







# O que é malware?

Malware, abreviação de "software malicioso", é um termo genérico que se refere a programas indesejados ou código prejudicial projetado para se infiltrar em um sistema de computador sem o conhecimento ou consentimento do usuário.



# Tipos de malware

-  **Vírus**  
Um tipo de malware que se anexa a um arquivo ou programa e se espalha quando o arquivo ou programa é executado.
-  **Ransomware**  
Malware que criptografa os arquivos de uma vítima e exige pagamento para descriptografá-los.
-  **Cavalos de Troia**  
Malware disfarçado como software legítimo, muitas vezes usado para roubar informações confidenciais.

# Tipos de malware



## Worms

Um tipo de malware que se propaga automaticamente entre computadores, sem necessitar se anexar a um arquivo ou programa específico.



## Spyware

Um tipo de software malicioso que é instalado em um computador sem o conhecimento do usuário, com o objetivo de monitorar atividades, coletar informações pessoais ou dados de navegação e enviá-los a terceiros.



## backdoor

Um método de acesso remoto a um computador ou rede que foi intencionalmente criado ou explorado por um atacante, permitindo o controle ou a obtenção de dados sem o conhecimento ou consentimento do usuário.

# Como o malware se espalha

1

## E-mails de Phishing

Enganando os usuários para clicarem em links ou baixarem anexos maliciosos.

2

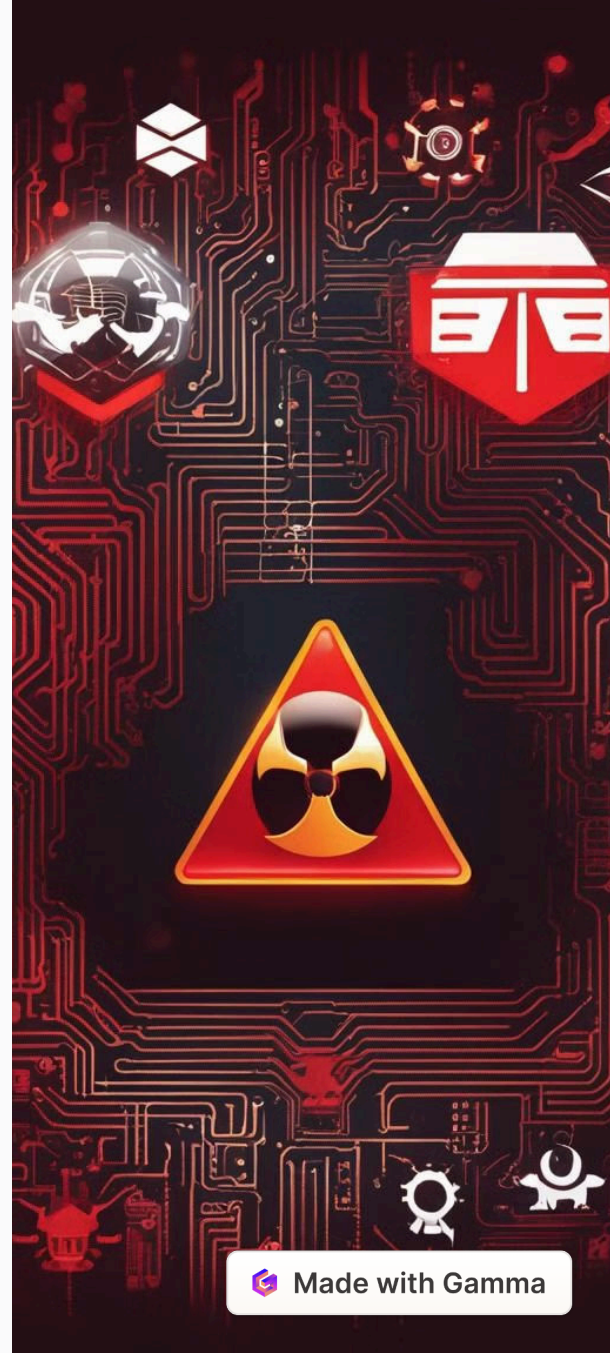
## Exploração de Vulnerabilidades

Aproveitando brechas de segurança em sistemas desatualizados ou mal configurados.

3

## Dispositivos USB Infetados

Transferindo malware quando dispositivos USB contaminados são conectados a um computador.





# Impactos do malware

## Perda de Dados

O malware pode corromper, destruir ou roubar dados confidenciais, resultando em perda financeira ou danos à reputação.

