

Faculdade de Tecnologia de Sorocaba

Tecnologia em Análise e Desenvolvimento de Sistemas

**Segurança na Web**

ATIVIDADE 2

Prof. Denilce

Disciplina: Programação para Web

José de Oliveira Neto 0030482111039

Sorocaba

Agosto/2022

**Sumário**

[1 Introdução 3](#_Toc112625912)

[2 Ameaças à segurança na Web 4](#_Toc112625913)

[3 Como se proteger ao navegar pela internet 5](#_Toc112625914)

[4 Segurança de rede 7](#_Toc112625915)

[5 Conclusão 9](#_Toc112625916)

[6 Referências 11](#_Toc112625917)

# Introdução

A segurança na web é um conceito que define as medidas de segurança e proteção nas transações e atividades feitas na internet. Ela abrange vários tópicos relacionados à segurança online.

Neste trabalho, será abordado como deve ser o comportamento do usuário na web, proteção de redes, segurança do navegador, ameaças à segurança etc.

Além disso, mostrará a importância de se manter seguro ao navegar pela internet perante as diversas maneiras de se roubar dados e prejudicar o usuário e sua privacidade.

# Ameaças à segurança na Web

É necessário conhecer as principais ameaças que existem para garantir uma melhor segurança online.

**Malware**

É conhecido como vírus e é definido como qualquer software criado para danificar um computador, rede, sistema ou servidor. Pode ser usado para roubar informações ou invasão de privacidade e é espalhado de diversas formas.

**Phishing**

É um tipo de ataque virtual que envolve e-mails falsos ou mensagens que simulam outros sites ou aplicativos. É uma das ameaças mais utilizadas e simples de se fazer. Por exemplo: Um e-mail de solicitação de confirmação de banco pedindo número e senha de cartão.

**Hackeamento e acesso remoto**

Os softwares de acesso remoto permitem que os usuários acessem e controlem um computador remotamente e, desde a pandemia, com mais pessoas trabalhando remotamente, sua utilização aumentou. Os hackers usam diferentes técnicas para explorar vulnerabilidades de RDP até que tenham total acesso a uma rede e aos seus dispositivos. Eles mesmos podem roubar dados ou vender as credenciais na dark web.

**Ransomware**

Ransomware é um tipo de malware que impede você de usar o seu computador ou acessar arquivos específicos no seu computador se um resgate não for pago. Geralmente, ele é distribuído como um cavalo de Troia, ou seja, malware disfarçado de software legítimo. Os preços dos resgates variam, dependendo da variante de ransomware e do preço ou da taxa de câmbio das moedas digitais.

# Como se proteger ao navegar pela internet

**Use o firewall**

Os firewalls bloqueiam tráfego indesejado e podem ajudar a impedir que software malicioso infecte o seu computador. Normalmente, o seu sistema operacional e sistema de segurança vêm com um firewall pré-instalado. Para maximizar a segurança na Internet, é uma boa ideia certificar-se de que esses recursos estejam ativados, com suas configurações definidas para executar atualizações automaticamente.

**Use um navegador seguro**

Nossos navegadores são a porta de entrada principal para a web e por isso desempenham um papel fundamental na segurança na Internet. Um bom navegador da web deve ser seguro e ajudar a proteger você de violações de dados.

**Crie senhas fortes**

* Evita o óbvio – como usar números em sequência (“1234”) ou informações pessoais que alguém que conhece você possa adivinhar, como sua data de nascimento ou o nome do seu animal de estimação.
* Longa – composta de até 12 ou mais caracteres.
* Evite caminhos no teclado que sejam fáceis de memorizar.
* Uma combinação de caracteres – ou seja, letras minúsculas e maiúsculas, além de símbolos e números.

**Use um antivírus**

O melhor software de segurança na Internet protege você de diferentes tipos de ataques na Internet e protege seus dados on-line. É importante manter o software antivírus atualizado.

