

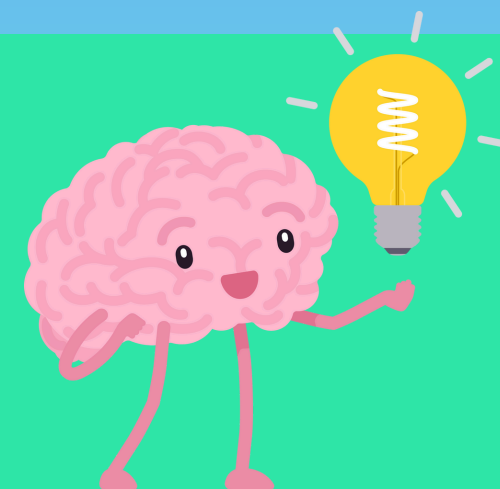
GOLPES DIGITAIS NA ERA DA INTELIGÊNCIA ARTIFICIAL:

USAR A NOSSA INTELIGÊNCIA É A
MELHOR FORMA DE PREVENÇÃO!



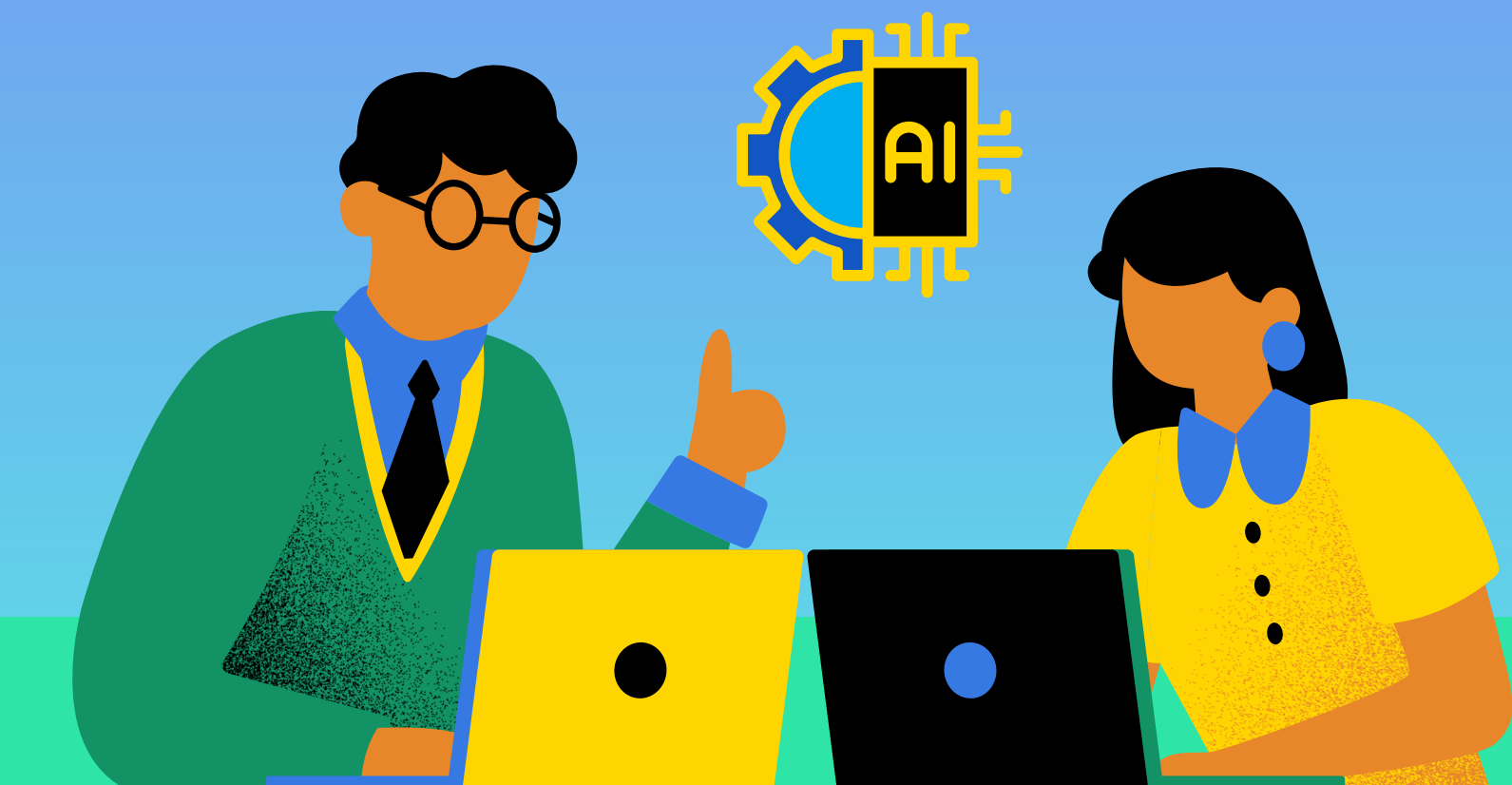
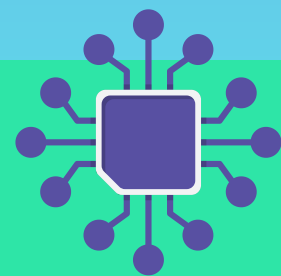
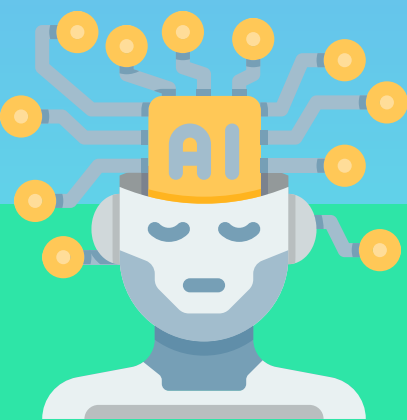
Procon **MPMG**
Ministério Público de Minas Gerais

