**ANÁLISE E DESENVOLVIMENTO DE SISTEMAS – AMS**

**FATEC**

**Pesquisa**

**SEGURANÇA NA WEB**

Matheus de Araujo Emidio

**Sorocaba/SP**

**Fevereiro de 2024**

**Introdução**

A segurança na Internet pode ser entendida como os cuidados que devemos ter para proteger os nossos equipamentos que estão conectados com a internet, como por exemplo a infraestrutura, ou seja, nossos computadores e as informações que são os alvos principais dos cibercriminosos.

Este tipo de segurança conta com bases de dados, arquivos e aparelhos que fazem com que as informações importantes não caiam em mãos de pessoas erradas.

Uma das melhores formas de se manter seguro na internet é usando **antivírus** nos computadores, por isso sempre tenha um instalado nos seus equipamentos.

**O que é segurança da Internet? – Definição e significado**

Segurança da internet é o termo que se refere a segurança de atividade e transações feitas pela internet. Trata-se de um componente particular de ideias maiores, tal como a segurança virtual e do computador, com tópicos que são segurança do navegador, comportamento on-line e segurança da internet.

**Quais são as ameaças mais comuns à segurança na Internet?**

1. **Phishing**

Phishing é um ataque virtual envolvendo e-mails enganosos.

1. **Hackeamento e acesso remoto**

O protocolo que permite aos usuários controlar um computador conectado à Internet remotamente é chamado de Remote Desktop Protocol, ou RDP.

1. **Malware e malvertising**

Malware é a combinação dos termos "malicious" (malicioso) e "software". É um termo amplo relacionado a vírus, worms, cavalos de Troia e outros programas danosos que os hackers usam para causar estragos e roubar informações confidenciais.

1. **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.

1. **Botnets**

Uma botnet é uma rede de computadores que foram intencionalmente infectados por um malware, de forma que eles possam realizar tarefas automatizadas na internet sem a permissão ou o conhecimento dos proprietários dos computadores.

Quando o proprietário de uma botnet controla o seu computador, ele pode usá-lo para realizar atividades maliciosas. Entre elas:

* Gerar tráfego falso na Internet em sites de terceiros para ganho financeiro.
* Usar o poder da máquina para auxiliar ataques de negação de serviço distribuído (DDoS, Distributed Denial of Service) para derrubar sites.
* Enviar e-mails de spam a milhões de usuários da Internet.
* Cometer fraudes e roubos de identidade.
* Atacar computadores e servidores.

1. **Ameaças a Wi-Fi, público ou doméstico**

O Wi-Fi público apresenta riscos porque a segurança dessas redes, em cafeterias, shoppings, aeroportos, hotéis, restaurantes, entre outros, costuma ser relaxada ou inexistente. Falta de segurança significa que criminosos virtuais e ladrões de identidade podem monitorar o que você está fazendo on-line e roubar suas senhas e informações pessoais. Os perigos do Wi-Fi incluem:

* **Packet sniffing** – os invasores monitoram e interceptam dados descriptografados enquanto transitam em uma rede desprotegida.
* **Ataques "man-in-the-middle"** – os invasores comprometem um hotspot Wi-Fi para se inserir nas comunicações entre a vítima e o hotspot para interceptar e modificar os dados em trânsito.
* **Redes de Wi-Fi criminosas** – os invasores estabelecem um honeypot na forma de Wi-Fi gratuito para colher dados valiosos. O hotspot do invasor torna-se o veículo para todos os dados trocados na rede.

**Como proteger seus dados on-line**

* 1. **Ative a autenticação multifatorial sempre que puder**

Autenticação multifatorial (MFA) é um método de autenticação que pede aos usuários que forneçam dois ou mais métodos de verificação para acessar uma conta on-line.

* 1. **Use um firewall**

Um firewall funciona como uma barreira entre o computador e outra rede, como a Internet. Os firewalls bloqueiam tráfego indesejado e também podem ajudar a impedir que software malicioso infecte o computador.

* 1. **Escolha seu navegador com cuidado**

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.

* 1. **Crie senhas fortes e use um gerenciador de senhas seguro**

Uma senha forte ajudará você a manter a segurança na Internet. Uma boa senha é:

* Longa – composta de até 12 ou mais caracteres.
* Uma combinação de caracteres – ou seja, letras minúsculas e maiúsculas, além de símbolos e números.
* Evite 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.
* Evite caminhos no teclado que sejam fáceis de memorizar.

Hoje em dia, substituir letras e números por caracteres parecidos não é mais suficiente; por exemplo, "S3nh@" para "senha", pois os hackers estão atentos a isso. Quanto mais complexa for sua senha, mais difícil de descobri-la. Um gerenciador de senhas pode ajudar – gerando, armazenando e gerenciando todas as suas senhas em uma conta on-line segura.

* 1. **Mantenha um programa de segurança atualizado instalado nos seus dispositivos**

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.

**Como se proteger on-line**

* 1. **Você precisa de um software de segurança na Internet que proteja você o tempo todo**

O melhor software de segurança na Internet protegerá você de várias ameaças à segurança na Internet, incluindo hackeamento, vírus e malware.

* 1. **Bloqueie o acesso à webcam, de forma que sua privacidade na Internet seja assegurada**

O hackeamento da webcam ocorre quando os hackers acessam a câmera do seu dispositivo móvel e computador e gravam você.

* 1. **Um bloqueador de anúncios pode proteger você de malvertising**

Os bloqueadores de anúncios limpam os anúncios das páginas da web e, ao bloquear a exibição de anúncios, você remove o risco de ver e clicar em um que possa ser danoso.

* 1. **Cuide de toda a família com o controle de pais**

Controle de pais refere-se às configurações que permitem que você controle o conteúdo que o seu filho pode ver na Internet.

* 1. **PC Cleaner**

O PC Cleaner é uma ferramenta que remove arquivos e programas desnecessários e temporários do seu sistema.

* 1. **Proteção entre plataformas**

Hoje em dia, a proteção na Internet precisa dar conta de todos os dispositivos que usamos on-line – notebooks, desktops, smartphones e tablets.

* 1. **Transações bancárias e compras on-line seguras**

**As dicas de segurança de compras on-line a serem lembradas incluem:**

* Certifique-se de estar fazendo transações com um site seguro – a URL deve começar com https:// em vez de http:// – o "s" significa "seguro" e indica que o site possui um certificado de segurança.
* Verifique a URL com atenção.
* Evite enviar informações financeiras ao usar Wi-Fi público.

**Dicas de segurança em transações bancárias incluem:**

* Novamente, evite enviar informações financeiras ou pessoais ao usar Wi-Fi público.
* Use senhas fortes e altere-as regularmente.
* Use autenticação multifatorial sempre que possível.
* Para evitar ser vítima de um golpe de phishing, digite a URL do seu banco ou use o seu aplicativo de transações bancárias diretamente, em vez de clicar em links em e-mails.
* Verifique as faturas bancárias regularmente para identificar qualquer transação que você não reconheça.
* Mantenha seu sistema operacional, navegador e aplicativos atualizados. Isso garantirá que todas as vulnerabilidades conhecidas sejam corrigidas.
* Use um produto de segurança na Internet robusto, como os produtos oferecidos pela Kaspersky.

**Conclusão**

Em um mundo em que passamos a maior parte da nossa vida on-line, a segurança na Internet é uma questão importante. Entender como enfrentar as ameaças à segurança na Internet e os diferentes tipos de ataques na Internet é fundamental para permanecer seguro e proteger seus dados on-line.

**Referencias**

<https://www.kaspersky.com.br/resource-center/definitions/what-is-internet-security>

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