7º ANO

Tecnologia e inovação

MATERIAL DIGITAL

Segurança cibernética: práticas para proteção digital - Desinformação online

1º bimestre
Aula 13

Ensino Fundamental:
Anos Finais

start by alura

GOVERNO DO ESTADO DE SÃO PAULO

Conteúdos

- Ameaças digitais: engenharia social e desinformação (fake news);
- Desinformação e manipulação de conteúdo (imagens e áudios);
- Riscos do compartilhamento de dados e imagens na internet.

Objetivos

- Analisar como a engenharia social e a desinformação ameaçam a segurança digital;
- Reconhecer riscos associados à exposição de dados pessoais na internet;
- Propor estratégias de proteção contra golpes que utilizam dados e imagens pessoais.

O que você compartilha?

Analise o perfil fictício da personagem Cody.

VIREM E CONVERSEM

Quais informações do perfil poderiam ser usadas por pessoas mal-intencionadas?

Cody

Pop e K-pop | Escola Start by Alura | ♥ @maria_souza8701 @vovonadir @nando-dboaa

Playlists

Trends & Dancinhas

Edições & Efeitos

Fandom & Celebs

Quando os dados viram uma ameaça

Os dados que divulgamos publicamente online podem ser usados em dois tipos de ameaças digitais:

Engenharia social

Desinformação

Foco no conteúdo

@ Freepik

A **engenharia social** é um método usado para enganar, manipular ou explorar a confiança das pessoas.

É uma forma de ataque sem violência física que busca fazer com que a vítima realize voluntariamente ações prejudiciais a si mesma, como divulgar informações sensíveis ou transferir dinheiro para desconhecidos.

Agência Brasileira de Inteligência

2026_AF_V1

Engenharia social

Na engenharia social, alguém pode ser manipulado por:

1. **Engano**

   Perfil falso de alguém confiável.

2. **Urgência**

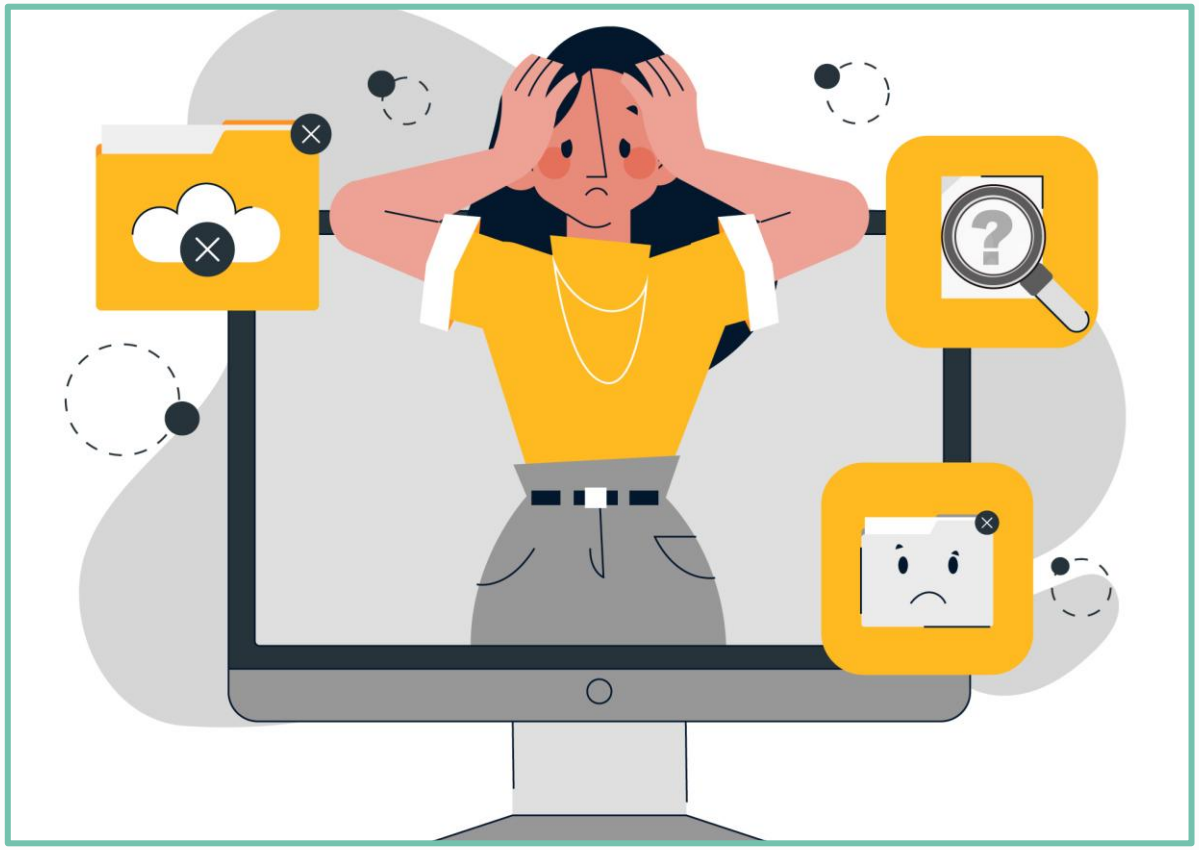
   Pressão para decidir algo rápido.

