InclusãoDigital

Fernanda Nagaishi
Assessora de Tecnologia da Informação
tecinformacao@ipresb.barueri.sp.gov.br

Programa PÓS Aposentadoria

Juntos, ressignificamos o presente!

IPRESB

INSTITUTO DE PREVIDÊNCIA SOCIAL
DOS SERVIDORES MUNICIPAIS DE BARUERI

InclusãoDigital

Conteúdo

1. Inteligência Artificial

2. Dicas de Segurança e Golpes

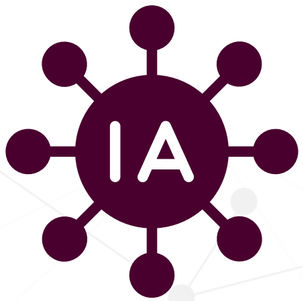
InclusãoDigital

1.

IA - Inteligência Artificial

InclusãoDigital

IA - Inteligência Artificial



O que é?

A Inteligência Artificial (IA) refere-se à capacidade de máquinas ou sistemas computacionais simularem a inteligência humana, permitindo que aprendam, raciocinem, tomem decisões e resolvam problemas de forma autônoma.

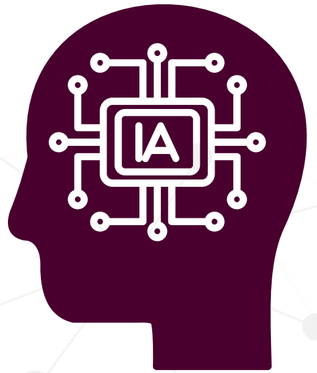
Como funciona?

A IA funciona através do uso de algoritmos* e modelos computacionais que processam grandes quantidades de dados para identificar padrões, fazer previsões e tomar decisões. Os sistemas de IA podem ser treinados para realizar tarefas específicas, como reconhecimento de fala, visão computacional, processamento de linguagem natural, entre outros.

*Algoritmo: é um conjunto finito de passos ou instruções detalhadas para resolver um problema ou realizar uma tarefa.

InclusãoDigital

IA - Inteligência Artificial

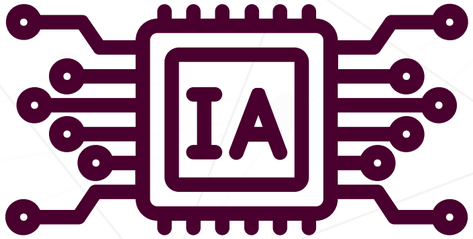


Tipos

- **IA Limitada (ANI):** Sistemas que se concentram em tarefas específicas, como reconhecimento facial ou jogos de tabuleiro.
- **IA Geral (AGI):** Sistemas com capacidade cognitiva semelhante à humana, capazes de realizar qualquer tarefa intelectual que um ser humano possa fazer.
- **Superinteligência Artificial (ASI):** Sistemas com inteligência superior à humana, um conceito ainda teórico.
- **IA Generativa (GenAI):** Sistemas capazes de gerar conteúdo novo, como textos, imagens e vídeos.

