

Definição

- Um vírus de computador é um programa malicioso criado para alterar o funcionamento de um computador e se propagar para outros sistemas. Ele se insere ou anexa a programas ou documentos legítimos, muitas vezes usando macros, para executar seu código.

Funcionamento

- Os vírus de computador podem ser divididos em duas categorias:
 - Ativação imediata: Alguns vírus começam a infectar e se replicar assim que entram em um computador.
 - Dormentes: Outros vírus permanecem inativos, esperando serem acionados quando você executa um código sem perceber.

Proteção

Para se proteger contra vírus de computador, considere o seguinte:

- Software antivírus: Use um software antivírus poderoso para detectar e remover vírus.
- Evite fontes suspeitas: Não clique em links ou baixe arquivos de fontes não confiáveis.
- Atualizações regulares: Mantenha seu sistema operacional e programas atualizados para corrigir vulnerabilidades.
- Backup: Faça backups regulares para proteger seus dados contra perda por vírus

vírus computador

Tipos de Vírus

Existem vários tipos de vírus de computador, cada um com características específicas:

- Vírus de arquivo: Anexam-se a arquivos executáveis e se espalham quando esses arquivos são abertos.
- Vírus de macro: Escritos em linguagens de macro (como VBA) e geralmente afetam aplicativos como Microsoft Word e Excel.
- Vírus de boot: Infectam setores de inicialização de discos e mídias removíveis.
- Vírus de script: Escritos em linguagens de script (como JavaScript) e podem se espalhar por meio de páginas da web.
- Vírus de rede: Propagam-se por redes e sistemas conectados.

Impacto dos Vírus:

- Os vírus de computador podem causar:
 - Perda de dados: Arquivos corrompidos ou excluídos.
 - Roubo de informações: Senhas, dados bancários, etc.
 - Danos financeiros: Ransomware exige pagamentos.
 - Interrupção de serviços: Sistemas inoperantes.
 - Espionagem: Monitoramento não autorizado.
 - Reputação prejudicada: Empresas e indivíduos afetados.