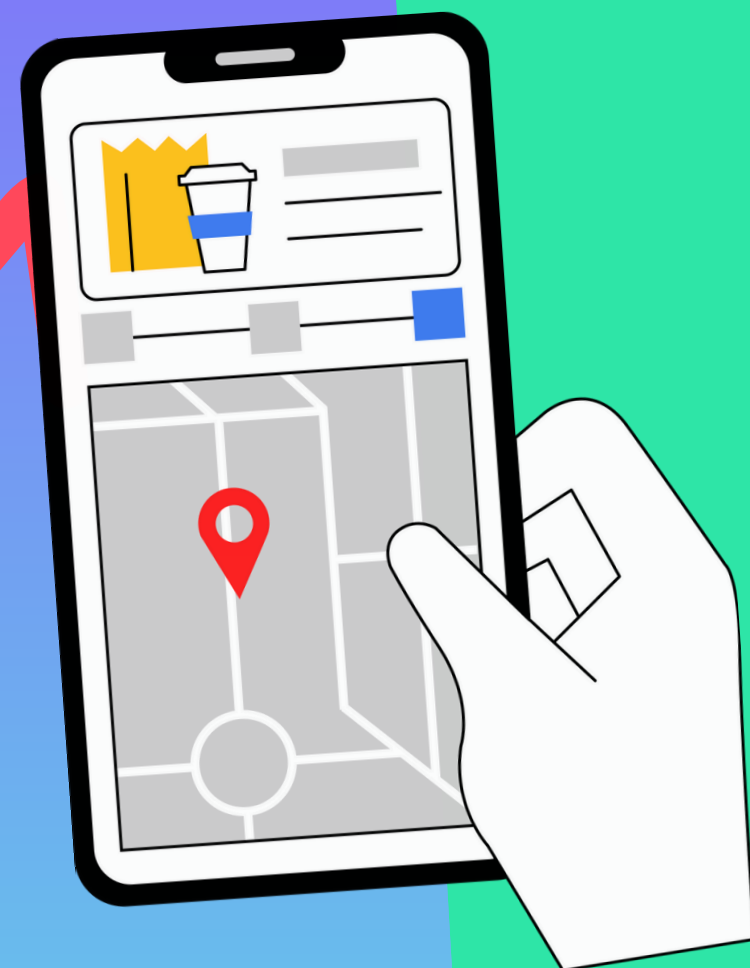
MPMG
Ministério Público
do Estado de Minas Gerais



SUMÁRIO

- 3 Introdução
- 4 O que é inteligência artificial
- 5 O que são golpes digitais?
- 6 Tipos comuns de golpes
- 7 Como identificar golpes
- 8 Como se proteger
- 9 O que fazer se você for vítima
- 10 Referências
- 10 Contate o Procon-MPMG