InclusãoDigital

IA - Inteligência Artificial



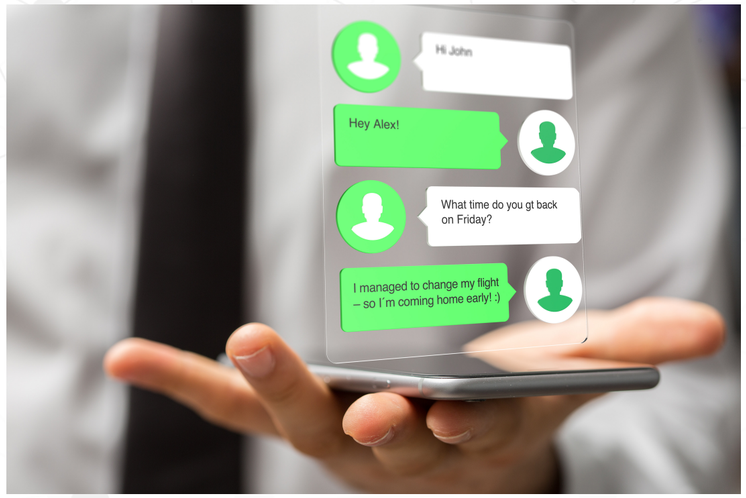
Aplicações

- Assistência virtual: Chatbots e assistentes pessoais.
- Reconhecimento de imagem e fala: Identificação de objetos e compreensão da linguagem falada.
- Processamento de linguagem natural (fala e escrita): Tradução automática e análise de texto.
- Veículos autônomos: Carros que se dirigem sem motorista.
- Recomendação de produtos: Sugestões personalizadas em plataformas de e-commerce.
- Saúde: Diagnóstico médico e desenvolvimento de novos tratamentos.
- Finanças: Detecção de fraudes e análise de risco.
- Educação: Aprendizagem personalizada e ferramentas de apoio ao ensino.

InclusãoDigital

IA - Inteligência Artificial

Aplicações

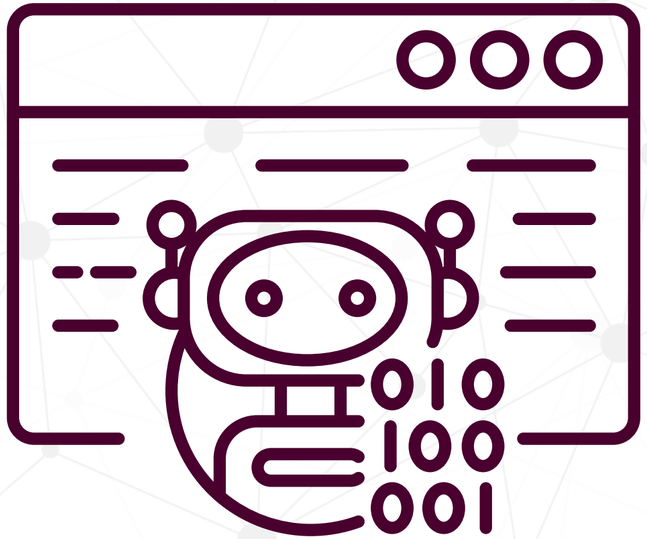


InclusãoDigital

IA - Inteligência Artificial

Vantagens

- Automatização de tarefas repetitivas
- Redução de custos operacionais,
- Melhora da eficiência em diversos processos
- Tomada de decisões mais rápidas e precisas
- Desenvolvimento de novas soluções e produtos.



InclusãoDigital

IA - Inteligência Artificial

Desafios e riscos

- Viés algorítmico, que pode perpetuar preconceitos.
- Preocupações com privacidade e segurança de dados.
- Possível substituição de empregos humanos.
- Responsabilidade em caso de erros ou acidentes.
- Complexidade dos sistemas e falta de transparência

https://youtu.be/KURJXd8zI5Y?si=7kO6ybJ4l3KNKY_c

InclusãoDigital

IA - Inteligência Artificial

Ferramentas

As ferramentas de IA são softwares/programas que utilizam da IA para realizar tarefas

OpenAI

GPT - 4

Gemini

Copilot

InclusãoDigital

“Qual é o maior medo de uma inteligência artificial?
Que os humanos descubram que ela não é tão inteligente quanto eles pensam.”

InclusãoDigital

2. Dicas de Segurança e Golpes

InclusãoDigital

Dicas de Segurança
Riscos

Conhecer os Riscos

Informação é a chave

Se informe sobre os riscos e como evitá-los com fontes confiáveis

Medidas de Segurança

Seguir as orientações de segurança

Mediante ao conhecimento dos riscos tome medidas que venham a minimizar.

Pensamento critico

Desenvolva o pensamento critico

Desconfie de soluções fáceis, milagrosas ou que prometam ganhos de forma simples.

