7º ANO

Tecnologia e inovação

MATERIAL DIGITAL

Segurança cibernética: práticas para proteção digital - Ameaças digitais

1º bimestre
Aula 12

Ensino Fundamental:
Anos Finais

start by alura

GOVERNO DO ESTADO DE SÃO PAULO

Conteúdos

- Tipos de ameaças digitais: malware e phishing;
- Estratégias utilizadas por golpistas para obter dados pessoais;
- Dicas práticas de prevenção e segurança na internet.

Objetivos

- Analisar como dados pessoais podem ser usados em golpes digitais;
- Relacionar ameaças cibernéticas a comportamentos inseguros online;
- Identificar formas seguras de agir frente a mensagens e links suspeitos.

2026_AF_V1

VIREM E CONVERSEM

Ameaça digital

Todos os dias, milhares de golpes são aplicados nos meios digitais.

Você conhece alguém que já caiu em um golpe pela internet? Como aconteceu?

Brasil é vice-campeão em ataques cibernéticos, com 1.379 golpes por minuto, aponta estudo

Especialista orienta que além de tecnologia, usuários devem investir em capacitação

João Nakamura, da CNN, em São Paulo

30/10/24 às 08:15 | Atualizado 30/10/24 às 08:15

Manchete de notícia publicada pela CNN Brasil. Disponível em: https://www.cnnbrasil.com.br/economia/negocios/brasil-e-vice-campeao-em-ataques-ciberneticos-com-1-379-golpes-por-minuto-aponta-estudo. Acesso em: 17 dez. 2025.

Na prática

Assista ao vídeo a seguir para conhecer um tipo de golpe digital.

Link para vídeo

Vídeo do canal **Jornalismo TV Cultura** explicando como o golpe da Mão Fantasma acontece.

JORNALISMO TV CULTURA. Golpe da Mão Fantasma: hackers instalam vírus em celular e roubam dinheiro através do PIX. Disponível em: https://youtu.be/JKegkQYBgK0. Acesso em: 17 dezembro 2025.

Na prática

TODO MUNDO ESCREVE

Agora, responda em seu caderno:

1. Quais golpes são citados no início do vídeo?

2. Como acontece o golpe da Mão Fantasma?

3. Quais dados pessoais são acessados pelos criminosos?

4. Quais estratégias são usadas para enganar as vítimas?

5. O que as pessoas podem fazem para se proteger?

Para onde vão nossos dados?

Muitos desses golpes acontecem quando dados pessoais ficam disponíveis na internet ou são acessados por criminosos.

Dois tipos de ameaças comuns são:

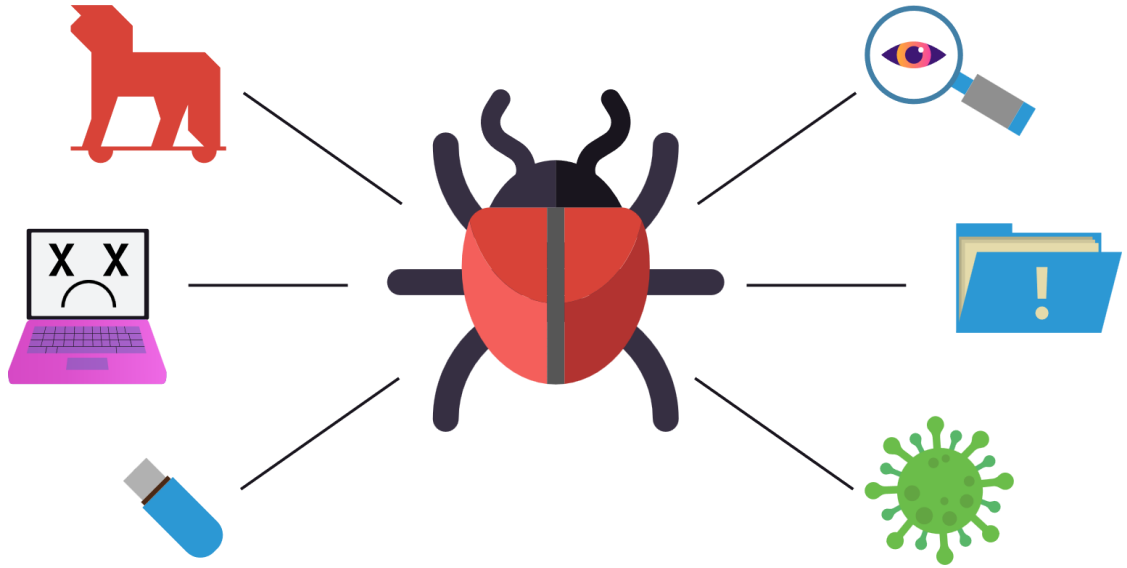
Malware

Phishing

O que é Malware?

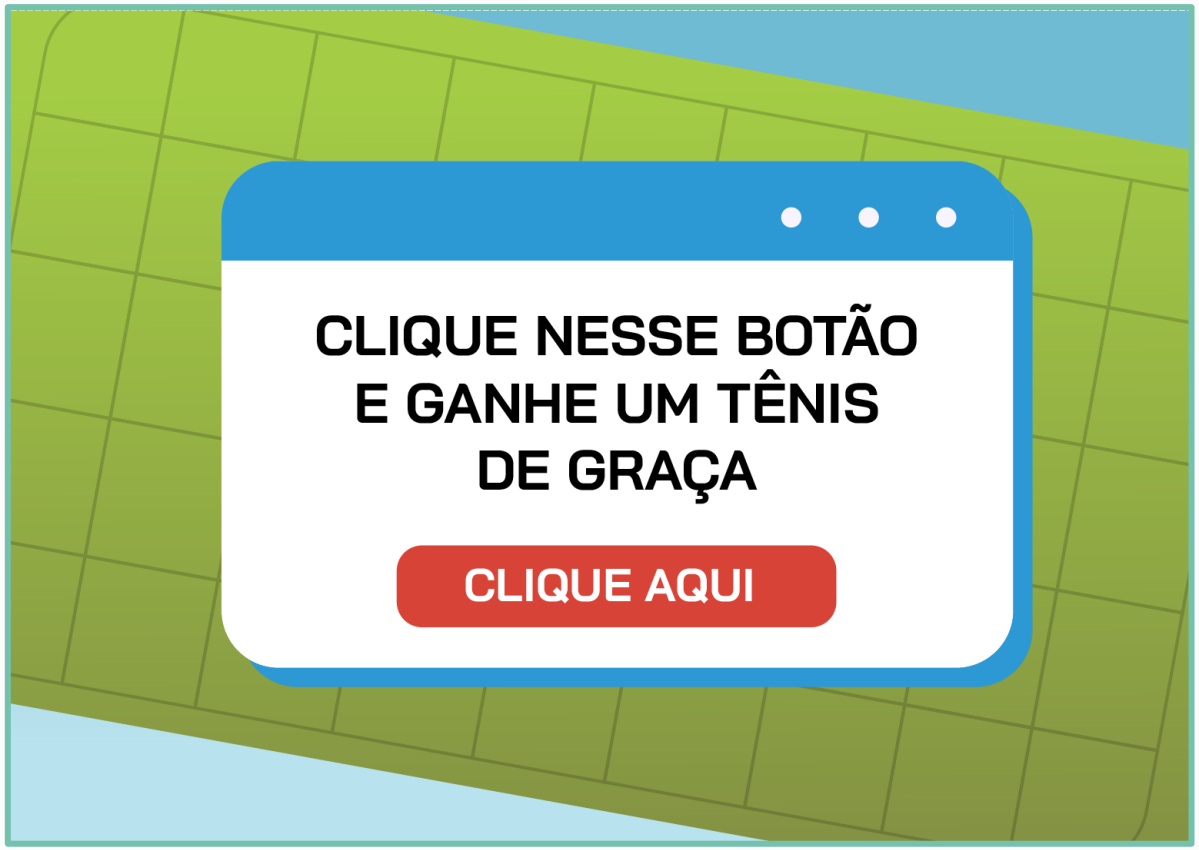
Malware é um **software malicioso** que invade dispositivos para instalar vírus ou roubar informações.

