

**Educação
Profissional
Paulista**

Técnico em
**Ciência de
Dados**

Introdução à informática

Navegação na internet e segurança on-line

Aula 1

Código da aula: [DADOS]ANO1C1B3S22A1

**Introdução à
informática**

Mapa da Unidade 5 Componente 1

semana

19

Produtividade com
software (parte II)

Você está aqui!

Navegação na internet
e segurança on-line

semana

22

semana

11

Sistemas
operacionais
(parte II)

semana

15

Produtividade com
software (parte I)



Introdução à
informática

Mapa da
Unidade 5
Componente 1

Você está aqui!

Navegação na internet e
segurança on-line

Aula 1

Código da aula: [DADOS]ANO1C1B3S22A1

22



Objetivos da aula

- Aprender fundamentos de navegação na internet;
- Aprender alguns tipos de golpes famosos na internet.



Recursos didáticos

- Recurso audiovisual para exibição de vídeos e imagens;
- Acesso ao laboratório de informática e/ou à internet.



Duração da aula

50 minutos.



Competências técnicas

- Aprender a se comunicar e a pensar de forma crítica e analítica.



Competências socioemocionais

- Trabalhar em equipe, compartilhando conhecimentos, contribuindo com ideias e colaborando para alcançar objetivos comuns.

Primeiras ideias

- Você acessaria esse site?
Que indícios temos de que um site não é malicioso?
- Se nos depararmos com um site ou app suspeito, o que podemos fazer para nos proteger?
- Quais são os riscos dos ataques digitais? O que podem roubar ou descobrir sobre nós?

Ponto de partida

Como a Target, uma das maiores varejistas dos Estados Unidos, descobriu uma gravidez antes da família?

Leiam atentamente o texto abaixo:

BIG DATA: como a Target descobriu uma gravidez antes da família? *Guide*, 18 fev. 2019. Disponível em: <https://conteudos.guide.com.br/textos/big-data-como-a-target-descobriu-uma-gravidez-antes-da-propria-familia/>. Acesso em: 21 jun. 2024.



© Getty Images

Como funciona a navegação na internet?

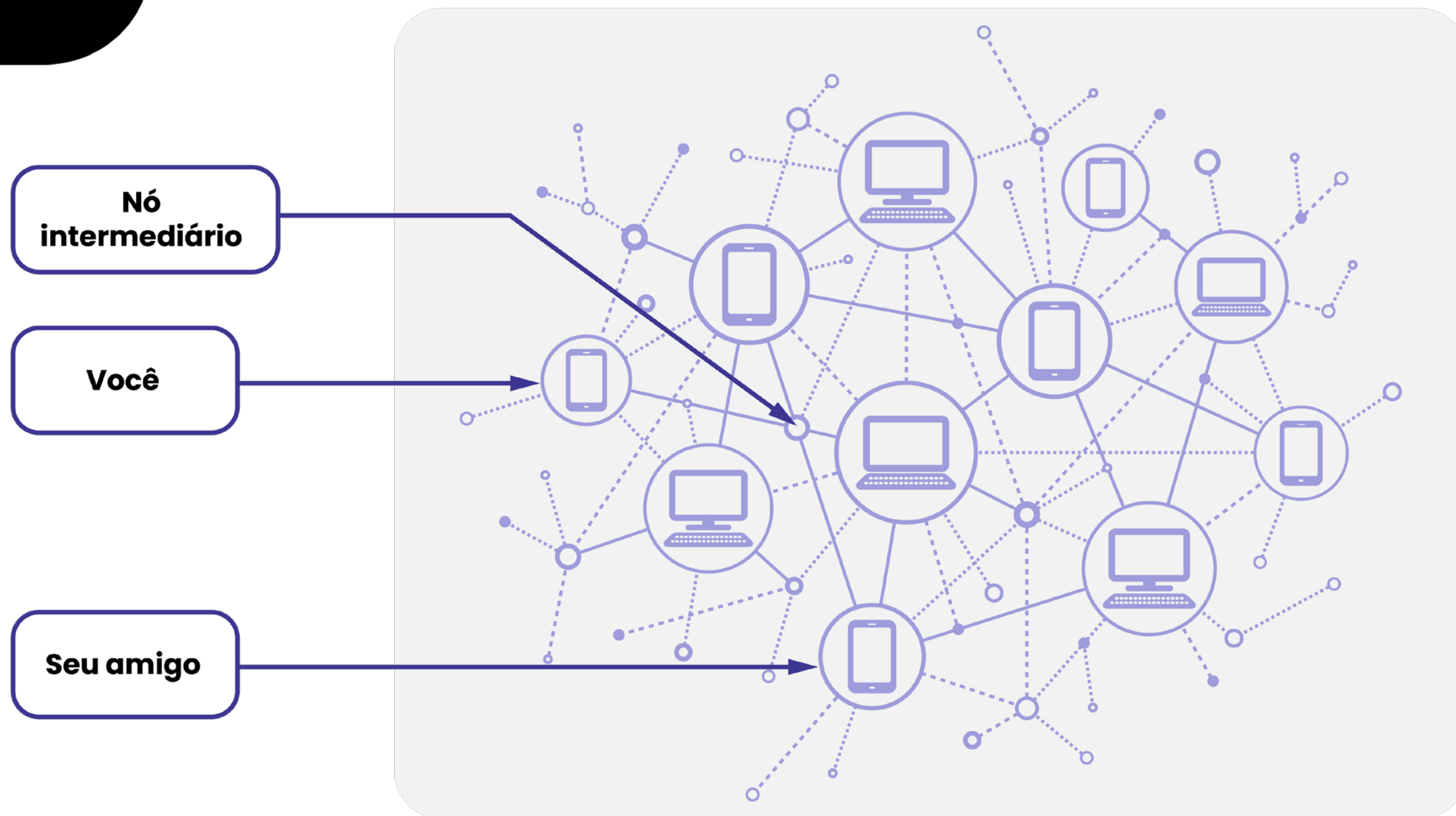
- ▶ A navegação na internet baseia-se na **troca de dados** em pequenas unidades chamadas **“pacotes”**. Cada pacote contém uma parte dos dados enviados e informações sobre seu destino.
- ▶ Quando você acessa um site, seu navegador envia uma **requisição** para o **servidor em que o site está hospedado**. Essa requisição é dividida em pacotes, que viajam por meio de diferentes rotas na rede até chegarem ao servidor.
- ▶ Após processar sua requisição, o servidor responde enviando os dados do site de volta ao seu computador, também em forma de pacotes.