InclusãoDigital

Dicas de Segurança

Proteção de Dispositivos e Aplicativos

Atualização

Mantenha os dispositivos sempre atualizados

Verifique nas configurações a ultima versão.

Utilize senha na tela inicial

Use senha para acessar ao celular

Bloqueie o acesso por meio de senha.

Desabilite funções na tela bloqueada

Desabilite funções da tela inicial

Desabilite funções como visualização de mensagens e acessos rápidos

Baixe aplicativos somente em sites oficiais

Baixe somente em meios oficiais

Use a loja oficial do fabricante ou do sistema. Nunca instale aplicativos recebidos por mensagens ou links.

Ajuste as permissões dos aplicativos

Ajuste as permissões de acesso

Avalie a necessidade de ter aquele aplicativo ou o que ele pode acessar.

InclusãoDigital

Dicas de Segurança

Autenticação e senha

Tamanho da senha e formato

Crie senhas com o minimo de caracteres e formato

Preferencialmente uma senha segura deve ter no mínimo 8 caracteres contendo números, letras e caracteres especiais, sendo recomendável o uso de frases.
Não repita senhas, não utilize data, números sequenciais, nomes de parentes ou qualquer palavra que se relacione diretamente com você.

Ative a verificação em duas etapas

Utilize a verificação em mais de um fator

Use a identificação em dois fatores, por tokens, aplicativos, SMS

InclusãoDigital

Golpes

Fake News e Boatos

Avaliar a notícia

Tenha pensamento critico

- Use o bom senso. Às vezes a notícia é tão sem sentido (“sem pé nem cabeça”) que basta refletir um pouco para identificá-la como boato
- Fique atento aos detalhes, verifique todo o conteúdo antes de repassar uma notícia. Observe a data, a notícia pode ser verdadeira mas se referir a fatos antigos.
- Verifique a origem da notícia, mesmo que a notícia cite fontes confiáveis, as informações podem estar fora do contexto ou com partes excluídas
- Confirme em outras fontes: consulte o site oficial das empresas citadas à procura de comunicados que confirmem ou desmintam a notícia
- Consulte sites especializados em desmentir boatos online, como:

G1 – Fato ou Fake https://g1.globo.com/fato-ou-fake/
Agência lupa: https://lupa.uol.com.br/
Aos fatos: https://www.aosfatos.org/
Google: https://support.google.com/websearch/answer/7315336?hl=pt-BR

InclusãoDigital

Golpes

Boatos e Fake News

Como identificar

Caracteristicas comuns de boatos/fake news

Afirma não ser um boato

- Possui título bombástico, resumido e com destaques em maiúsculo e tom alarmista usando palavras como “Cuidado” e “Atenção”
- Omite a data e/ou o local e não possui fonte ou cita fontes desconhecidas
- Não apresenta evidências e nem embasamento dos fatos noticiados
- Explora assuntos que estão repercutindo no momento
- Usa endereço do site e identidade visual similares às de sites conhecidos
- Apresenta erros gramaticais e de ortografia
- Usa imagens adulteradas ou fora de contexto
- Pede para ser repassado para um grande número de pessoas
- Possui grande quantidade de curtidas e compartilhamentos
- Vem de um perfil ou site já conhecido por divulgar boatos

InclusãoDigital

Golpes

Golpes e como se proteger

Phishing - pesca de dados

Como funciona

Os criminosos enviam e-mails ou mensagens de texto se passando por empresas reais. Nessas mensagens, eles podem pedir para que a pessoa faça o download de um arquivo, acesse um determinado link ou respondam alguns dados pessoais e bancários.

Como se proteger

- Não clicar em links ou baixar arquivos enviados por indivíduos que você não conhece;
- Mesmo que o link ou arquivo venha de uma pessoa que você conhece, principalmente em grupos de WhatsApp, certifique-se de que foi ela mesma que enviou e entenda qual é a origem desse link;
- Desconfie de ofertas que prometem grandes ganhos ou que tragam promoções com valores muito abaixo dos praticados . Geralmente essas condições são iscas para atrair as pessoas a clicarem no link;
- Não informe seus dados pessoais e bancários por e-mail ou fora de ambientes como o internet banking oficial do seu banco.

