



# KI-Tools verändern die Methoden der Hacker.

**Sind Sie darauf  
vorbereitet?**



## Vorher ...

Hochgradig irreführende Angriffe erforderten viel Zeit und Mühe und konnten nur von erfahrenen Hackern durchgeführt werden.

**Die meisten Phishing-Versuche befanden sich demzufolge auf Anfängerniveau** (z. B.

Rechtschreibfehler, verdächtiges Design, holprige Sprache usw.) und waren deshalb ziemlich einfach als Fälschung zu erkennen.





## Heutzutage ...

Mithilfe von KI-Tools können Hacker schnell und einfach hochprofessionell aussehende E-Mails und Inhalte erstellen.

Aus diesem Grund, **kommen immer ausgefeiltere Angriffe in unsere Postfächer.** Diese äußerst betrügerischen Angriffe sind schwerer als Bedrohung zu erkennen und erhöhen das Risiko, dass wir auf sie hereinfallen.

# Wie erkennt man Phishing-Angriffe jetzt?

- Stellen Sie immer sicher, dass **die Absenderadressen** in E-Mails genau so aussehen, wie Sie dies erwartet haben. Hacker können dieses Detail nicht fälschen.
- Bewegen Sie den Mauszeiger über die angebotenen **Links**, bevor Sie darauf klicken, um sicherzustellen, dass sie auch wirklich echt sind. Hacker können bekannte Firmendesigns nachahmen, aber sie können nicht ihre echten Domänen verwenden.



## Was kann heutzutage **nicht mehr** als verlässliches Echtheitszeichen verwendet werden?

- Professionelle Designs
- Gut geschriebene Texte
- Sprachaufzeichnung von jemandem, den Sie kennen
- Hochwertige Videos



## Denken Sie an Folgendes: Unsere Sicherheit liegt in unseren Händen.

Machen Sie es sich zur Gewohnheit, jede E-Mail zu prüfen, bevor Sie auf einen Link klicken, und lesen Sie niemals E-Mails, wenn Sie abgelenkt sind.