O protocolo HTTP e sua importância

- ▶ **HTTP (Hypertext Transfer Protocol)** é o **protocolo de comunicação** utilizado para transmitir dados na **World Wide Web**. Ele define não apenas como mensagens das requisições são formatadas e transmitidas, mas também como os servidores e navegadores devem reagir a essas mensagens.
- ▶ Quando você digita uma **URL (endereço do site)** em seu navegador, está iniciando uma requisição HTTP. Essa requisição pede ao servidor que hospeda o site para enviar os dados necessários para carregar a página no seu navegador.
- ▶ Para sua mensagem chegar até o servidor, ela viaja através de vários nós da internet (como computadores, roteadores, outros servidores), que vão repassando a mensagem de um para o outro.

Construindo
o **conceito**

Exemplo de comunicação

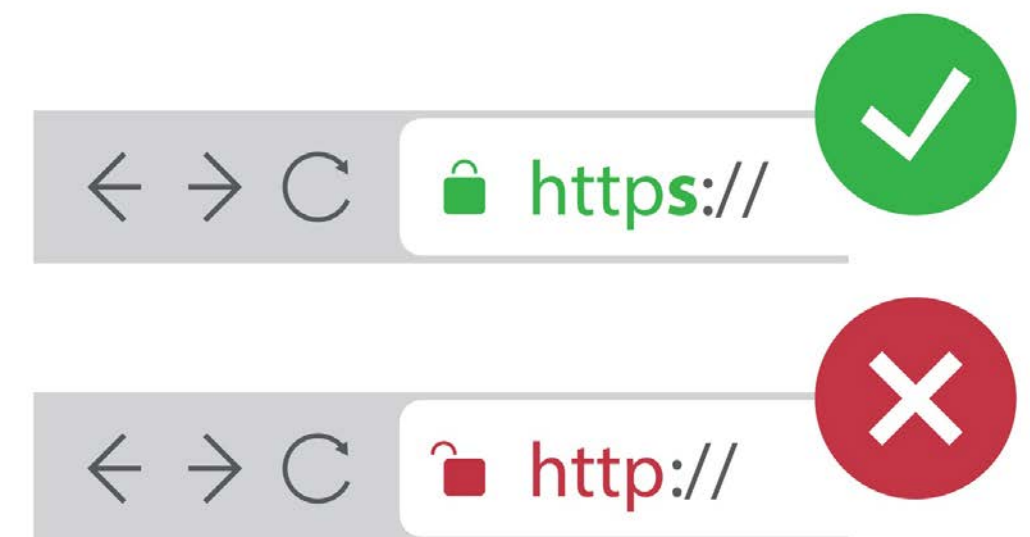


Elaborado especialmente para o curso com imagem © Getty Images.

