

III BNCC COMPUTAÇÃO · 9º ANO EF09C004

COMO AGEM OS ATAQUES

Malwares e outros ataques cibernéticos

Mundo digital

Segurança cibernética

Aula expositiva · 30 min

COMO UM PROGRAMA INVADIR UM CELULAR SEM NINGUÉM PERCEBER?

Pense antes de passar o slide.

O QUE VAMOS APRENDER

EF09C004 SEGURANÇA CIBERNÉTICA

Compreender o funcionamento de malwares e outros ataques cibernéticos.

Ao final da aula, você vai conseguir:

- diferenciar tipos de malware;
- explicar como um ataque começa;
- escolher defesas para cada tipo de ataque.

TIPOS DE **MALWARE**

Vírus

se gruda em arquivos e se espalha quando eles são abertos

Cavalo de Troia

parece um app legal, mas esconde o ataque

Ransomware

sequestra os arquivos e pede resgate

Spyware

espiona o que você digita e acessa

A PORTA DE **ENTRADA**

A maioria dos ataques começa com uma pessoa: um clique num link, um app pirata, um anexo.

Por isso se diz que o elo mais fraco da segurança costuma ser o **ser humano**.

OUTROS ATAQUES

Phishing

página falsa que imita
banco ou rede social

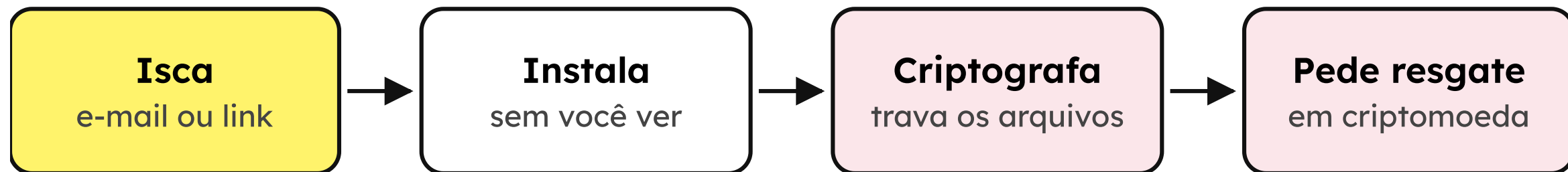
Engenharia social

enganar com conversa,
pressa ou medo

Negação de serviço

milhares de acessos ao
mesmo tempo derrubam
um site

COMO AGE UM **RANSOMWARE**



Melhor defesa: **cópia de segurança** atualizada. Pagar não garante nada.

DEFESAS

- Atualizações do sistema e dos apps: elas corrigem falhas.
- Antivírus e apps só da loja oficial.
- Cópia de segurança dos arquivos importantes.
- Desconfiar de anexos e links inesperados.
- Senhas fortes e verificação em duas etapas.

HACKER É **CRIMINOSO** ?

Nem sempre. Hackers éticos são contratados para achar falhas antes dos criminosos.

Invadir sistemas sem autorização é **crime** no Brasil (Lei 12.737/2012, conhecida como Lei Carolina Dieckmann).

ATIVIDADE: **ANÁLISE DE INCIDENTE**

7 MIN

1. Caso fictício: os computadores da escola travaram e apareceu um pedido de resgate.
2. Em grupos, descubram a porta de entrada provável.
3. Digam que tipo de malware foi.
4. Proponham 3 defesas que teriam evitado ou reduzido o estrago.

CONFIRA: RESPONDA RÁPIDO **4 MIN**

1. O que faz um ransomware?
2. O que é um cavalo de Troia?
3. Por que atualizar o sistema protege?

PARA **LEVAR**

- Malwares: vírus, cavalo de Troia, ransomware, spyware.
- A porta de entrada costuma ser um clique.
- Atualizar, desconfiar e ter cópia de segurança são as melhores defesas.

Próximo passo: criptografia (EF09CO05).

ROTEIRO DO PROFESSOR • 30 MIN

0-3 min	Abertura	Pergunte se alguém já teve o celular com vírus ou propaganda estranha.
3-5 min	Objetivos	Leia a habilidade e os objetivos em voz alta.
5-17 min	Explicação	Tipos de malware, porta de entrada, ataques, ransomware, defesas e lei (slides 4 a 9).
17-24 min	Atividade	Análise de incidente com o caso fictício da escola.
24-28 min	Confira	Perguntas rápidas: respostas no caderno ou em voz alta.
28-30 min	Fechamento	Retome os três pontos do “Para levar”.

Respostas do “Confira”: 1. trava (criptografa) os arquivos e pede resgate. 2. um programa que parece útil, mas esconde código malicioso. 3. as atualizações corrigem falhas usadas pelos ataques.