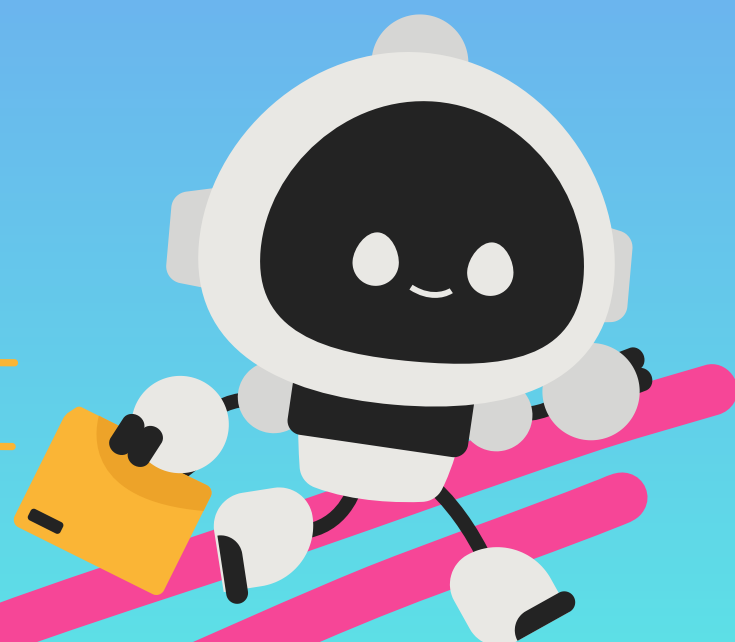
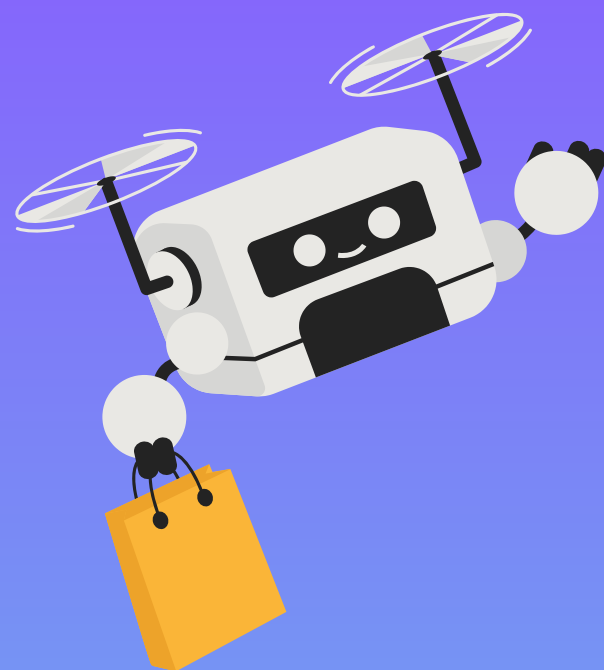
Introdução

A inteligência artificial (IA) está se tornando cada vez mais presente em nossas vidas, trazendo benefícios, mas também novos desafios. Infelizmente, golpistas estão utilizando essa tecnologia para aplicar fraudes. Esta cartilha tem como objetivo informar e orientar sobre como se proteger.



O que é inteligência artificial ?

Inteligência artificial (IA) é uma tecnologia que permite que computadores e máquinas simulem o aprendizado, a compreensão, a resolução de problemas, a tomada de decisões, a criatividade e a autonomia dos seres humanos.



O que são golpes digitais?

Golpes digitais são fraudes que ocorrem no ambiente online, onde os criminosos utilizam táticas enganosas para obter informações pessoais, financeiras ou para induzir as vítimas a realizar ações prejudiciais.

Com a IA, esses golpes estão se tornando mais complexos e difíceis de detectar.





Tipos comuns de golpes



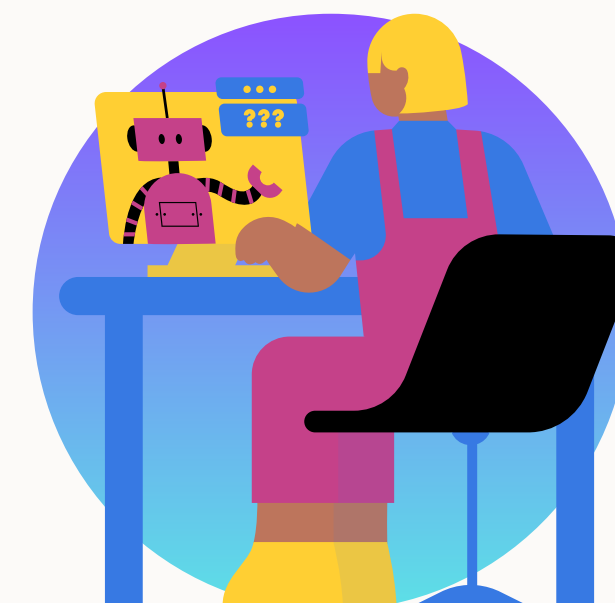
Phishing

Golpistas estão utilizando IA para criar e-mails e mensagens falsas que imitam perfeitamente a comunicação de empresas legítimas. A personalização das mensagens, baseada em dados coletados, torna mais fácil para os golpistas enganarem as vítimas.