Construindo o **conceito**

O protocolo HTTPS

- ▶ **HTTPS** (Hypertext Transfer Protocol Secure) é a versão segura do HTTP, o **protocolo** sobre o qual os dados são enviados entre seu navegador e o website que você está conectado.
- ▶ O uso do HTTPS garante que todos os dados transmitidos sejam **criptografados**, o que significa que qualquer informação enviada ou recebida é protegida contra interceptação por terceiros.

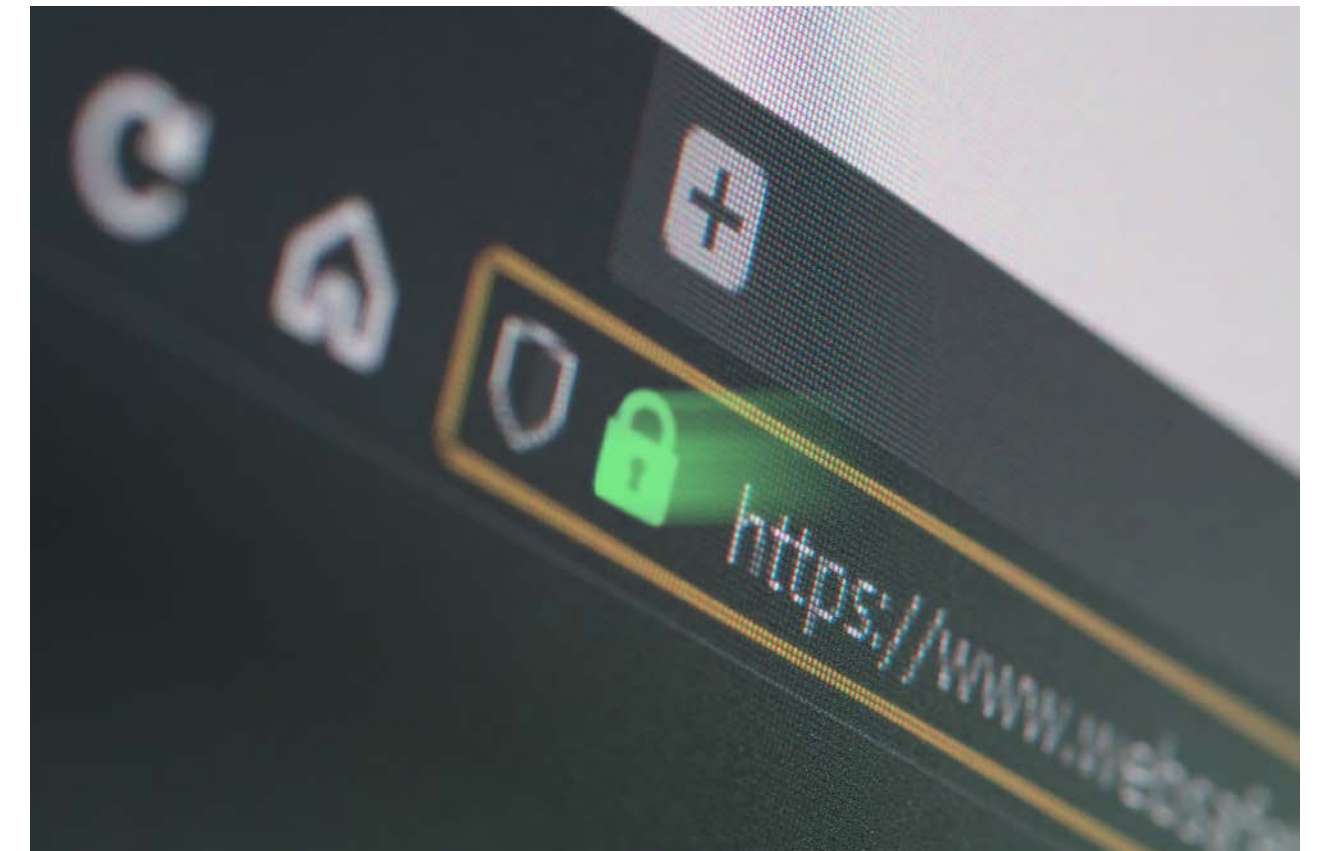


© Getty Images

Construindo o **conceito**

Por que o HTTPS é crucial?

