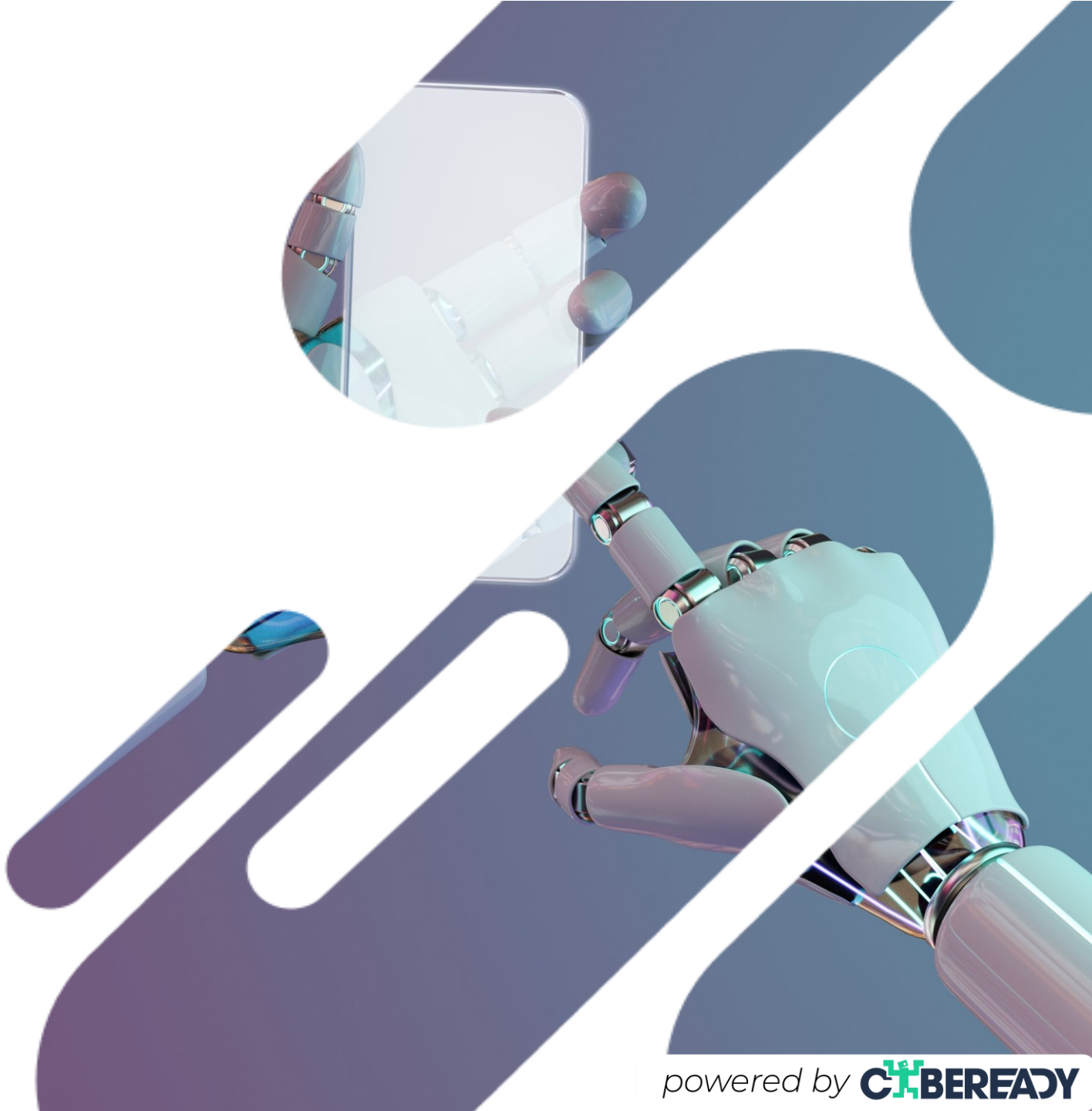
CYBEREADY

As ferramentas de IA estão a alterar a forma como os hackers operam.

Está preparado?



Antigamente...

Os ataques altamente enganadores exigiam muito tempo e esforço e só podiam ser criados por hackers experientes.

