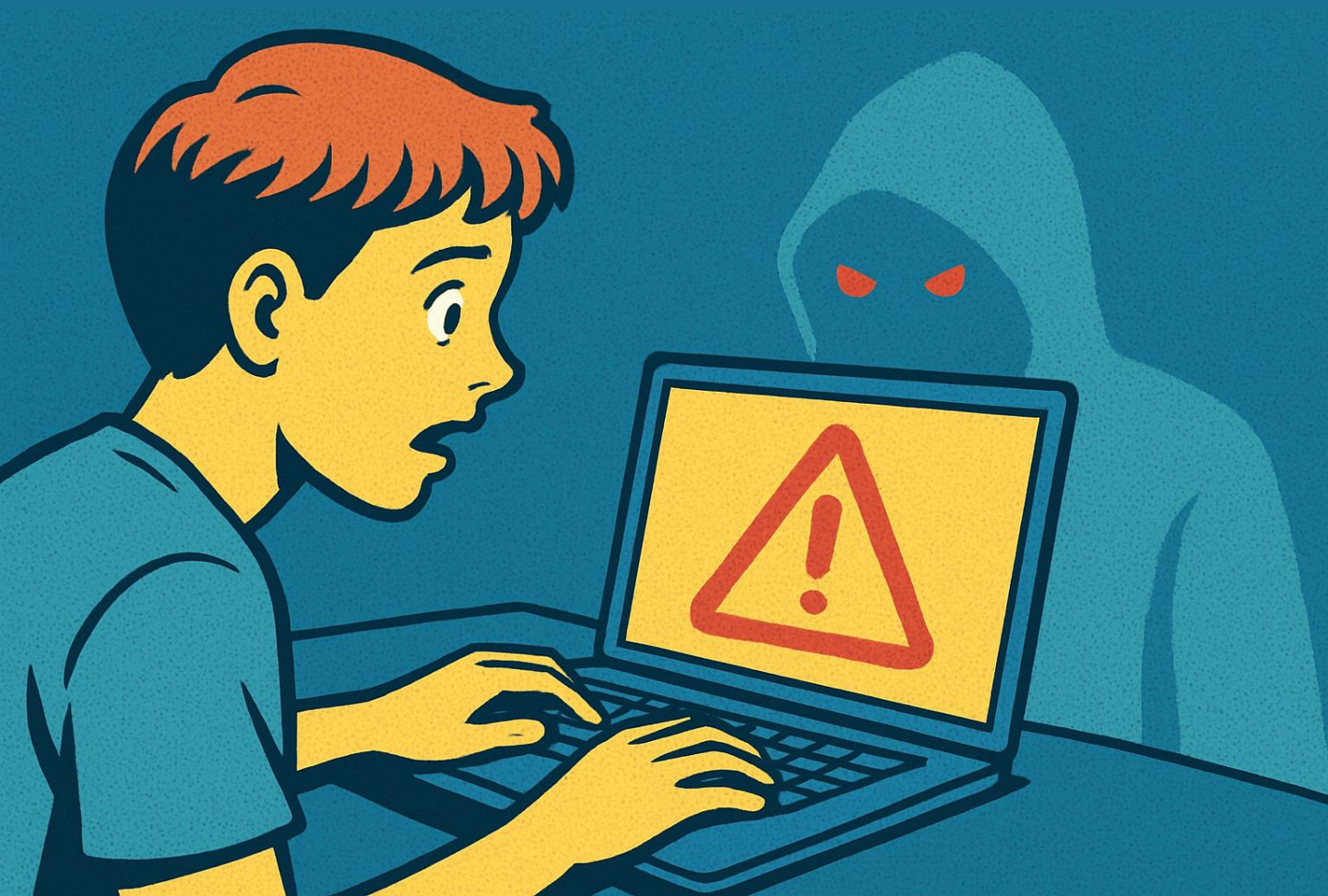
GUERRA CIBERNETICA

COMO VENCER OS INIMIGOS INVISÍVEIS DA INTERNET

RODRIGO F M GALVÃO



Guia Prático de Segurança Digital:

Como se Proteger de Golpes e Ataques Cibernéticos

Vivemos em um mundo cada vez mais conectado e, junto com as facilidades, surgem também os riscos.