- ▶ O HTTPS é fundamental para proteger a **integridade** e a **confidencialidade** dos dados entre o usuário e o site. Isso é especialmente importante quando realizamos transações bancárias ou compras on-line, em que **informações sensíveis**, como senhas e detalhes do cartão de crédito, são trocadas.
- ▶ Sites que utilizam HTTPS mostram um **ícone de cadeado** na barra de endereços, indicando que a **conexão é segura**.



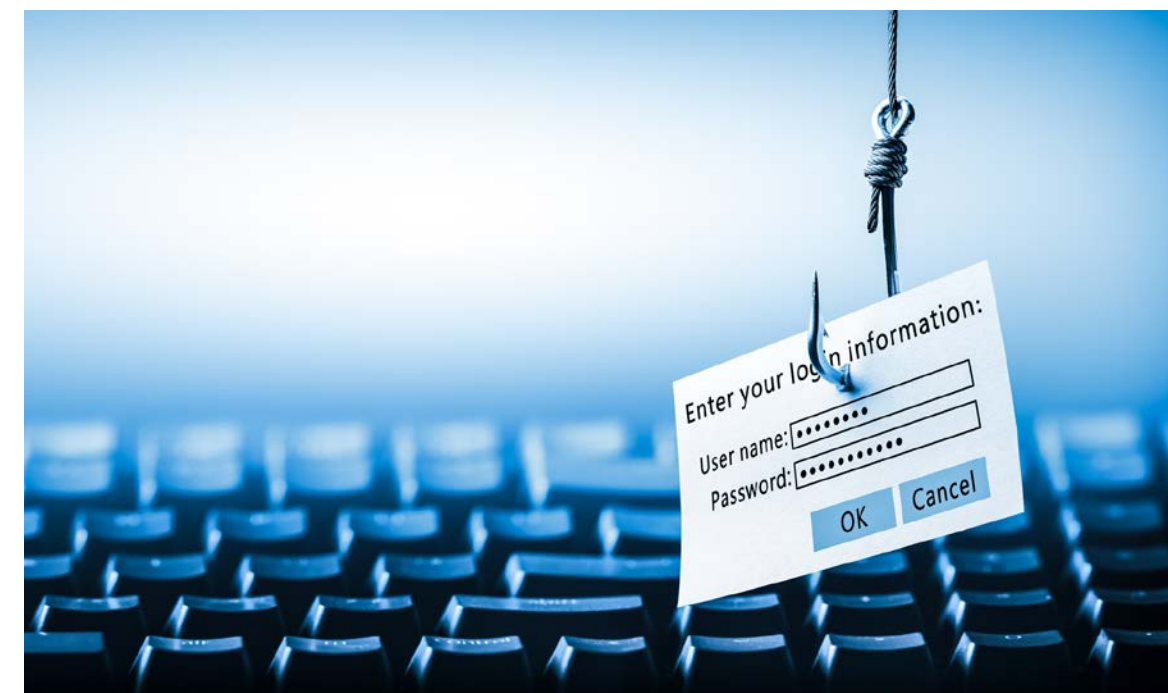
© Getty Images

Mas será que o HTTPS é o suficiente para nos proteger de ataques na internet?

Construindo o **conceito**

O que é *phishing*?

- ▶ **Phishing** é um tipo de **ataque cibernético** que usa **e-mails fraudulentos** ou **websites falsos** para levar você a fornecer informações pessoais, como senhas, números de cartão de crédito e detalhes de identidade.
- ▶ Os ataques de *phishing* frequentemente imitam organizações legítimas e **usam o medo, a urgência** ou **a curiosidade** para persuadir as vítimas a clicar em links maliciosos ou abrir anexos infectados.



© Getty Images

Como se defender do *phishing*?