Assim, **a maior parte das tentativas de phishing estavam a um nível de principiante** (por exemplo, com erros ortográficos, designs suspeitos, linguagem incorreta, etc.), pelo que detetar uma falsificação era bastante fácil.

Hoje em dia...

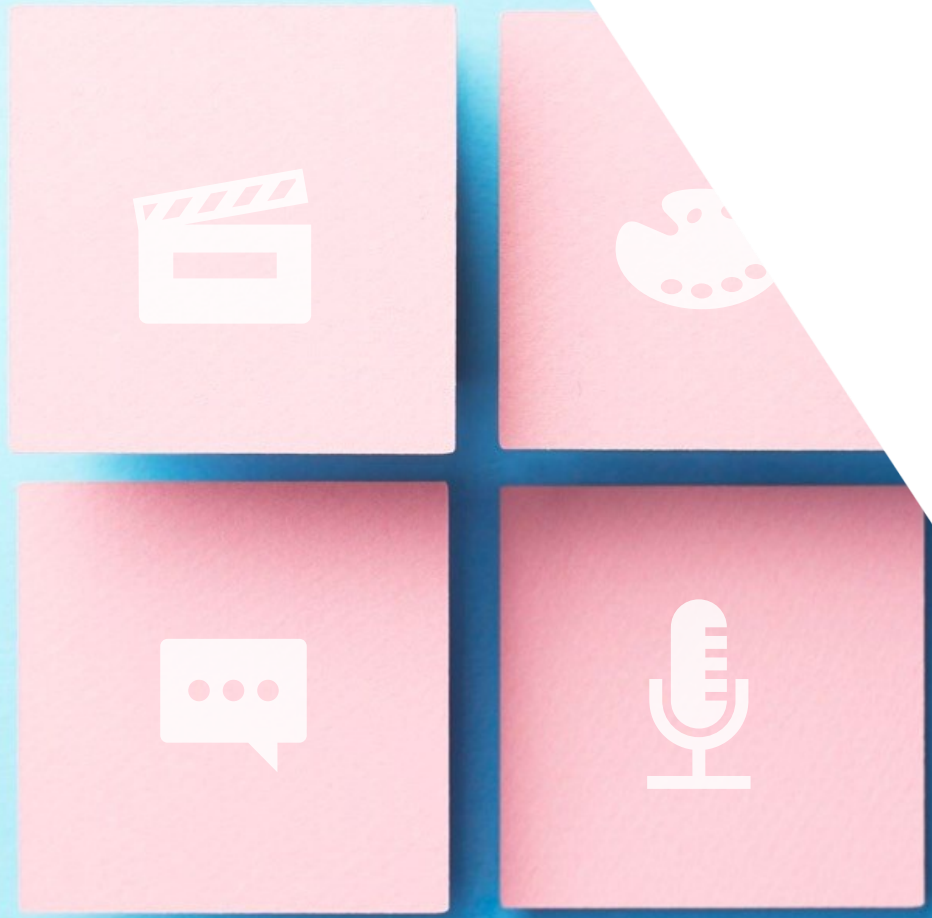
As ferramentas de IA permitem que os hackers criem de forma rápida e fácil e-mails e conteúdos com um aspeto altamente profissional.

Por este motivo, **começaram a chegar ataques mais sofisticados aos nossos e-mails.** Estes ataques altamente enganadores são mais difíceis de identificar como ameaças, aumentando o risco de cairmos neles.

Como pode detetar phishing agora?

- Nos e-mails, certifique-se de que o **endereço do remetente** aparece exatamente como esperado. Os hackers não podem falsificar este pormenor.

- Passe o rato sobre **ligações** antes de clicar para garantir que parecem legítimas. Os hackers podem imitar o design de empresas famosas, mas não podem utilizar os seus domínios verdadeiros.



O que já não é um sinal fiável de autenticidade?

- Designs profissionais
- Texto bem redigido
- Uma gravação de voz de alguém que conhece
- Vídeos de alta qualidade

CYBEREADY

Lembre-se: A nossa segurança está nas nossas mãos.

Crie o hábito de examinar todos os e-mails antes de clicar em qualquer ligação e nunca verifique os e-mails quando estiver distraído.