Ele se **infiltra** por links suspeitos, downloads, sites falsos ou aplicativos não confiáveis.



FICA A DICA

O malware pode aparecer em qualquer aparelho conectado à internet, como Smart TVs ou videogames.



Exemplo de uso do phishing.

Pescaria digital?

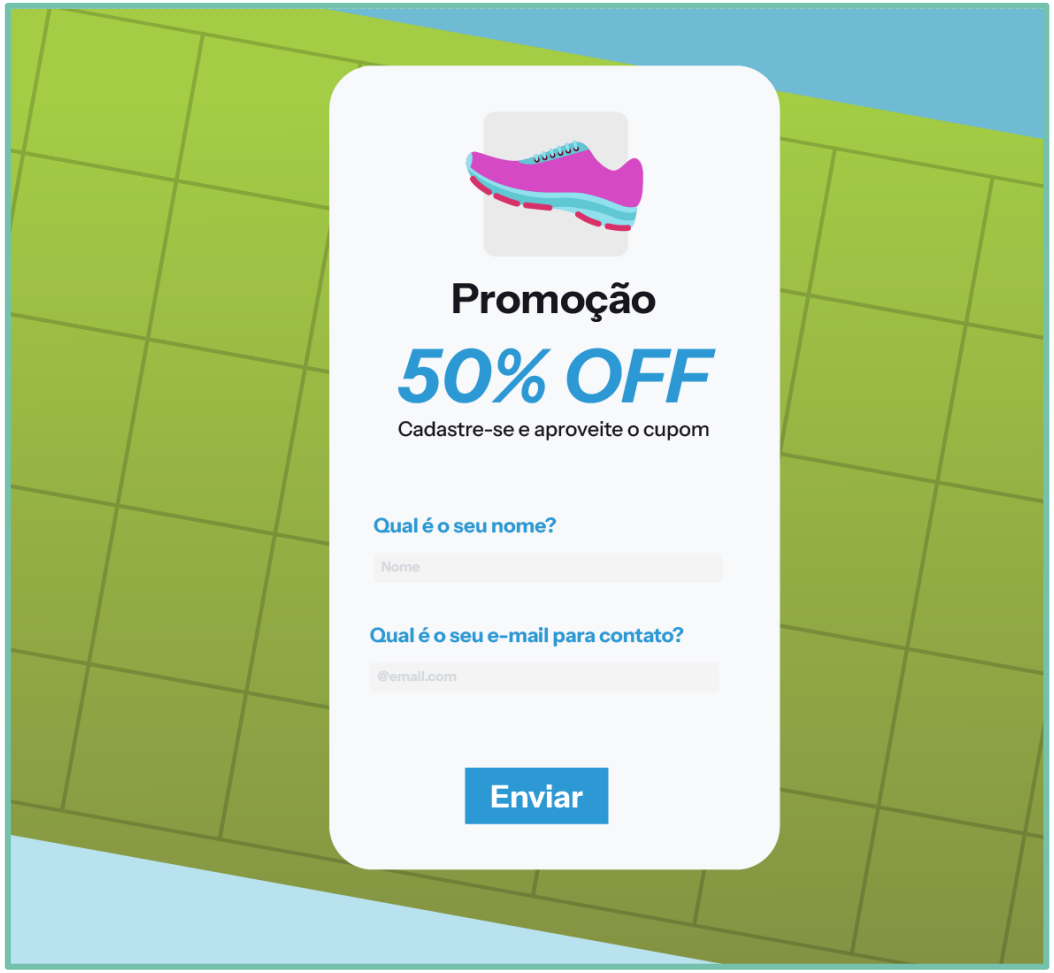
Phishing vem da palavra inglesa *fishing*, que significa pescar.

