TECHBELÉM

UNAMA

Segurança Digital: Vírus, Golpes e Fake News

A internet é uma ferramenta incrível, mas para navegar com segurança, é fundamental entender os perigos que existem. Esta aula vai abordar três dos principais riscos: **vírus**, **golpes** e **fake news**.

1. Vírus de Computador e Malwares

Um **vírus** de computador é um tipo de programa malicioso (conhecido como **malware**) criado para causar danos ao seu dispositivo ou roubar informações. Ele pode se espalhar de várias maneiras e ter diferentes objetivos.

Como ele pode te infectar:

- **Anexos de e-mail:** Clicar em um arquivo anexado a um e-mail de um remetente desconhecido.
- **Downloads suspeitos:** Baixar programas de sites não confiáveis.
- **Pendrives infectados:** Conectar um pendrive que já foi usado em um computador com vírus.
- **Sites falsos:** Clicar em anúncios ou links em sites que parecem legítimos, mas não são.

Como se proteger:

- **Antivírus:** Instale um software antivírus de boa qualidade e mantenha-o sempre atualizado. Ele vai escanear arquivos e sites em tempo real para detectar e bloquear ameaças.
- **Atualize seus programas:** Mantenha o sistema operacional (Windows, macOS) e todos os seus programas atualizados. As atualizações frequentemente corrigem falhas de segurança.
- **Cuidado com anexos:** Nunca abra anexos de e-mails de desconhecidos. Se o e-mail for de alguém que você conhece, mas parecer estranho, confirme antes de abrir.
- **Baixe de fontes confiáveis:** Sempre baixe programas e aplicativos das lojas oficiais (Google Play Store, App Store) ou dos sites dos desenvolvedores.

2. Golpes na Internet (Phishing e outros)

Os **golpes** digitais tentam enganar você para que revele informações pessoais ou financeiras. O golpe mais comum é o **Phishing**.

O que é Phishing? O phishing é uma técnica na qual o golpista se passa por uma empresa, banco ou serviço conhecido. Ele envia um e-mail ou uma mensagem de texto com um link falso, pedindo para você atualizar seus dados, confirmar sua senha ou fazer um pagamento. A página para onde o link te leva é uma cópia idêntica da página original, mas o objetivo é roubar suas informações.

Sinais de alerta de um golpe:

- **Urgência exagerada:** "Sua conta será bloqueada em 24 horas! Clique aqui para resolver."
- **Errosde português:** E-mails ou mensagens com erros de gramática e digitação são um forte indício de golpe.
- **Endereços de e-mail estranhos:** Um e-mail que supostamente é do seu banco, mas vem de um endereço como `banco.oficial.br@hotmail.com`.
- **Ofertas boas demais:** "Você ganhou um prêmio!" ou "Clique aqui para ter 50% de desconto."

Como se proteger:

- **Desconfie sempre:** Se a mensagem é muito urgente ou a oferta é inacreditável, desconfie.
- **Não clique em links:** Em vez de clicar no link, digite o endereço do site (do banco, da loja) diretamente no seu navegador.
- **Nunca forneça dados sensíveis:** Senhas, números de cartão de crédito e códigos de segurança (CVV) nunca devem ser informados em resposta a um e-mail ou mensagem.

3. Fake News (Notícias Falsas)

Fake News são informações falsas, espalhadas geralmente pelas redes sociais e aplicativos de mensagens, com a intenção de enganar as pessoas. Elas podem ser usadas para manipular a opinião pública ou simplesmente espalhar desinformação.

Como identificar uma Fake News:

- **Títuloschocantese sensacionalistas:** "URGENTE: Notícia que a mídia não quer que você saiba!"

- **Falta de fontes:** A notícia não cita de onde a informação veio (um jornal, uma agência de notícias, um especialista).
- **Conteúdo vago e sem detalhes:** Textos que não especificam datas, locais ou nomes de pessoas importantes.
- **Fotos e vídeos fora de contexto:** Imagens verdadeiras que são usadas para ilustrar uma história falsa.

Como se proteger e não espalhar Fake News:

- **Verifique a fonte:** Antes de compartilhar, pesquise o site que publicou a notícia. É um veículo de notícias conhecido ou um blog desconhecido?
- **Pesquise em outrasfontes:** Procure a mesma notícia em sites de notícias confiáveis. Se ninguém mais estiver falando sobre o assunto, provavelmente é falso.
- **Cuidado com as emoções:** Fake news são feitas para gerar raiva ou indignação. Pare, respire e pense antes de compartilhar.
- **Não repasse sem checar:** Se você não tem certeza se uma notícia é verdadeira, não a envie para seus amigos e familiares.

A segurança digital é uma responsabilidade de todos. Com atenção e um pouco de cautela, você pode aproveitar tudo o que a internet tem a oferecer, mantendo-se protegido.

Aprofundando em Segurança Digital

O mundo da segurança digital é vasto, e entender os detalhes ajuda muito a se proteger. Vamos aprofundar cada um dos tópicos e incluir algumas novas informações.