3. **Autoridade**

   Contato falso de alguém importante.

4. **Curiosidade**

   Textos chamativos.



Desinformação

A desinformação pode também ser chamada de ***fake news*** ou notícia falsa.

Ela ocorre quando textos, imagens, vídeos e/ou áudios são manipulados para enganar alguém.

2026_AF_V1

Como se proteger?

1. **Reflita primeiro, poste depois**:
cuidado com a publicação de dados que podem ser usados e manipulados.

2. **Confira a fonte**:
não divulgue informações pessoais antes de checar se a pessoa ou a empresa do outro lado são verdadeiras.

Na prática

Vamos ajudar outras pessoas a se protegerem?

Em grupos, escolha uma dessas situações:

1. Empresa entra em contato pedindo informações para atualização de cadastro.
2. Oferta com um desconto alto em um produto que você quer.
3. Divulgação de fotos e dados em redes sociais.
4. Mensagem de um conhecido pedindo seus dados.

Na prática

Criem um cartaz sobre esse tema! Ele deve ter:

- Título;
- Apresentação da situação (texto ou imagem);
- Duas estratégias de proteção;
- Frase final de alerta.

© Freepik

Depois, exponha os cartazes na escola e ajude mais pessoas a se prevenir de ameaças digitais!

Encerramento

© Freepik

O que aprendemos hoje?

Nesta aula, aprendemos como dados pessoais podem ser usados e manipulados por outras pessoas.

Qual cuidado você terá a partir de agora ao postar algo online?

Referências

BRASIL. Ministério da Educação. Base Nacional Comum Curricular. **Computação: complemento à BNCC**. Brasília, DF: Ministério da Educação, 2022. Disponível em: https://www.gov.br/mec/pt-br/escolas-conectadas/BNCCComputaoCompletodiagramado.pdf. Acesso em: 7 dez. 2025.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. Cartilha de segurança para internet. **Núcleo de Informação e Coordenação do Ponto BR**, São Paulo, 2012. Disponível em: https://cetic.br/media/docs/publicacoes/1/cartilha-seguranca-internet.pdf. Acesso em: 7 dez. 2025.

LEMOV, Doug. **Aula nota 10 3.0:** 63 técnicas para melhorar a gestão da sala de aula / Doug Lemov; tradução: Daniel Vieira, Sandra Maria Mallmann da Rosa; revisão técnica: Fausta Camargo, Thuinie Daros. 3. ed. Porto Alegre: Penso, 2023.

Referências

ROSENSHINE, B. Principles of instruction: research based strategies thaT all teachers should know. In: **American Educator**, v. 36, n. 1., Washington, 2012. pp. 12-19. Disponível em: https://eric.ed.gov/?id=EJ971753. Acesso em: 7 dez. 2025.

SÃO PAULO (Estado). Secretaria da Educação. **Currículo Paulista:** etapa Ensino Fundamental. São Paulo: Secretaria da Educação, 2019. Disponível em: https://efape.educacao.sp.gov.br/curriculopaulista/wp-content/uploads/2023/02/Curriculo_Paulista-etapas-Educa%C3%A7%C3%A3o-Infantil-e-Ensino-Fundamental-ISBN.pdf. Acesso em: 7 dez. 2025.

Para professores

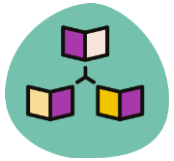
Slide 2

Habilidade:

(EF07CO07) Identificar problemas de segurança cibernética e experimentar formas de proteção.

Slide 3

Tempo: 10 minutos.



Dinâmica de condução: inicie a aula propondo uma dinâmica de análise de um perfil fictício da personagem Cody. O objetivo é que os estudantes identifiquem quais informações disponíveis publicamente no perfil podem ser consideradas sensíveis e usadas por criminosos para aplicar golpes. Essa atividade propõe uma reflexão inicial sobre a importância de refletir antes de publicar algo na internet, o que será aprofundado durante a aula.

Expectativas de respostas: algumas informações que podem ser identificadas como sensíveis são o gosto musical da personagem, que pode ser usado para produzir anúncios direcionados; o nome de uma escola, provavelmente na qual Cody estuda; a menção a outros perfis, provavelmente de pessoas próximas, com os quais um criminoso pode entrar em contato fingindo ser Cody; o destaque “Trends & Dancinhas”, que pode conter vídeos e áudios da personagem; o destaque “Fandom & Celebs”, que pode conter informações específicas sobre gostos pessoais; e até mesmo a foto de perfil pública, que pode ser copiada e usada em um perfil fake.