Nele, os criminosos usam mensagens chamativas para atrair (pescar) suas vítimas.

Foco no conteúdo

Ao clicar na mensagem, o usuário precisa informar alguns dados para receber o prêmio ou o desconto.

Pensando ser uma página verdadeira, a vítima divulga seus dados pessoais sem perceber.



Nunca informe dados pessoais na internet sem antes conferir se a fonte é verdadeira e confiável.

Como se proteger?

1. Não clicar em links desconhecidos.
2. Sempre verificar se a fonte é confiável.
3. Não baixar aplicativos fora de lojas oficiais.
4. Não divulgar dados pessoais online.
5. Desconfiar de prêmios e descontos surreais.

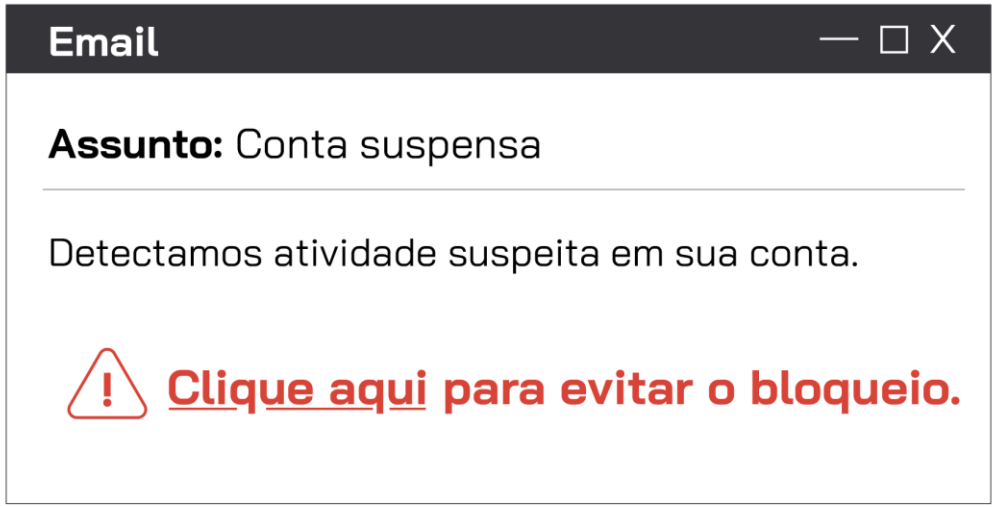
Na prática

O que você faria?

VIREM E CONVERSEM

Em grupos, analisem um dos casos a seguir. Depois, respondam às perguntas e apresentem as conclusões do grupo para a turma.

E-mail



Janela de aviso em site

Na prática

VIREM E CONVERSEM

Mensagem de amigo em rede social

Anúncio em um jogo de celular

Na prática

COM SUAS PALAVRAS

1. Você clicaria nessa mensagem? Por quê?
2. O que poderia ser feito para se proteger de um golpe?
3. Quais dados pessoais estão envolvidos?
4. Quais comportamentos podem colocar em risco esses dados?
5. Qual técnica é usada para chamar a atenção dos usuários?
6. Que tipo de ameaça digital está envolvida?

Encerramento

Transformando conhecimento em ação

Hoje, aprendemos sobre alguns tipos de ameaças digitais, como identificá-las e como se prevenir.

A partir disso, o que você mudaria no seu comportamento online para se proteger dessas ameaças?

2026_AF_V1

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. Códigos Maliciosos. **Núcleo de Informação e Coordenação do Ponto BR**, São Paulo, 2023. Disponível em: https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf. Acesso em: 7 dez. 2025.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. Phishing e outros golpes. **Núcleo de Informação e Coordenação do Ponto BR**, São Paulo, 2022. Disponível em: https://cartilha.cert.br/fasciculos/phishing-golpes/fasciculo-phishing-golpes.pdf. Acesso em: 7 dez. 2025.

