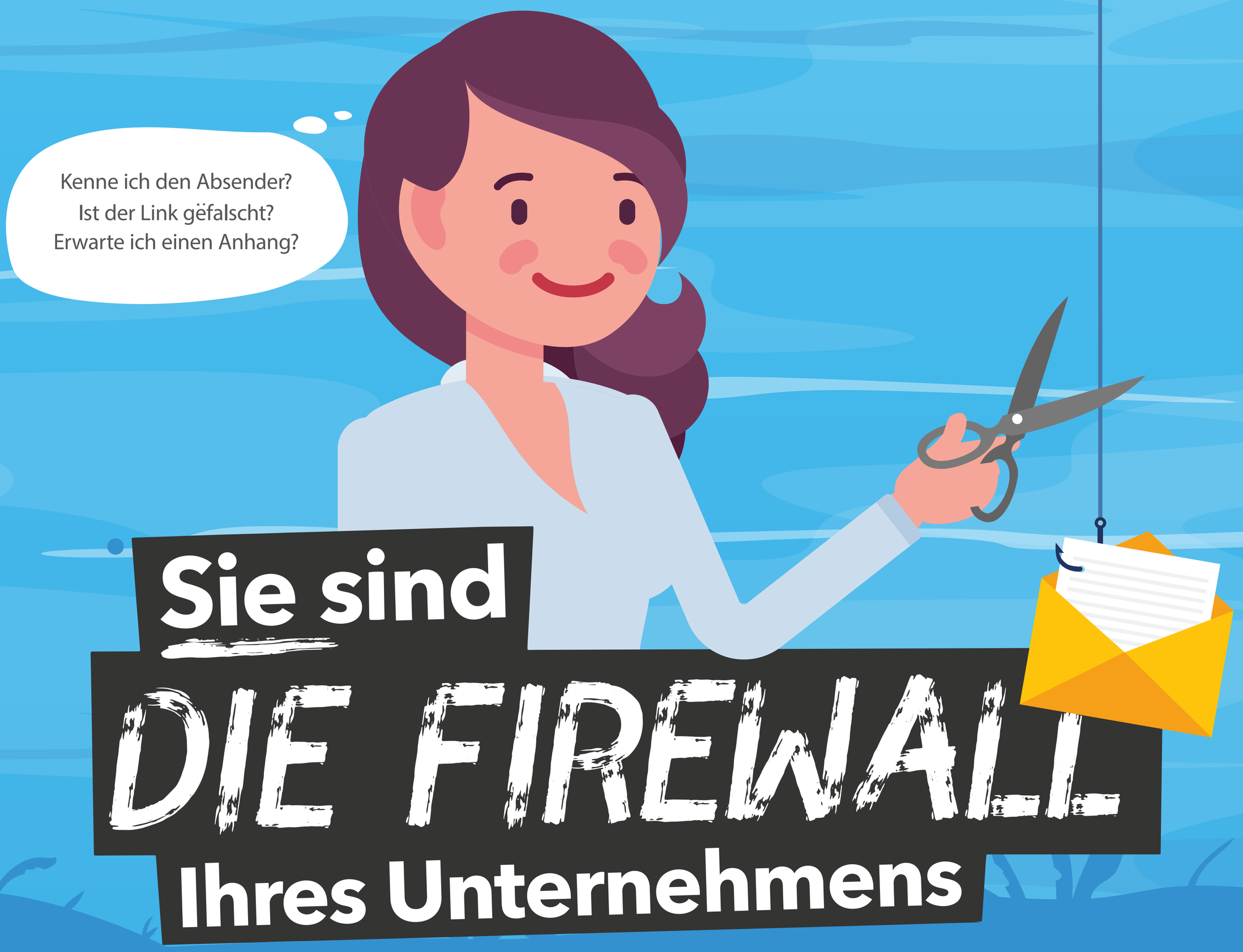
WIE ERKENNE ICH PHISHING-MAILS?

Gut vorbereitet in nur drei Schritten



Verifizieren Sie den Absender!

Ist der Absender und Betreff der E-Mail im Kontext plausibel?

Insbesondere die E-Mail-Adresse des Absenders sollte genau betrachtet werden, da die Domain täuschend echt gefälscht werden kann.

Seien Sie skeptisch! Im Zweifel vor dem Öffnen auf anderem Weg beim Absender nachfragen, ob diese E-Mail von ihm versendet wurde

Achten Sie auf die Zieldomain, bevor Sie Links anklicken!

Halten Sie hierzu die Maus über den Link, achten Sie auf den Bereich vor dem dritten Slash „/“

Ein kleines Beispiel:

https://www.google.de/services
führt Sie zu Google

https://www.google.de.myaccounts.biz/services
führt Sie auf die URL von myacounts.biz

Vorsicht bei Anhängen!

Bei E-Mails mit Anhängen ist besondere Vorsicht geboten!

Aktivieren Sie bei externen Dokumenten nicht den Bearbeitungsmodus.

Hier können Schadprogramme nachgeladen werden und Ihren Rechner und das Netzwerk infizieren.

HORNETSECURITY