Título do Curso: Fundamentos de Segurança Digital

Objetivo do curso:

Ensinar os conceitos básicos de segurança digital para iniciantes, com foco em proteção de dados pessoais, prevenção contra ataques cibernéticos e boas práticas no uso da internet.

Módulo 1: Introdução à Segurança Digital

Segurança Digital

Atualmente, cerca de 5,4 bilhões de pessoas têm acesso à internet em todo o mundo. Esse amplo acesso, embora traga inúmeros benefícios, também nos expõe a diversos riscos, como ataques cibernéticos, vazamento de dados e outros crimes digitais. Diante desse cenário, a segurança digital torna-se essencial para proteger as informações dos usuários e garantir uma navegação mais segura. Investir em medidas de segurança digital é, portanto, fundamental para dificultar o acesso de criminosos aos nossos dados e promover um ambiente digital mais confiável para todos.

A segurança digital é a aplicação de medidas para proteger a confidencialidade, a integridadae, a disponibilidade e a autenticidade de documentos e dados pessoais. Esse segmento dedica-se a bloquear ameaças no ambiente digital em diferentes realidades, como empresas ou pessoas.

Informações roubadas podem causar inúmeras consequências negativas para pessoas e organizações. Com acesso a determinados dados, criminosos podem fazer compras, empréstimos e até abrir empresas em nome das vítimas, entre outras ações que podem prejudicar os envolvidos.

No caso das crianças, a segurança digital se mostra ainda mais importante. Em primeiro lugar porque, segundo a Constituição Federal, os direitos infantis devem ser considerados prioridade absoluta na implementação de qualquer medida, isto é, devem ser prioritários em relação a quaisquer interesses econômicos. Dentre esses direitos, está incluído o direito à privacidade.

O objetivo da segurança digital é garantir que redes, servidores, programas, computadores e demais dispositivos conectados à internet estejam protegidos contra ataques. E, para isso, diversos métodos podem ser utilizados para preservar a privacidade dos dados e serão mostrados no módulo 2.

Tipos de ameaças virtuais

São muitas as ameaças à segurança digital. Abaixo, selecionamos algumas das principais responsáveis por crimes virtuais e pelo vazamento de dados.

Malwares

São arquivos enviados com o objetivo de prejudicar ou mesmo de roubar informações de uma máquina ao serem executados por ela. Existem casos em que esses arquivos solicitam a permissão dos administradores, que acabam sendo induzidos a conceder.

Em outras situações, os malwares se aproveitam de vulnerabilidades de um programa específico para acessar documentos confidenciais. Existem inúmeros tipos de malwares, que funcionam de maneiras diferentes.

Um exemplo de malware são os famosos “vírus”, que se instalam nos aparelhos e o prejudicam de diversas formas.

Phishing

Phishing é uma pratica de envio de e-mails fraudulentos, nesse caso os bandidos enviam mensagens que muito se assemelham a fontes confiáveis. A vítima acredita que se trata de uma empresa ou de um contato confiável e acaba tendo seus dados roubados, incluindo números de cartões de crédito ou mesmo informações de login.

O phishing é considerado um dos ataques virtuais mais comuns. Por isso, sempre que notar que se trata de um e-mail fraudulento, é fundamental marcá-lo como phishing na sua caixa de entrada para filtrá-los e, ao mesmo tempo, ajudar o sistema a se manter mais protegido contra o endereço responsável pelo envio.

Engenharia social

Trata-se de uma técnica empregada por criminosos para induzir as vítimas a enviar dados confidenciais. Muitas vezes, ela é combinada com as outras ameaças citadas anteriormente, manipulando o indivíduo a clicar em links maliciosos ou a baixar programas que podem infectar sua rede e/ou dispositivo.

Conteúdo copiado de https://viverbem.unimedbh.com.br/qualidade-de-vida/seguranca-digital/

Importância da segurança digital no dia a dia

Todos os dias nós temos contato com a internet, usando para trabalhar, estudar, fazer compras, pagar contas e etc... Nesse ambiente digital, nossos dados ficam expostos a riscos de ataques cibernéticos, como foi abordado no modulo 1. A partir disso, podemos afirmar que a segurança digital é sem duvidas uma pratica extremamente necessária nos dias de hoje e sem essa prática, podemos ser vitimas , de golpes roubo de identidade, invasão de contas, vazamento de dados e entre outros crimes cibernéticos. Portanto, entender e aplicar medidas de segurança digital no dia a dia é fundamental para garantir nossa privacidade, evitar transtornos e navegar com mais tranquilidade.

Exemplo prático:

Aqui estão alguns exemplos de ataques cibernéticos reais:

LinkedIn – Em junho de 2012, a rede social LinkedIn sofreu uma invasão que expôs os dados pessoais de mais de 117 milhões de usuários. Além de permitir o acesso a senhas, o vazamento expôs dados pessoais como endereço de e-mail e nome de usuários.

eBay – Em maio de 2014, um vazamento de dados expôs as contas de 145 milhões de usuários (nomes, endereços, datas de nascimento e senhas criptografadas) da eBay, uma das maiores empresas de comércio eletrônico do mundo. Segundo a empresa, hackers usaram as credenciais de três funcionários para acessar sua rede e tiveram livre acesso ao banco de dados dos usuários por 229 dias.