InclusãoDigital

Golpes

Golpes e como se proteger

Golpes em redes sociais

Como funciona

O criminoso consegue o acesso à conta de uma pessoa e começa a pedir dinheiro para os seguidores dela ou a vender produtos inexistentes.
Quando uma pessoa afirma que consegue multiplicar o dinheiro da vítima e pede para que ela envie uma determinada quantia para que ele possa fazer isso. Quando recebe a transferência, o criminoso desaparece.

Como se proteger

- Não clique em links enviados por pessoas que você não conhece. Mesmo se vier de um conhecido, verifique se foi ele mesmo que mandou e se ele sabe o origem do link;
- Desconfie quando ver alguém vendendo algum produto em um perfil pessoal. Entre em contato com a pessoa por outro meio para verificar se a conta não pode ter sido invadida;
- Desconfie de propostas que ofereçam muitos ganhos de dinheiro a partir de um primeiro depósito ou de promoções que ofereçam descontos muito grandes;

InclusãoDigital

Golpes

Golpes e como se proteger

Golpes do WhatsApp

Como funciona

- O WhatsApp é um dos alvos preferidos dos cibercriminosos. As fraudes mais conhecidas envolvendo esse aplicativo são a clonagem e o novo número.
- A clonagem pode ser feita de várias formas, e uma delas é quando o golpista tem acesso ao código de 6 dígitos enviado à vítima por mensagem de texto. Para conseguir o número, ele pode se passar por atendente de suporte técnico ou até mesmo de setores de cobranças.
- Outra maneira é enviando links maliciosos e contendo vírus em mensagens com promoções, que levam a pessoa até páginas falsas que solicitam informações através do preenchimento de formulários.
- Já o golpe do novo número ocorre quando o cibercriminoso já está com os números da sua agenda telefônica. Ele então cria uma nova conta no WhatsApp, se apropria da sua foto e envia mensagens pedindo dinheiro para os contatos, dizendo que está com um novo número.

InclusãoDigital

Golpes

Golpes e como se proteger

Golpes do WhatsApp

Como se proteger

- Sempre verifique no aplicativo ou internet banking oficial do seu banco as informações sobre os Pix enviados;
- Cheque os dados dos destinatários dos seus Pix, para conferir se quem vai receber realmente é a pessoa/instituição para quem você está mandando o dinheiro;
- Faça compras somente de lojas virtuais oficiais e idôneas;
- Não aceite suporte nem peça atendimento fora dos canais oficiais do seu banco.