- ▶ Sempre verifique o **e-mail do remetente** para garantir que a mensagem veio de uma fonte confiável. Desconfie **SEMPRE** de e-mails que solicitam informações confidenciais. Eles podem ser idôneos, mas verifique antes de tirar tal conclusão
- ▶ Evite clicar diretamente em **links em e-mails**. Em vez disso, vá diretamente ao site da empresa digitando o URL na barra de endereços do navegador.



Dica

Sites fraudulentos não costumam ser indexados por buscadores. Se tiver dúvida sobre um remetente ou link, faça buscas na internet.

Por exemplo:

- O domínio “@meubancobr.com” pertence de fato ao meu banco?
- Site oficial da “loja que está fazendo uma superpromoção”.

Construindo o **conceito**

O que são *scams*?

- ▶ **Scams** são **esquemas fraudulentos** executados por **criminosos** na internet com o objetivo de roubar dinheiro ou identidade. Eles podem acontecer por meio de ofertas falsas, “promoções incríveis” ou alertas de segurança enganosos.
- ▶ Esses golpes podem aparecer em **e-mails, mensagens de texto, publicações** em redes sociais ou mesmo por meio de **anúncios** em sites populares.



Curiosidade

Um exemplo clássico desse golpe é o “golpe do príncipe nigeriano”, que recebe esse nome por causa de sua história elaborada, geralmente envolvendo um “príncipe” estrangeiro que está esperando para enviar à vítima uma grande quantia em dinheiro. Na realidade, o golpista está apenas tentando receber dinheiro ou informações bancárias da vítima.

Construindo
o **conceito**

Como evitar *scams*?

- ▶ Nunca forneça informações pessoais ou financeiras em resposta a ofertas que parecem boas demais para ser verdade.
- ▶ Utilize um software de segurança confiável e mantenha-o atualizado.
- ▶ Configure o seu navegador para bloquear *pop-ups*, que muitas vezes são usados por *scammers*.



Vamos
fazer um
quiz

Qual é a principal função do HTTPS?

Acelerar a navegação na internet.

Proteger a transmissão de dados entre o usuário e o site.

Garantir que você não sofra nenhum golpe no site.

Exibir anúncios personalizados.

Vamos
fazer um
quiz

Qual é um sinal comum de um e-mail de *phishing*?

Ofertas de produtos gratuitos.

Solicitações para verificar sua conta.

Links para mudar sua senha.

Todas as opções estão corretas.



Vamos
fazer um
quiz

Como você pode evitar ser vítima de um *scam* na internet?

Ignorando ofertas que parecem boas demais para ser verdade.

Comprando apenas em sites desconhecidos.

Usando senhas fáceis de memorizar com no máximo oito caracteres.

Usando sempre a mesma senha para evitar cair em propostas de redefinição de senha.



© Getty Images

O que nós
**aprendemos
hoje?**

Então ficamos assim...

- 1** Aprendemos que a navegação na internet opera por meio da troca de dados em forma de pacotes, que são pequenas unidades contendo informações e instruções de roteamento;
- 2** Aprendemos sobre a importância do protocolo HTTPS para evitar ataques de interceptação desses pacotes;
- 3** Aprendemos sobre dois outros tipos de ataques digitais, os *phishings* e os *scams*, e como nos proteger deles.

Saiba mais

Já teve a conta de alguma rede social invadida? E seus dados pessoais, você sabe como se proteger do *phishing*, um dos principais golpes digitais?

TUDO sobre prevenção e golpes de phishing: o que você precisa saber. *Kaspersky*, [s.d.].

Disponível em:

<https://www.kaspersky.com.br/resource-center/preemptive-safety/phishing-prevention-tips>. Acesso em: 21 jun. 2024.

Referências da aula

BIG DATA: como a Target descobriu uma gravidez antes da família? *Guide*, 18 fev. 2019. Disponível em: <https://conteudos.guide.com.br/textos/big-data-como-a-target-descobriu-uma-gravidez-antes-da-propria-familia/>. Acesso em: 21 jun. 2024.

MASCARENHAS NETO, P. T.; ARAÚJO, W. J. *Segurança da Informação: uma visão sistêmica para implantação em organizações*. João Pessoa: UFPB, 2019. Disponível em: <http://www.editora.ufpb.br/sistema/press5/index.php/UFPB/catalog/book/209>. Acesso em: 21 jun. 2024.

Identidade visual: Imagens © Getty Images

**Educação
Profissional
Paulista**

Técnico em
**Ciência de
Dados**