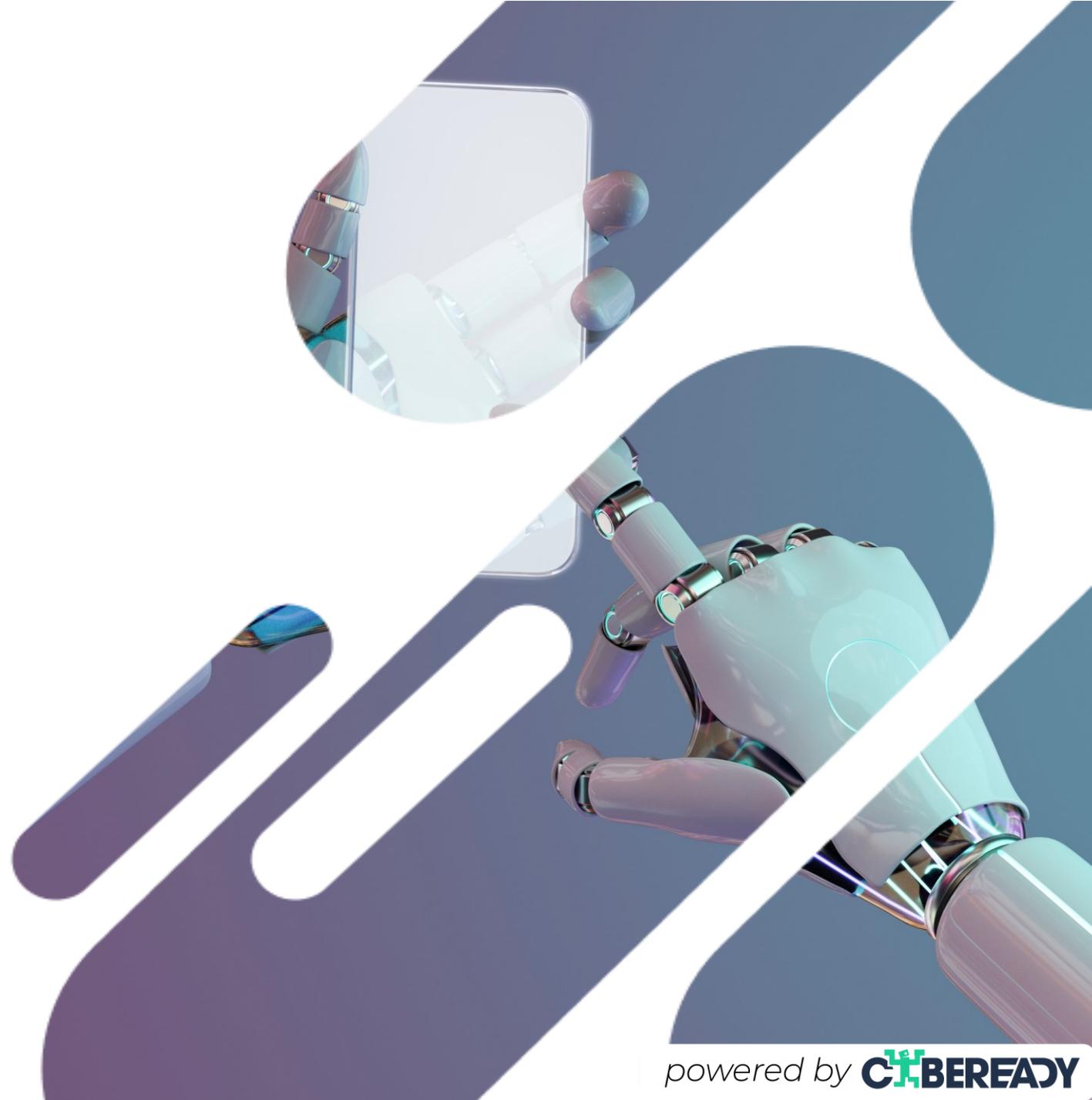




**Para los piratas  
informáticos, las  
herramientas de  
inteligencia artificial  
están cambiando las  
reglas del juego.**

**¿Está preparado?**



## Antes...

Ataques sumamente engañosos requerían mucho tiempo y esfuerzo y solo piratas informáticos expertos podían crearlos.

Por consiguiente, **la mayoría de los intentos de phishing eran de nivel principiante** (por ejemplo, con faltas de ortografía, diseños sospechosos, lenguaje entrecortado, etc.), por lo que detectar una falsificación era bastante fácil.



## Hoy en día...

Mediante las herramientas de IA, los piratas informáticos pueden crear rápida y fácilmente mensajes de correo electrónico y contenidos de aspecto muy profesional.

Por este motivo, **a nuestros buzones comienzan a llegar ataques más elaborados.** Resulta más difícil identificar estos ataques sumamente engañosos como amenazas, lo que aumenta el riesgo de que nos dejemos engañar por ellos.

## ¿Cómo se puede detectar ahora el phishing?

- En mensajes de correo electrónico, asegurarse de que la **dirección del remitente** aparezca tal y como es de esperar. Los piratas informáticos no pueden falsificar este detalle.
- Antes de hacer clic en **enlaces**, pasar el ratón sobre ellos para asegurarse de que parecen legítimos. Los piratas informáticos pueden imitar diseños de empresas famosas, pero no pueden utilizar sus dominios genuinos.



## ¿Qué ha dejado de ser una señal fiable de autenticidad?

- Diseño profesional
- Texto bien redactado
- Grabación de voz de alguien conocido
- Vídeos de alta calidad

## **Recuerde: Nuestra seguridad depende de nosotros.**

Es preciso acostumbrarse a examinar todos los correos electrónicos antes de hacer clic en los enlaces y nunca examinarlos al estar distraído.