Uber – Em 2016, o aplicativo de transporte Uber foi vítima de uma invasão que resultou no roubo de dados de mais de 57 milhões de usuários, incluindo 200 mil brasileiros. Esse caso de vazamento de dados, no entanto, só veio a público em 2017 e a empresa foi multada em US$ 150 milhões pelo governo do estado da Califórnia, nos Estados Unidos.

—

Módulo 2: Boas Práticas de Segurança na Internet

Criação de senhas fortes

Uma senha forte é a principal barreira para evitar que a maioria de suas contas on-line sejam invadidas. Sem práticas atualizadas, você pode estar usando senhas que os fraudadores cibernéticos conseguem adivinhar facilmente em poucas horas. Expor-se ao roubo de identidades e à extorsão é um risco que você nunca deve correr. Você deve criar senhas capazes de combater os métodos modernos de roubo.

Para se proteger dos mais novos métodos de invasão, você precisa de senhas robustas. Aqui estão algumas formas de deixar a sua senha robusta e difícil de combater:

- Senhas longas: Tente usar pelo menos 10 ou 12 caracteres, ou o máximo possível.
- Senhas óbvias: Evite sequências, como "12345" ou "qwerty", pois elas podem ser hackeadas por força bruta em segundos. Pelo mesmo motivo, evite também palavras comuns ("senha1")
- Senhas com caracteres especiais: Letras minúsculas e maiúsculas, símbolos e números devem fazer parte da senha. A variedade pode tornar a sua senha mais imprevisível.
- Senha com combinação de palavras incomuns: As senhas podem ser mais seguras se usarem palavras inesperadas. Mesmo que você use palavras comuns, é possível organizá-las em uma ordem estranha e certificar-se de que não estejam relacionadas. Ambos os métodos podem neutralizar os hackeamentos baseados em dicionários.

- Senhas “fáceis”: Use algo que faça sentido para você, mas que será difícil para os computadores adivinharem. Mesmo senhas aleatórias podem ser lembradas pela memória muscular, sendo semilegíveis. Mas senhas que impeçam o seu acesso não ajudam muito.

Com alguns dessas formas de criar senhas mais robustas, podemos afirmar que a segurança digital estará mais protegida.

Autenticação em dois fatores

A autenticação de dois fatores é uma camada extra de proteção que pode ser ativada em contas online. Também conhecido pela sigla 2FA, originária do inglês "*two-factor authentication*", o recurso insere uma segunda verificação de identidade do usuário no momento do login, evitando o acesso às contas mesmo quando a senha é vazada.

A funcionalidade está presente nos principais sites e aplicativos atuais,como Google, Facebook, Instagram, Amazon, Dropbox, PayPal e Mercado Livre. Cada plataforma oferece diferentes métodos de verificação, que podem compreender códigos SMS, dispositivos de token e biometria, por exemplo

Cuidados com redes Wi-Fi públicas

Em cafés, hotéis, shoppings, aeroportos e muitos outros locais que oferecem a seus clientes acesso a um Wi-Fi público, é conveniente conferir e-mails, interagir nas redes sociais ou acessar a Internet durante o tempo livre. Entretanto, os criminosos virtuais costumam espionar redes Wi-Fi públicas e interceptar os dados transferidos pelo link. Dessa forma, o criminoso consegue acessar as credenciais bancárias, senhas de contas e outras informações valiosas dos usuários.

Aqui estão alguns cuidados a serem tomados com redes wifi públicas:

Uma conexão Wi-Fi pública é basicamente desprotegida, então tome cuidado. Laptops, smartphones e tablets são suscetíveis aos riscos de segurança de uma conexão sem fio. Não presuma que o link do Wi-Fi é legítimo. Pode ser um link falso, configurado por um criminoso virtual que tenta capturar informações pessoais valiosas de usuários mais desatentos. Questione tudo e não se conecte a pontos de acesso sem fio desconhecidos ou não reconhecidos. Use uma VPN (rede virtual privada), quando você usa uma VPN para se conectar a uma rede Wi-Fi pública, na verdade está usando um "túnel particular" que criptografa todos os dados que passam pela rede. Isso ajuda a evitar que criminosos virtuais, que ficam de tocaia na rede,

interceptem seus dados. Se for necessário acessar sites que armazenam ou exigem informações sigilosas, incluindo redes sociais, sites de compras on-line e bancos on-line, vale a pena acessá-los pela rede do seu celular, e não pela conexão Wi-Fi pública.

Módulo 3: Ferramentas e Recursos de Proteção

firewall

Um firewall é um dispositivo de segurança que monitora o tráfego de rede de entrada e saída e decide **permitir** ou **bloquear** tráfegos específicos de acordo com um conjunto definido de regras de segurança.