**Mantenha seu e-mail seguro**

* Marque e-mails de spam como spam – isso ajuda o provedor de e-mail a refinar sua filtragem de spam. Como marcar uma mensagem de spam varia de acordo com o cliente de e-mail que você usa – Outlook, Gmail, Apple Mail, Yahoo Mail e assim por diante.
* Nunca clique em um link ou abra um anexo em um e-mail de spam. Ao fazer isso, você pode baixar um malware no seu dispositivo. Na pior das hipóteses, você confirma para os golpistas que sua conta de e-mail está ativa, incentivando-os a enviar mais spam.
* Cuidado com os locais onde você divulga seu endereço de e-mail. É uma boa ideia ter uma conta de e-mail secundária e descartável que você usa somente para inscrições e assinaturas e separada da que você usa para amigos e familiares e da que você usa no trabalho.
* A maioria dos provedores de e-mail oferece configurações de privacidade analise-as e certifique-se de que estejam definidas em um nível com o qual você se sinta confortável.
* Analise filtros de spam de e-mails de terceiros. Eles oferecem uma camada adicional de segurança virtual, pois os e-mails têm que passar por dois filtros de spam antes de chegar até você – o filtro de spam do provedor de e-mail e o aplicativo de terceiros.

# Segurança de rede

Segurança de rede refere-se a qualquer atividade criada para proteger a usabilidade e a integridade da sua rede e dos seus dados. Destina-se a uma variedade de ameaças e as impede de entrar ou se espalhar na sua rede.

**Configure o roteador Wi-Fi com segurança**

Há vários recursos e configurações que você pode desativar para aumentar a segurança do seu roteador Wi-Fi. Programas de malware podem tirar vantagem de recursos como acesso remoto, plug and play universal e configuração de Wi-Fi protegido. Embora possam ser práticos, desativá-los torna sua rede doméstica mais segura.

**Usar uma VPN (principalmente ao acessar Wi-Fi público)**

Uma VPN cria um túnel criptografado entre você e um servidor remoto operado por um serviço de VPN. Todo o seu tráfego de Internet é roteado através desse túnel, o que torna seus dados mais seguros. Se você se conectar a uma rede pública usando VPN, outras pessoas nessa rede não poderão ver o que você está fazendo. Isso fornece maior proteção na Internet.

**Segurança da rede e Internet das Coisas**

Internet das Coisas (IoT) é um termo usado para descrever dispositivos físicos que não sejam computadores, telefones e servidores, que se conectam à Internet e podem coletar e compartilhar dados. Não só o volume de dados compartilhados via IoT nunca foi tão grande como a natureza desses dados é com frequência altamente confidencial. Isso destaca a necessidade de conhecer as ameaças à segurança da Internet e de praticar uma boa higiene de segurança virtual.

**Dicas de segurança na Internet**

* Instalar um software de segurança na Internet que proteja você o tempo todo
* Bloqueie o acesso à webcam
* Um bloqueador de anúncios pode proteger de malvertising.
* Proteção entre plataformas

Transações bancárias e compras on-line seguras.

# Conclusão

Após apresentar as diversas maneiras de como seus dados podem ser roubados na internet, percebemos a extrema importância de se manter atualizado em relação as formas de se proteger na web.

Mesmo estando sendo constantemente ameaçados ao navegar na web, temos vários jeitos de se proteger e garantir a integridade e segurança de seus dados pessoais. Ter o conhecimento e aplicar essas medidas de segurança vão te ajudar a se manter seguro a todo momento.

# Referências

Acesso em 29/08/2022

https://edu.gcfglobal.org/pt/seguranca-na-internet/o-que-e-seguranca-na-internet/1/

https://www.boavontade.com/pt/tecnologia/7-dicas-para-navegar-com-seguranca-na-internet

https://www.cloudflare.com/pt-br/learning/security/what-is-web-application-security/

https://www.eset.com/br/artigos/dicas-de-seguranca-na-internet/