1. Mais sobre Malwares

O termo **vírus** é muito popular, mas na verdade ele faz parte de uma categoria maior de programas maliciosos chamada **Malware**. Existem vários tipos, cada um com um objetivo diferente:

- **Ransomware:** Este é um dos mais perigosos. O Ransomware "sequestra" seus arquivos, criptografando-os para que você não consiga mais acessá-los. Para tê-los de volta, o criminoso exige um resgate (em inglês, ***ransom***), geralmente pago com criptomoedas. A melhor defesa contra esse tipo de ataque é ter **cópias de segurança (backups)** de todos os seus arquivos importantes em um HD externo ou na nuvem.
- **Spyware:** Como o nome sugere, este malware é um espião. Ele se instala no seu computador ou celular e monitora tudo o que você faz, como sites que

você visita, senhas que digita e mensagens que envia. Ele envia essas informações para o criminoso sem que você perceba.

2. A Arte do Golpe: Engenharia Social

A maioria dos golpes digitais não usa apenas programas maliciosos. Eles se baseiam na **engenharia social**, que é a arte de manipular pessoas para que elas revelem informações confidenciais. Os golpistas usam gatilhos psicológicos como **curiosidade**, **medo** e **urgência** para fazer com que você clique em um link ou revele um dado.

- **Phishing e suas variantes:** O phishing por e-mail é o mais conhecido, mas o golpe também pode vir por outros meios:
  - **Smishing:** O golpe vem por mensagem de texto (**SMS**). Você recebe uma mensagem dizendo que sua entrega foi cancelada e pedindo para você clicar em um link para resolver o problema.
  - **Vishing:** O golpe acontece por telefone (**voz**). Você recebe uma ligação de alguém que se passa por um funcionário de um banco, pedindo para você confirmar seus dados para evitar uma fraude.

A regra de ouro é sempre **desconfiar**. Empresas legítimas não pedem dados pessoais ou senhas por e-mail, SMS ou telefone.

3. Combatendo a desinformação: Verificação de Fatos

Entender a motivação por trás das **Fake News** é o primeiro passo para combatê-las. Elas podem ser espalhadas por:

- **Dinheiro:** Alguns sites ganham dinheiro com anúncios a cada clique. Eles criam notícias falsas e sensacionalistas para atrair o maior número de visitantes possível.
- **Ideologia ou manipulação política:** Grupos podem espalhar notícias falsas para atacar adversários ou influenciar a opinião pública.

Para checar uma notícia, você pode usar **sites de checagem de fatos**, também chamados de **fato-checadores**. Existem organizações especializadas em verificar informações publicadas na internet. No Brasil, alguns exemplos são o **Agência Lupa** e o **Aos Fatos**. Quando tiver dúvida, procure por essas plataformas.

4. O pilar da segurança: Senhas e Autenticação

Ter senhas fortes e únicas é a sua primeira linha de defesa.

- **Senhas fortes:** Use senhas longas, com uma mistura de letras maiúsculas e minúsculas, números e símbolos. Evite usar palavras comuns ou informações pessoais.
- **Senhas únicas:** Crie uma senha diferente para cada serviço (e-mail, redes sociais, banco, etc.). Se um site for invadido e sua senha for roubada, os criminosos não poderão usar a mesma senha para acessar suas outras contas.
- **Gerenciador de senhas:** Para não ter que decorar dezenas de senhas, use um gerenciador de senhas. Ele é um aplicativo que armazena todas as suas senhas de forma segura, e você só precisa se lembrar de uma única senha mestra.
- **Autenticação de dois fatores (2FA):** Ative a 2FA em todas as suas contas. Mesmo que alguém descubra sua senha, ela precisará do seu celular para receber um código de acesso e entrar na sua conta. Isso adiciona uma camada de proteção praticamente intransponível.

A segurança digital é um processo contínuo. Quanto mais você souber, mais protegido estará.

1. Qual termo é usado para descrever programas maliciosos, como vírus, criados para danificar seu dispositivo ou roubar informações?

A) Software Utilitário
B) Firewall
C) Sistema Operacional
D) Malware

2. Qual técnica de golpe se baseia em e-mails falsos que se parecem com os de empresas legítimas para roubar dados pessoais, como senhas e números de cartão de crédito?

A) Hacking
B) Ransomware
C) Spam
D) Phishing

3. Qual destes sinais é um forte indicativo de que uma notícia pode ser uma 'Fake News'?
   A) A notícia é sobre um evento importante.
   B) O título é longo e detalhado.
   C) Não há uma fonte confiável citada ou o conteúdo parece vago.
   D) Ela foi publicada em um grande e conhecido portal de notícias.

4. Qual é a melhor prática para proteger suas contas online?
   A) Compartilhar suas senhas com amigos e familiares.
   B) Ativar a autenticação de dois fatores (2FA).
   C) Anotar todas as suas senhas em um papel e guardá-lo na carteira.
   D) Usar a mesma senha para todas as contas.

5. Para se proteger de vírus, a melhor ação é:
   A) Desativar o seu antivírus para que ele não consome bateria.
   B) Manter o software antivírus e o sistema operacional sempre atualizados.
   C) Abrir todos os anexos de e-mails, mesmo que pareçam suspeitos.
   D) Baixar programas de sites desconhecidos para economizar tempo.