Slides 4 a 8

Tempo: 15 minutos.

Dinâmica de condução: apresente aos estudantes os conceitos de engenharia social e desinformação. É importante que eles identifiquem que esses são dois tipos de ameaças digitais (em complemento ao malware e phishing, abordados na aula anterior). Durante a explicação, se possível, dê exemplos de casos que envolvem essas ameaças ou pergunte aos estudantes quais casos eles conhecem. Além disso, enfatize quais comportamentos online aumentam o risco de exposição dos nossos dados pessoais e encerre a explicação com as duas principais formas de se prevenir: refletir antes de postar qualquer informação na internet, pois, mesmo que simples e inocente, ela pode ser roubada e usada por criminosos; e nunca divulgar dados pessoais por meio de aplicativos, telefone, mensagens, formulários etc. sem antes conferir se a fonte é confiável e se o destinatário é verídico.

Aprofundamento: assista aos vídeos para saber mais sobre os conceitos de engenharia social e desinformação, além de conhecer exemplos e casos famosos de golpes que utilizaram essas técnicas.

Slides 4 a 8

Link para vídeo

Vídeo do canal **Senai São Paulo** sobre o que é engenharia social, quais os prejuízos que ela causa e como é aplicada.

SENAI SÃO PAULO. Cyber segurança: o que é engenharia social? Disponível em: https://youtu.be/R9RcENv-jo4. Acesso em: 7 dezembro 2025.

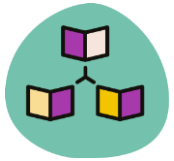
Link para vídeo

Vídeo do canal **Carta Capital** sobre o que é desinformação, como ela pode utilizar mídias reais e manipular seu sentido, além de se aproveitar das emoções dos usuários para se propagar.

CARTACAPITAL. O que são as fake news e quem lucra com elas? Disponível em: https://youtu.be/tCs5_pBXzgI. Acesso em: 7 dezembro 2025.

Slides 9 e 10

Tempo: 25 minutos.



Dinâmica de condução: inicie a atividade dividindo a sala em quatro grupos. Em seguida, sorteie ou peça que cada time escolha uma das situações propostas. Feito isso, explique que eles devem produzir um cartaz de conscientização, que será exposto para a comunidade escolar, com dicas de proteção contra a ameaça digital em questão. Os cartazes podem utilizar diferentes materiais, como variados tipos de canetas, imagens, colagens, desenhos etc. Se não for possível acesso aos materiais, proponha que cada um faça, individualmente, a atividade em uma folha de sulfite, como um flyer, para entregar para a família e ajudar na conscientização dentro de casa.

Slides 9 e 10

Expectativas de respostas:

- **Situação 1:** empresa entra em contato pedindo informações para atualização de cadastro.

Título: O perigo se disfarça.

Situação: Imagine que você recebe uma mensagem ou ligação de uma empresa conhecida. A pessoa do outro lado é muito educada e pede alguns dados seus para atualizar seu cadastro. O que você faz?

Estratégias de proteção: Nunca informe dados pessoais por mensagem ou ligação; entre em contato com a empresa pelos canais oficiais.

Frase final: Se pedir seus dados, desconfie!

- **Situação 2:** oferta com um desconto alto em um produto que você quer.

Título: NÃO clique aqui

Situação: “TV 50” com 50% de desconto! SÓ HOJE: compre a TV e leve um videogame com 80% de desconto. Últimas unidades disponíveis. Clique aqui.”

Estratégias de proteção: Desconfie de ofertas muito abaixo do preço normal; não clique em links sem antes confirmar se o site é oficial e confiável.

Frase final: Quando a esmola é grande, o santo desconfia!

Slides 9 e 10

Expectativas de respostas:

- **Situação 3:** divulgação de fotos e dados em redes sociais.

Título: O que você posta nas suas redes?

Situação: desenho de um perfil público em rede social contendo fotos com familiares e amigos, localização e WhatsApp.

Estratégias de proteção: Evite postar fotos com dados pessoais, marcando pessoas próximas ou com localização; de preferência, use perfis privados.

Frase final: Pense primeiro, poste depois!

- **Situação 4:** mensagem de um conhecido pedindo seus dados.

Título: Nem tudo é o que parece

Situação: Uma mensagem chega no seu celular. O perfil tem a foto e o nome de uma pessoa que você conhece e ela pede alguma informação pessoal, senha ou até dinheiro.

Estratégias de proteção: Entre em contato com a pessoa por outro meio antes de responder; nunca envie dados pessoais por mensagem.

Frase final: Confirme antes de confiar!

GOVERNO DO ESTADO
DE SÃO PAULO

start
by alura

2026_AF_V1