Os dados entram e saem dos dispositivos por meio do que chamamos de portas. Um firewall é o que controla o que é e, mais importante, não é permitido passar por essas portas. Você pode pensar nisso como um segurança parado na porta, verificando a ID de tudo o que tenta entrar ou sair.

Para a maioria dos computadores normais ou redes domésticas, o firewall deve permitir muito pouco, se houver, tráfego de entrada. Raramente há qualquer motivo legítimo para que outros dispositivos precisem se conectar ao seu dispositivo, ou rede doméstica, não solicitados.

Os firewalls têm sido a linha de frente da defesa na segurança de rede e Internet há mais de 25 anos. Eles colocam uma barreira entre redes internas protegidas e controladas que podem ser redes externas confiáveis ou não, como a Internet.

Firewalls podem ser software ou hardware e, provavelmente, você está sendo protegido por ambos.O roteador (às vezes chamado de "modem") que traz a Internet do provedor de Internet para sua casa ou escritório geralmente é um firewall de hardware. E seu computador, seja executando Windows ou macOS, provavelmente tem um firewall de software em execução.

Antivirus

O antivírus é um software que identifica e protege os dispositivos de malwares, também conhecidos como vírus. Esse programa pode ser instalado em computadores e dispositivos móveis, como celulares e tablets.

A função mais simples de um antivírus é monitorar arquivos e outros programas de um dispositivo para detectar vírus. Quando novas aplicações são instaladas, o programa faz a verificação delas para saber se existe alguma ação suspeita. Se algo foi identificado, a instalação é bloqueada ou a nova aplicação é encaminhada para a quarentena.

A quarentena é um espaço de proteção criptografado e gerenciado pelo antivírus, para que o possível vírus não se espalhe pelo sistema operacional do dispositivo. Arquivos e programas são encaminhados para a quarentena quando o antivírus ainda não identificou exatamente o tipo de vírus ou problema apresentado

As vantagens de ter um anti vírus instalado são

- Segurança para aproveitar os recursos digitais
- Prevenção contra fraude de dados
- Suporte técnico(Dependendo do anti vírus)

A escolha do melhor antivírus é essencial para garantir a segurança do seu computador. Com o avanço constante das ameaças cibernéticas, ter um software de proteção confiável se tornou uma necessidade para qualquer usuário que utilize a internet. Neste contexto, entender a importância de selecionar o antivírus adequado é fundamental. Aqui estão alguns exemplos dos anti vírus mais conhecidos no mercado hoje em dia:

- McAfee
- Norton
- Avast
- Kaspersky

VPN (Virtual Private Network)

VPN significa **"Virtual Private Network"** (Rede Privada Virtual) e descreve a oportunidade de estabelecer uma conexão de rede protegida ao usar redes públicas. As VPNs criptografam

seu tráfego de Internet e disfarçam sua identidade online. Isso torna mais difícil para terceiros rastrear suas atividades online e roubar seus dados. A criptografia ocorre em **tempo real**.

Uma VPN oculta seu endereço IP deixando que a rede redirecione você por meio de um servidor remoto especialmente configurado executado por um host VPN. Isso significa que se você navegar online com uma VPN, o servidor VPN se tornará a fonte de seus dados. Isso significa que seu Provedor de Serviços de Internet (ISP) e terceiros não podem ver quais sites você visita ou quais dados você envia e recebe online. Uma VPN funciona como um filtro que transforma todos os seus dados em "rabiscos". Mesmo que alguém apreendesse dados, seria inútil.

Referencias

ALAMO (S.D.)

O QUE É SEGURANÇA DIGITAL

https://alana.org.br/glossario/seguranca-digital/#:~:text=A%20seguran%C3%A7a%20digital%20%C3%A9%20a,realidades%2C%20como%20empresas%20ou%20pessoas.

UNIMED(2023)

https://viverbem.unimedbh.com.br/qualidade-de-vida/seguranca-digital/

Exemplos de ataques ciberneticos

https://laramartinsadvogados.com.br/artigos/28-principais-casos-de-vazamentos-de-dados-na-historia/

senhas

https://www.kaspersky.com.br/resource-center/threats/how-to-create-a-strong-password

autenticação em dois fatores

https://www.techtudo.com.br/noticias/2021/08/autenticacao-de-dois-fatores-o-que-e-e-para-que-serve-o-recurso.ghtml

rede wiwi publicas

https://www.kaspersky.com.br/resource-center/preemptive-safety/public-wifi

firewall

https://www.sin.ufscar.br/servicos/conectividade/firewall/o-que-e-um-firewall

https://support.microsoft.com/pt-br/office/o-que-%C3%A9-um-firewall-6870c88d-69b6-4db4-9cb1-0e4afa7a8603

antivirus

http://eset.com/br/artigos/o-que-e-um-antivirus/?srsltid=AfmBOopv1yPxhZoS8CsYh-cH0klfd0VE041dyTbM2hwPlwU91n2z8GFE

https://bravotecnologia.com.br/tipos-de-antivirus-como-escolher-o-melhor/

VPN

https://www.kaspersky.com.br/resource-center/definitions/what-is-a-vpn