Referências

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.

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: 5 minutos.

Dinâmica de condução: inicie a aula lendo a manchete da notícia publicada pela CNN Brasil. Em seguida, incentive os estudantes a contarem casos de golpes digitais que eles viram na mídia ou aconteceram com algum conhecido. Tanto nesta atividade quanto na proposta do slide seguinte, é importante mediar a discussão para que as vítimas não sejam culpabilizadas, mas sim acolhidas com empatia. Mencione que qualquer pessoa pode estar sujeita a cair em um golpe, pois são usadas mecânicas de falsificação muitas vezes difíceis de identificar e até mesmo estratégias emocionais para enganar a vítima, como fingir ser um familiar precisando de ajuda.

Expectativas de respostas: as respostas irão variar e dependerão do repertório dos estudantes. Alguns golpes que podem ser citados são: alguém entrar em contato via SMS ou WhatsApp se passando por um conhecido e pedindo dinheiro; produtos comprados e não entregues; roubos de dados pessoais; contas de redes sociais invadidas; cobranças indevidas; cartões de crédito clonados; entre outros.

2026_AF_V1

Slides 4 e 5

Tempo: 15 minutos.

Dinâmica de condução: apresente o vídeo sobre o golpe da Mão Fantasma até a minutagem 2:02 para que os estudantes analisem os casos e criem hipóteses por meio das perguntas sugeridas. Em seguida, peça para que eles as respondam no caderno. Feito isso, reproduza o restante do vídeo que traz informações de especialistas sobre como se proteger desse golpe.

Slides 4 e 5

Expectativas de respostas:

1. Golpista finge ser outra pessoa ao usar a foto dela em uma rede social; golpe realizado por meio de link divulgado no TikTok; recebimento de proposta de trabalho falsa; golpe bancário; transferência de valores que vão para contas desconhecidas (do início do vídeo até a minutagem 0:46).
2. Um vírus é instalado no computador ou celular do usuário quando ele clica em um link, que pode ser divulgado em jogos, falsa notificação bancária, entre outros aplicativos. A partir disso, o criminoso consegue acesso total ao aparelho, sendo capaz de redirecionar transações bancárias (de 0:47 a 1:43).
3. Como o golpista consegue controlar o celular da vítima, ele pode ter acesso a vários dados pessoais, como documentos, endereço, telefone, dados bancários, cartão de crédito, fotos e outras informações.
4. Oferecimento de prêmios e link para baixar o aplicativo falso enviado por WhatsApp ou e-mail se passando por alguma instituição ou loja oficial (de 1:44 a 2:02).
5. Nesta pergunta, espera-se que os estudantes criem hipóteses que, posteriormente, podem ser confirmadas com o restante do vídeo. O ponto principal é não clicar em links desconhecidos, não fazer o download de aplicativos fora de lojas oficiais ou publicados por contas desconhecidas, sempre checar a origem do contato e desconfiar de ofertas e promoções surreais (de 2:02 até o final).