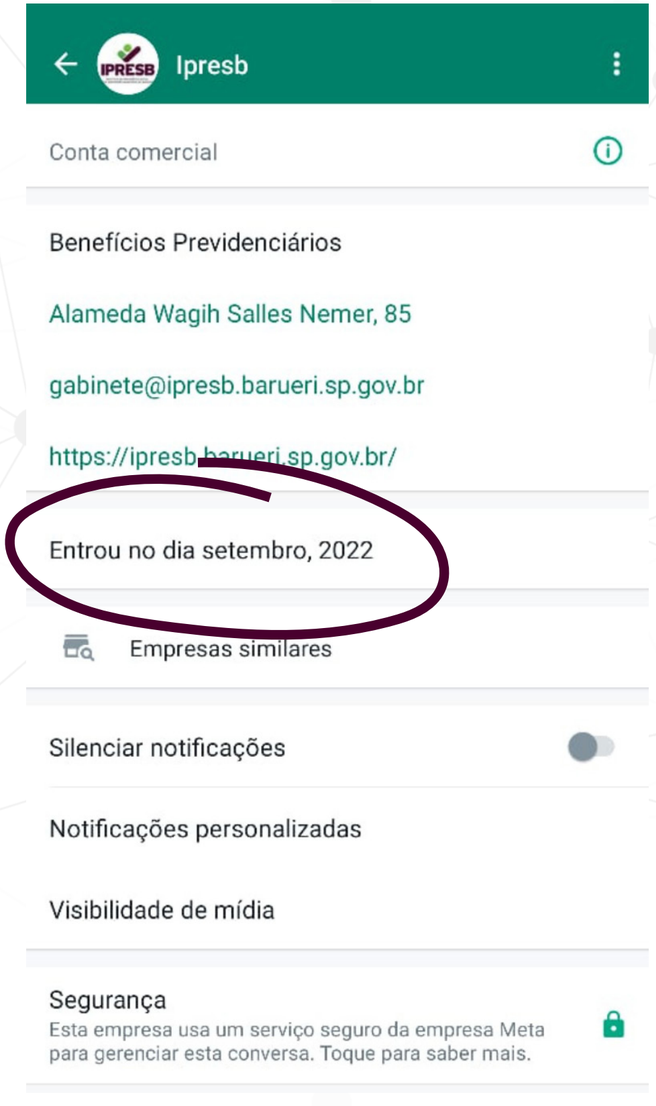
Golpes

Golpes e como se proteger

Conta Verificada WhatsApp

CONTA COMERCIAL

SERVIÇO SEGURO META



InclusãoDigital

Golpes

Golpes e como se proteger

Golpes do PIX

Como funciona

- Comprovante falso: o comprovante é adulterado para parecer com valor menor, sendo solicitado um novo PIX do restante do valor;
- Venda falsa: a cobrança é feita antes do envio da mercadoria que não é entregue e o vendedor desaparece;
- Atendimento bancário: é feito um atendimento falso em nome do banco solicitando a criação de uma chave pix, com isso é roubado os dados da pessoa;
- QR Code falso: é feito um QR Code como se fosse de uma empresa idônea mas o valor na verdade vai para o criminoso.
- Falha do PIX: os criminosos divulgam boatos sobre falhar no PIX informando se transferirem um valor especifico para uma determinada chave quem enviou receberá um valor maior de volta.

InclusãoDigital

Golpes

Golpes e como se proteger

Golpes do PIX

Como se proteger

- Não compartilhe seus dados pessoais com ninguém por e-mail, telefone e WhatsApp – inclusive senhas e códigos de acesso ao aplicativo recebidos por SMS;
- Mantenha o aplicativo do WhatsApp atualizado e só use o aplicativo oficial;
- Ative a verificação em duas etapas (também conhecida como identificação em dois fatores);
- Tenha cuidado ao utilizar o WhatsApp Web, não esquecendo de deslogar da plataforma quando estiver usando um computador compartilhado;
- Não clique em links suspeitos. Mesmo se tiver recebido de alguém que você conhece, pergunte se foi a pessoa mesmo que mandou e se ela sabe a origem do link;
- Não faça depósitos ou transferências de dinheiro a partir de pedidos no WhatsApp, mesmo se a pessoa se identificar como alguém conhecido – e principalmente se disser que está com um número novo.

InclusãoDigital

Referências

- IBM O que é inteligência artificial (IA)? https://www.ibm.com/br-pt/think/topics/artificial-intelligence
- Cartilha CERT/NIC br Phishing e Outros Golpes, Boatos , autor CERT.br/NIC.br - https://cartilha.cert.br/."
- Conta Azul Blog disponível em: https://contaazul.com/blog/principais-golpes-da-internet/

Playlist (lista de vídeos) do Youtube vídeos da palestra

InclusãoDigital

OBRIGADO!

Fernanda Nagaishi
Assessora de Tecnologia da Informação
tecinformacao@ipresb.barueri.sp.gov.br

Programa PÓS Aposentadoria
Juntos, ressignificamos o presente!

IPRESB
INSTITUTO DE PREVIDÊNCIA SOCIAL
DOS SERVIDORES MUNICIPAIS DE BARUERI