Deepfakes

Os golpistas criam imagens, áudios ou vídeos falsos que parecem reais. As formas mais comuns de deepfakes envolvem: substituição de um rosto por outro; clonagem de voz e adulteração da região da boca, para que o movimento dos lábios acompanhe um áudio. Isso pode ser usado para fraudes financeiras, falsos sequestros, para confundir funcionários de empresas, fazendo-os executar ordens de pagamento inexistentes, gerando a perda de dinheiro.



Chatbots Maliciosos e Assistentes Virtuais Falsos

Golpistas estão utilizando chatbots alimentados por IA para interagir com as vítimas simulando o atendimento ao cliente de empresas legítimas. Podem guiar a vítima para realizar pagamentos falsos ou fornecer dados sensíveis.

Como identificar golpes



Desconfie de mensagens desconhecidas.
Se receber uma ligação, mensagem ou e-mail suspeito pedindo informações pessoais ou dinheiro, nunca forneça informações pessoais, não realize transações financeiras e não responda a estes tipos de solicitações. Verifique a autenticidade por outros canais! No caso de dúvidas, busque pessoalmente a sua instituição financeira ou a empresa.



Cuidado com a urgência!
Golpistas costumam criar um senso de urgência para pressionar a vítima a agir rapidamente.

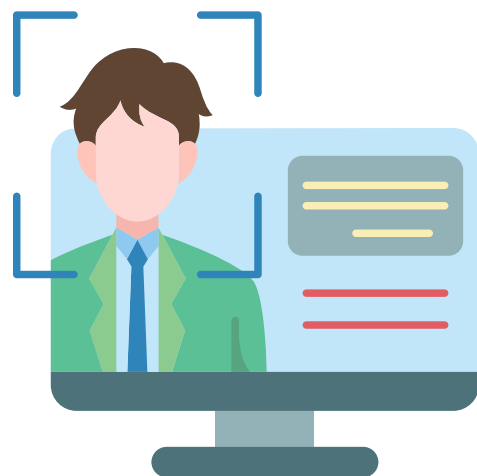


Mantenha seus dados pessoais em segurança
O compartilhamento de informações pessoais com estranhos, seja por mensagem ou telefone, em redes sociais e outros espaços públicos on-line, podem ser utilizados por golpistas. Nunca preencha formulários desconhecidos ou clique em links recebidos por e-mail, SMS, WhatsApp, redes sociais, etc.





Como se proteger



Use autenticação em duas etapas. Isso adiciona uma camada extra de segurança às suas contas. Troque suas senhas de sites, aplicativos e bancos com frequência. Evite usar a mesma senha em diferentes plataformas, pois isso pode facilitar a ação dos golpistas.



Mantenha seu software atualizado. Atualizações frequentemente corrigem vulnerabilidades que podem ser exploradas por golpistas.



Eduque-se sobre IA. Conhecer como a IA funciona pode ajudar a identificar fraudes que utilizam essa tecnologia.



O que fazer se você for vítima



Não entre
em pânico!

Respire fundo e
avalie a situação.



Entre em contato
com as autoridades

Registre um boletim
de ocorrência e informe
a sua instituição
financeira.



Altere suas
senhas

Se você forneceu
informações pessoais,
mude suas senhas
imediatamente.



Referências

GUITARRARA, Paloma. "Inteligência artificial"; Brasil Escola. Disponível em: <https://brasilecola.uol.com.br/informatica/inteligencia-artificial.htm>. Acesso em 25 de setembro de 2024.

Cartilha de Prevenção contra golpes
"O Golpe Tá Aí. Cai Quem Não Se Informa". Polícia Civil de Santa Catarina.

Cartilha Guia de orientações e prevenção a golpes –
Polícia Civil do Estado de São Paulo.

Engenharia social: Guia para proteção de conhecimentos sensíveis – Agência Brasileira de Inteligência
Ano 2021 – Produção Departamento de Contrainteligência
Programa Nacional de Proteção do Conhecimento Sensível (PNPC)

Engenharia social em golpes virtuais e prevenção:
principais técnicas Academia de Polícia Civil de Minas Gerais – Belo Horizonte – 2024

MARQUES, Karina Leite de Almeida Florentino –
Estelionato [manuscrito]: o ardil do autor e a torpeza da vítima – Trabalho de Conclusão de Curso
(Especialização direito penal e processual penal) –
Universidade Estadual da Paraíba, Centro de Ciências Jurídicas, 2014.



Elaborado pelo Procon-MG a partir de recursos, imagens e elementos do Canva.com.

Contate o Procon-MPMG



Rua Gonçalves Dias, 2039 – Lourdes



procon@mpmg.mp.br



(31) 3768-1700



procon.mpmg.mp.br



Registro de reclamação:
<https://aplicacao.mpmg.mp.br/ouvidoria/service/procon>



@procon.mpmg



ProconMG