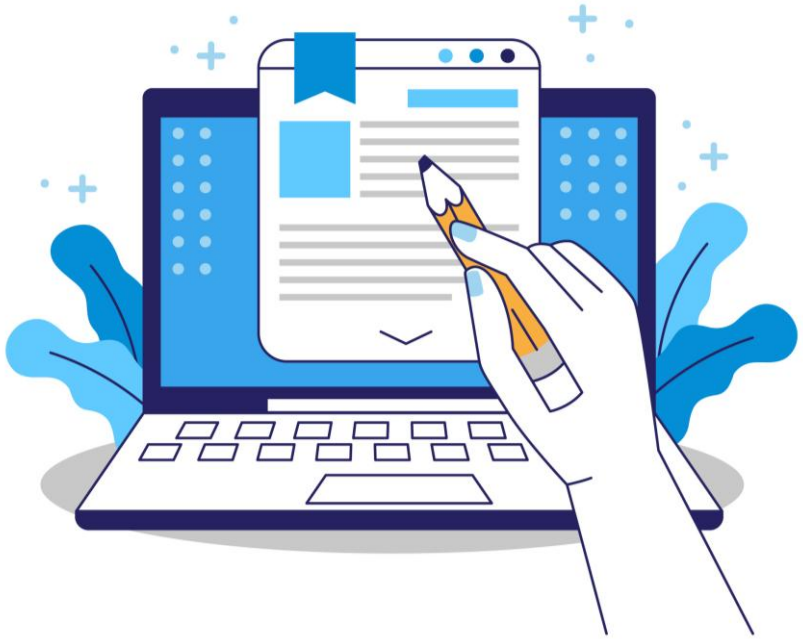
Slides 6 a 10

Tempo: 10 minutos.

Dinâmica de condução: apresente aos estudantes os dois tipos de ameaças digitais e como são usadas para enganar as vítimas. Traga exemplos para ilustrar os conceitos: o golpe da Mão Fantasma, citado na seção Para começar, é um exemplo de uso de malware; e as imagens dos slides 8 e 9 são exemplos de phishing.

Aprofundamento: leia o artigo para conhecer os diferentes tipos de malware e exemplos de seu uso.

Link para PDF

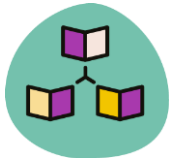


Acesse o artigo clicando aqui.

KASPERSKY. Quais são os diferentes tipos de Malware? **Kaspersky**. Disponível em: https://www.kaspersky.com.br/resource-center/threats/types-of-malware. Acesso em: 17 dez. 2025.

Slides 11 a 13

Tempo: 20 minutos.



Dinâmica de condução: esta atividade reforça o conteúdo trabalhado em sala e ajuda os estudantes a revisarem o que aprenderam de forma criativa e colaborativa.

Primeiro, divida a turma em grupos: em caso de uma turma menor, sugere-se quatro grupos para que cada um analise uma situação. Em turmas maiores, divida em oito grupos de modo que cada situação seja analisada por dois grupos diferentes.

Em seguida, o grupo deve analisar o cenário atribuído a ele com base nas perguntas norteadoras do slide 13. Não é necessário o registro escrito das respostas. O mais importante aqui é o debate entre a turma. Porém, pode-se sugerir aos estudantes que anotem as respostas em tópicos simples e curtos para não esquecer o que discutiram. Ao final, um representante de cada grupo relata brevemente a conclusão do seu time. Neste momento, incentive o estudante a fazer um resumo da discussão considerando as perguntas norteadoras em vez de responder diretamente cada uma.

Slides 11 a 13

Expectativas de respostas: em todas as situações, espera-se que o estudante relate que seria necessário manter um comportamento seguro antes de clicar na mensagem. Para isso, pode-se verificar a fonte ou destinatário ou entrar em contato com a instituição, empresa ou pessoa por outro canal para verificar se o pedido ou prêmio é verdadeiro.

Em cada situação, vários dados pessoais poderiam ser roubados, como documentos, endereço, dados bancários, senhas, fotos, vídeos, conversas, informações pessoais etc.

O principal comportamento que colocaria em risco esses dados seria clicar em links, botões, divulgar seus dados pessoais para outra pessoa ou preencher formulários com essas informações.

Em todos os casos, a mensagem apela para o sentimento de urgência da vítima, mobilizando sua preocupação (e-mail), desejo (janela de aviso e anúncio) ou confiança (mensagem de amigo).

Por fim, e-mail usa a técnica malware; janela de aviso e mensagem usam o phishing; e o anúncio pode usar as duas técnicas.

GOVERNO DO ESTADO
DE SÃO PAULO

start
by alura

2026_AF_V1