Vermes, Vírus e outros Códigos Maliciosos

Como evitá-los e usar a Internet com mais Segurança

BRUNO@CALHEIRA.COM

Os computadores estão tão presentes no nosso dia-a-dia, que é muito difícil imaginar como seria nossa rotina sem eles.

Usamos *smartphones, tablets, notebooks* e uma infinidade de *softwares* para nos ajudar a comunicar, divertir, locomover, comprar, trabalhar...

Mas, assim como na vida *off-line*, o universo dos computadores possui uma série de perigos. Neste e-book aprenderemos sobre ***Códigos Maliciosos*** e veremos algumas dicas de como nos protegermos deles.

Boa leitura!

Bruno Calheira
Consultor Web

calheira.com

O que são *Códigos Maliciosos*?

São **programas de computador** desenvolvidos para **causar danos** ou **promover atividades ilegais** no equipamento infectado (notebooks, tablets, smartphones, roteadores, ou qualquer outro aparelho computacional). Também são conhecidos como Pragas Virtuais, *Malwares* ou Vírus de Computador.

bruno@calheira.com

Mesmo que você não use o seu equipamento para trabalhar ou realizar transações financeiras, é preciso mantê-lo seguro. Ele está repleto de recursos e informações valiosas para você e também para um potencial invasor.

Imagine se você perdesse todas as suas fotos e contatos armazenadas no seu celular, ou que alguém utilizasse o seu computador para guardar fotos de pedofilia, atacar outros computadores, ou praticar outros atos criminosos. Seria terrível, não é verdade?

O primeiro passo para a defesa é conhecer nossos inimigos. Veremos a seguir quais são os principais tipos de pragas virtuais.

bruno@calheira.com

Vírus

Tipos de Pragas Virtuais

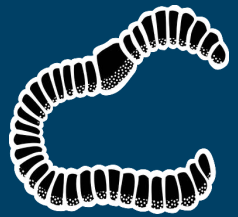
Tem a capacidade de se reproduzir, infectando outros arquivos com cópias dele mesmo.

bruno@calheira.com

Worm (Verme)

Tipos de Pragas Virtuais

É uma praga que pode se **auto-replicar** sozinha, enquanto que um vírus precisa de outro programa ou alguma ação do usuário para se reproduzir.



bruno@calheira.com

Trojan (Cavalo de Tróia)

Tipos de Pragas Virtuais

Aparenta ser apenas um programa útil, mas executa ações maliciosas de forma oculta.

bruno@calheira.com

Backdoor (Porta dos Fundos)

Tipos de Pragas Virtuais

Cria ou modifica serviços dentro do sistema para permitir que outras pragas infectem o equipamento.

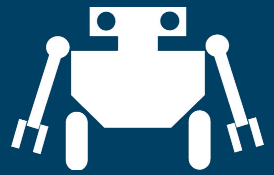
bruno@calheira.com

Bot (Robô)

Tipos de Pragas Virtuais

Programa que permite que o computador infectado seja controlado pelo invasor, transformando-o num **zumbi.**

Botnet: conjunto de computadores-zumbis.



bruno@calheira.com

Spyware (Espião)

Tipos de Pragas Virtuais

Captura informações do usuário e as envia para o invasor remotamente.

Keylogger: captura as teclas digitadas.

Screenlogger: captura a imagem da tela.

bruno@calheira.com

Adware (Propaganda)

Tipos de Pragas Virtuais

Exibe propagandas não solicitadas na tela do usuário.

bruno@calheira.com

Rootkit

Tipos de Pragas Virtuais

Conjunto de técnicas e programas usados pelo invasor para garantir que o computador da vítima continue infectado.

bruno@calheira.com

Ransomware (Sequestrador)

Tipos de Pragas Virtuais

Impede que o usuário tenha acesso a sua máquina ou aos seus arquivos até que um resgate *(ransom)* seja pago ao invasor.

bruno@calheira.com

Como se defender?

bruno@calheira.com

Use softwares originais

- Softwares piratas podem estar infectados.
- Instale apenas softwares de **fontes conhecidas**.
- Prefira utilizar **softwares livres**.
- Fazer ***jailbreak*** *(desbloqueio)* pode expor o seu smartphone a riscos.

bruno@calheira.com

Atualize os seus softwares

- **Atualizações de segurança** resolvem brechas e deixam seu sistema mais robusto.
- Mantenha seu **navegador** atualizado.

bruno@calheira.com

Antivírus

- **Instale** UM antivírus e mantenha-o **atualizado**.
- NÃO instale mais de UM antivírus. Caso contrário, pode haver conflitos.
- Configure-o para verificar os e-mails e mídias antes de abrí-los no seu computador.

bruno@calheira.com

Firewall (Muro de Fogo)

Programa que monitora o que entra e sai da sua rede.

- Instale e ative o firewall em seu equipamento.

bruno@calheira.com

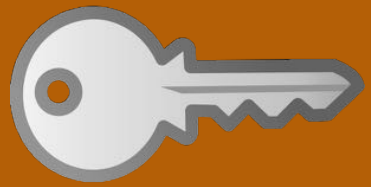
Backup (Cópia de Segurança)

*Aquela informação é **importante** ou **te faria falta** caso sumisse?*
Então faça **backup.**

- Faça backups constantes.
- Verifique se os arquivos não estão corrompidos ou infectados antes.
- Use a nuvem computacional.

bruno@calheira.com

Senhas Seguras

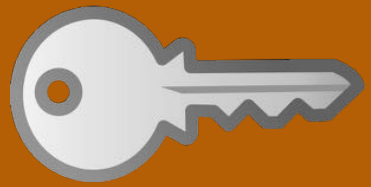


- Crie senhas com **frases** ao invés de **palavras**. Por exemplo:
  - MoroNaCasa#32
  - MeuuugatooohRoxo?
  - Choranaobebe3Pablo
  - #TelefoneTiaLeda9989

São mais seguras e fáceis de lembrar.

bruno@calheira.com

Senhas Seguras



- **Não** use a mesma senha em todos os sites. Você pode usar senhas **parecidas**, variando alguns detalhes. Por exemplo:
  - No Gmail:
    - MoroNaCasa#32GM
  - No Facebook:
    - MoroNaCasa#32FB

bruno@calheira.com

Fique alerta!

- Cuidado com os links e arquivos recebidos por mensagens eletrônicas.
- Ao usar sites de bancos, lojas e telas de login, certifique-se que a página utiliza o protocolo https.

bruno@calheira.com

Essas são apenas algumas dicas de como se proteger dos códigos maliciosos e pragas virtuais. Como diz o ditado: *"O preço da segurança é a vigilância constante."*

Se por um lado os bandidos criam esquemas cada vez mais sofisticados, por outro "os mocinhos" também criam softwares cada vez mais seguros e robustos. É uma batalha constante, em que não dá pra ficar parado.

Tendo **cuidado**, **atenção** e mantendo seus sistemas **seguros** e **atualizados** você tornar a vida dos invasores muito mais difícil.

bruno@calheira.com

Bruno Calheira
Consultor Web

calheira.com

Bruno Calheira é especialista em Engenharia de Software com ênfase em Software Livre. Trabalha como **servidor público** no TJ-BA e como **Consultor Web** para **pessoas e empresas que querem impulsionar seus projetos usando a Internet**.

brunocalheira

@brunocalheira

bruno@calheira.com