CARTILHA:

CÓDIGOS MALICIOSOS

Segurança da Informação

Introdução

Códigos maliciosos são ferramentas usadas por cibercriminosos para golpes, ataques e envio de spam.

Prevenção é a Chave.

Prevenir a infecção inicial é crucial. Nem sempre é possível reverter as ações de malware ou recuperar dados perdidos.

Antivírus – A Primeira Linha de Defesa.

01 Antivírus (antimalware) são ferramentas essenciais para detectar, prevenir e remover malware.

02 Não se limitam apenas a vírus, mas também abordam outros tipos de códigos maliciosos.

03 Escolher um antivírus adequado às suas necessidades e mantê-lo atualizado é fundamental.

Atualização de Sistemas e Aplicativos

O QUE FAZER?

Manter seus sistemas e aplicativos atualizados ajuda a evitar vulnerabilidades exploradas por códigos maliciosos.

Ative atualizações automáticas sempre que possível para garantir que você esteja sempre protegido.

Cautela ao Clicar em Links

01 Evite clicar em links suspeitos, especialmente aqueles de fontes desconhecidas ou não confiáveis.

02 Desconfie de mensagens recebidas, mesmo que aparentemente provenham de contatos conhecidos.

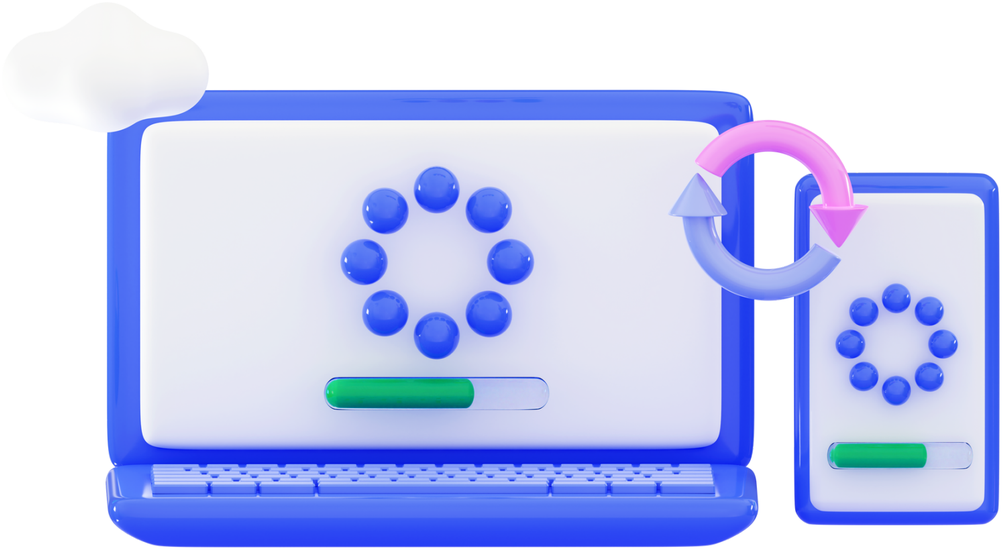
03 Verifique anexos de e-mail com um antivírus antes de abrir

Instalação de Aplicativos

FIQUE DE OLHO

Baixe aplicativos apenas de lojas oficiais e evite instalar aplicativos de fontes desconhecidas ou suspeitas.

Verifique o nome do aplicativo e o desenvolvedor antes de instalar.



Autenticação Forte:

01 Use autenticação em duas etapas sempre que possível para proteger suas contas.

02 Evite repetir senhas e armazene-as de forma segura.

03 Altere imediatamente as senhas se suspeitar de comprometimento ou uso não autorizado.

Realização de Backup

NÃO SE ESQUEÇA

Faça cópias de segurança regulares dos seus dados para evitar perdas devido a códigos maliciosos, como ransomware.

Programe backups automáticos sempre que possível.

Ação Rápida em Caso de Suspeita

01 Se suspeitar de infecção por malware, aja rapidamente usando um antivírus ou outras ferramentas de remoção.

02 Reinicie o dispositivo como uma possível solução.

03 Se necessário, reinstale o sistema ou restaure as configurações de fábrica

Uso da Conta de Administrador

NÃO SE ARRISQUE

Evite usar a conta de administrador para atividades cotidianas.

Use a conta de administrador apenas quando necessário e retorne à conta padrão quando não precisar de privilégios elevados.

TIPOS DE AMEAÇAS

Remote Access Trojan (RAT): Fornece ao invasor controle total sobre o dispositivo infectado. Uma vez instalado, o invasor pode acessar, modificar e deletar arquivos, entre outras atividades invasivas.

WORM: Se replica para se espalhar para outros computadores, explorando vulnerabilidades na rede.

Bot Zumbi e Botnet: Bot Zumbi é um dispositivo comprometido controlado por um invasor. Botnet é uma rede de bots zumbis usados para atividades maliciosas em massa.

Rootkit: Conjunto de softwares que permite acesso não autorizado ao nível do sistema operacional, escondendo-se no sistema para proporcionar acesso contínuo ao invasor.

Scareware: Engana usuários fazendo-os acreditar que estão comprometidos ou infectados, apresentando alertas falsos pedindo que compre ou baixe software prejudicial.

Ransomware: Criptografa arquivos do usuário, tornando-os inacessíveis e exigindo pagamento para descriptografar os arquivos.

Adware: Exibe ou baixa material publicitário automaticamente. Pode ser benéfico ou malicioso.

Alunos: Carolina Cruz e Augusto Amorim
Professor: Edgar Gurgel
Disciplina: Segurança da Informação