## Interrupção nos Negócios

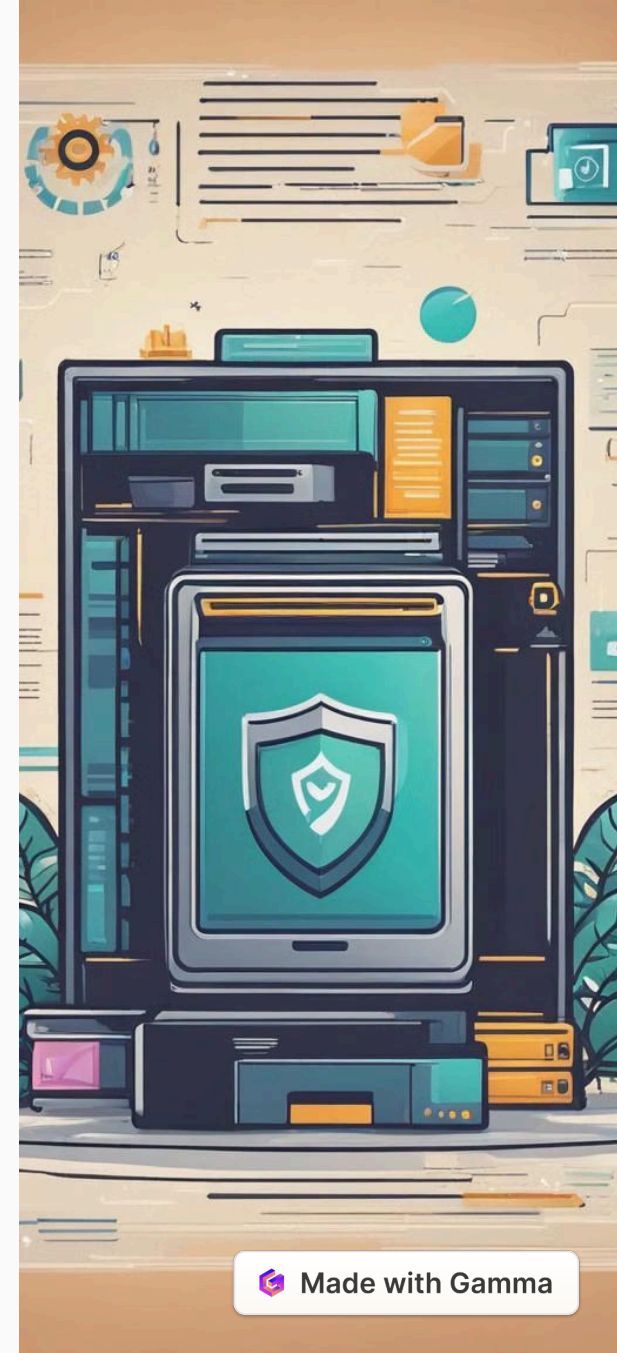
Ataques de malware podem paralisar operações comerciais, causando prejuízos financeiros significativos e impactos na produtividade.

## Riscos à Segurança

O malware pode abrir brechas de segurança que permitem acesso não autorizado a sistemas, criando potenciais riscos à privacidade e conformidade regulamentar.

# Como se proteger contra malware

- 1** Atualize Software Regularmente  
Corrija vulnerabilidades e fortaleça a segurança do sistema.
- 2** Use Antivírus e Antimalware  
Instale e mantenha software de segurança atualizado para detectar e remover ameaças.
- 3** Treinamento em Conscientização de Segurança  
Eduque os funcionários sobre práticas seguras online e como identificar ameaças potenciais.



# Ferramentas de segurança



## Firewall

Monitora e controla o tráfego de rede, impedindo acessos não autorizados.



## Encriptação

Protege dados confidenciais através de codificação, dificultando o acesso não autorizado.



## Autenticação de Dois Fatores

Fornece camadas adicionais de segurança ao exigir múltiplos métodos de autenticação.

# Exemplos de ataques de malware

## WannaCry

Ransomware que se espalhou globalmente, impactando organizações em todo o mundo.

## NotPetya

Malware destruidor disfarçado como ransomware, paralisando empresas e infraestruturas críticas.

## Stuxnet

Malware projetado para atacar sistemas de controle industrial, causando danos substanciais.



# Conclusão e dicas finais

90%

Atualizações Críticas

Realize atualizações de software críticas para corrigir vulnerabilidades conhecidas.

2FA

Autenticação de 2 Fatores

Implemente autenticação de dois fatores para proteger contas contra acessos não autorizados.

Backup

Backup Regular

Realize backups regulares para evitar perda de dados em caso de ataque de malware.

24/7

Vigilância 24/7

Utilize monitoramento contínuo para identificar possíveis ameaças e ataques em tempo real.