis;
- Use uma VPN (Rede Privada Virtual);
- Verifique se o site acessado utiliza HTTPS;
- Evite se Conectar a Redes Wi-Fi Públicas Desconhecidas;
- Mantenha seu dispositivo de acesso atualizado;

Considerações finais

Em conclusão, a segurança digital é fundamental para garantir a proteção de dados pessoais e financeiros no uso cotidiano da internet. Medidas como manter as **atualizações automáticas de software** em dia, adotar práticas seguras em **compras online**, utilizar **VPNs** para aumentar a privacidade, gerenciar o **controle de privacidade nas redes sociais** e evitar o uso de **Wi-Fi público** para transações sensíveis são essenciais para minimizar riscos. Ao adotar essas práticas, os usuários podem aproveitar os benefícios da tecnologia de forma mais segura e consciente, reduzindo a exposição a ameaças cibernéticas e mantendo a integridade das informações pessoais.

Referências

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 mar. 2025.

CERT.BR – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de Segurança para Internet. 4. ed. São Paulo: CGI.br, 2023. Disponível em: https://cartilha.cert.br. Acesso em: 1 mar. 2025.

G1. Golpes na internet: veja como evitar cair em fraudes em compras online. Disponível em: https://g1.globo.com/economia/noticia/2024/01/10/golpes-na-internet-compras-online.ghtml. Acesso em: 1 mar. 2025.

Kaspersky. O que é uma VPN? *Kaspersky Resource Center*. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-a-vpn. Acesso em: 1 mar. 2025.

Pereira, Marcela. “Não Ignore! A Importância Das Atualizações de Software Para Sua Segurança - CIASC.” CIASC -, 2 Dec. 2024, Não ignore! A importância das atualizações de software para sua segurança - CIASC. Acesso em 2 Mar. 2025.

Rocha, Leonardo. **ACorp.** Atualizações de software: por que são cruciais para a cibersegurança? *ACorp*. Disponível em: http://acorp.com.br/atualizacoes-de-software-por-que-sao-cruciais-para-a-ciberseguranca/?utm_source=chatgpt.com. Acesso em: 02 mar. 2025.

TECHTUDO. Dicas de Segurança para Usar Wi-Fi Público. Disponível em: https://www.techtudo.com.br. Acesso em: 03 mar. 2025.

OTAVIO, Murillo. Wi-Fi público tem risco baixo, mas pode permitir golpes; veja dicas para se prevenir. Globo G1, 2024. Disponível em: https://g1.globo.com/google/amp/tecnologia/noticia/2024/04/26/wi-fi-publico-tem-risco-baixo-mas-pode-permitir-golpes-veja-dicas-para-se-prevenir.ghtml. Acesso em: 03 de março de 2025.

MEDIAMANAGER. Guia Completo sobre Proteção de Privacidade nas Redes Sociais. Disponível em: https://mediamanager.com.br/blog/seguranca-online/proteger-privacidade-redes-sociais. Acesso em: 4 mar. 2025.

THABYTE. Como Proteger Seus Dados nas Redes Sociais. Disponível em: https://thabyte.com.br/privacidade-nas-redes-sociais-como-proteger-seus-dados. Acesso em: 4 mar. 2025.