Golpes digitais estão em todo lugar: no e-mail, nas redes sociais, no WhatsApp e até em sites aparentemente confiáveis.

Este guia vai te ajudar a se proteger de forma simples e prática.

1

CUIDADO COM LINKS SUSPEITOS

Um dos golpes mais comuns é o **phishing,** mensagens falsas que tentam te enganar para roubar senhas ou dados bancários.

Como se proteger:

Por exemplo: Você recebe um e-mail dizendo que seu banco bloqueou sua conta e pedindo para clicar em um link. Esse link leva a uma página falsa.

•Nunca clique em links de mensagens que pedem dados pessoais.
•Verifique o endereço do site (URLs falsas costumam ter erros sutis).
•Prefira digitar o endereço direto no navegador.

2

USE SENHAS FORTES E UNICAS

Usar a mesma senha em tudo é um erro comum.
Se um criminoso descobrir uma, ele pode acessar várias contas.

Como se proteger:

- Crie senhas longas, com letras, números e símbolos.
- Evite usar informações óbvias (como nome ou data de nascimento).
- Use um **gerenciador de senhas** (ex: Bitwarden, 1Password).

Exemplo:
Em 2023, uma grande plataforma de jogos teve vazamento de dados. Quem usava a mesma senha em outros serviços acabou com várias contas invadidas.

3

ATIVE A VERIFICAÇÃO EM DUAS ETAPAS

Mesmo que alguém descubra sua senha, a **autenticação em dois fatores (2FA)** adiciona uma camada extra de segurança.

Como funciona:

- Depois de digitar a senha, você confirma o login com um código enviado ao seu celular ou app autenticador.

Exemplo:
Se alguém tentar entrar na sua conta do Instagram, vai precisar do código que chega no seu celular — e isso costuma impedir o golpe.

4

DESCONFIE DE OFERTAS "BOAS DEMAIS"

Golpistas usam promoções falsas para atrair vítimas.

Como se proteger:

Exemplo real: anúncios falsos de “iPhone por R$ 500” circulam em redes sociais, levando a sites falsos que roubam dados e dinheiro.

- Pesquise se a loja é confiável.
- Desconfie de preços muito abaixo do normal.
- Veja se o site tem o **“cadeado”** na barra do navegador (https://).

5

MANTENHA TUDO ATUALIZADO

Softwares desatualizados podem ter falhas que criminosos exploram.

Como se proteger:

Exemplo: ataques de ransomware (como o WannaCry) afetaram empresas inteiras porque sistemas não estavam atualizados.

- Mantenha o sistema operacional, antivírus e aplicativos sempre atualizados.
- Ative as atualizações automáticas, se possível.

6

CUIDADO COM O QUE COMPARTILHA NAS REDES

Golpistas usam informações públicas para criar golpes personalizados.

Como se proteger:

Exemplo: alguém posta que vai viajar, e criminosos aproveitam para aplicar golpes de “falso parente pedindo ajuda”.

- Evite publicar dados pessoais (como endereço ou rotina).
- Configure a privacidade das suas redes.
- Desconfie de mensagens “urgentes” pedindo dinheiro.

7

USE ANTIVIRUS E FAÇA BACKUP REGULAR

Mesmo com todos os cuidados, é importante ter um plano B.

Como se proteger:

- Use um bom antivírus e mantenha-o atualizado.
- Faça **backup** dos seus arquivos importantes (em nuvem ou HD externo).

Exemplo: se seu computador for infectado por um vírus, você não perderá seus documentos e fotos.

8

CONCLUSÃO

Segurança digital não é um luxo, é uma necessidade.

OBRIGADO POR LER ATÉ AQUI

Esse Ebook foi gerado por IA, e diagramado por humano.
O passo a passo se encontra no meu Github

•

Esse conteúdo foi gerado com fins didáticos de construção, não foi realizado uma validação cuidadosa humana no conteúdo e pode conter erros gerados por uma IA.

https://github.com/RodrigoFMG/prompet-ebook.git