HORNETSECURITY

PHISHING-NACHRICHTEN
UND GEFÄLSCHTE LINKS ERKENNEN

Sie sind

DIE FIREWALL

Ihres Unternehmens

HORNETSECURITY

PHISHING-NACHRICHTEN
UND GEFÄLSCHTE LINKS ERKENNEN

Phishing-E-Mails erreichen uns unter dem Deckmantel eines vertrauenswürdigen Absenders oder eines plausiblen Anliegens und verschleiern so geschickt ihre wahren Absichten: Schadsoftware auf unseren Rechnern zu installieren oder uns zur Preisgabe von Zugangsdaten über gefälschte Login-Seiten zu bewegen.

Wie können wir dem vorbeugen?
Wie können Sie die Phishing-E-Mail erkennen?

Lesen Sie hier, auf was Sie achten und welche Fragen Sie sich stellen müssen, wenn Ihnen eine E-Mail seltsam erscheint.

- **Verifizieren Sie den Absender**
  Kommt die E-Mail tatsächlich vom Kollegen aus der Nachbarabteilung? Ist die Absende-Adresse richtig geschrieben? Kleinste Abweichungen machen hier schon einen großen Unterschied.

  Max.Mustermann@it-seal.de – **Korrekt**
  Martine.Mustermann@it-sea1.de – **Falsch**

- **Achten Sie auf die Zieldomains, bevor Sie Links anklicken**
  Machen Sie Links sichtbar? „Klicken Sie hier". Das liest man oft in E-Mails. Was aber ist „hier"? Wo will Sie der Link hinführen? Auch wenn der Link vollständig lesbar ist, lohnt sich ein genauerer Blick.

  - Fahren Sie mit dem Mauszeiger auf den Link – klicken Sie ihn aber nicht an. Das (wahre) Linkziel wird Ihnen dann angezeigt, z.B. neben dem Mauszeiger oder in der Statusleiste des E-Mail-Fensters. Das funktioniert auch bei mobilen Endgeräten. Tippen Sie hier auf den Link und halten ihn für ca. zwei Sekunden gedrückt.

- **Prüfen Sie den „Wer"-Bereich**
  Sie kennen nun den Link? Sehr gut! Führt er Sie aber auch tatsächlich auf die Seite des beliebten Online-Händlers oder des Elektro-Fachmarkts? Der „Wer"-Bereich im Link gibt Ihnen Auskunft.

Sie finden ihn um den Punkt herum, vor dem dritten "/" in der Linkadresse.

https://de.**wikipedia.org**/wiki/Wikipedia:Hauptseite

- **Schauen Sie sich den „Wer"-Bereich genau an!** Cyberkriminelle machen sich hier unsere Unaufmerksamkeit zu Nutze und versuchen uns durch Zusätze, Buchstabendreher oder ähnlich erscheinende Buchstaben und Zeichen in die Irre zu führen:

  https://de.wikipedia.org/ –
  https://de.wikipedia-de.org/

  https://mediamarkt.de/ –
  https://mediarnarkt.de

  https://paketservice.de –
  https://paketsrevice.de

Erkennen Sie den Unterschied?

Wenn Sie sich nicht sicher sind, ob der Link zur vorgegebenen Seite führt, kopieren Sie ihn einmal in eine Suchmaschine ein oder testen Sie ihn über spezialisierte Analyseseiten (z.B. virustotal.com). Im Zweifel fragen Sie beim Absender der E-Mail noch einmal nach und überprüfen Sie so die Echtheit von E-Mail und Link.

- **Vorsicht bei Anhängen**
  Bei Anhängen an E-Mails gilt:
  - Vorsichtig sein und nicht unbedacht öffnen! Über E-Mail Anhänge kann Schadsoftware auf Ihren Rechner und das Netzwerk gelangen.
  - Öffnen Sie nur Anhänge, die Sie auch erwarten.
  - Fragen Sie beim Absender nach, wenn Sie sich unsicher sind.

- Achtung: Auch die in der E-Mail angegebenen Kontaktdaten des Absender können gefälscht sein! Sie verbinden Sie mit dem Kriminellen, der Ihnen natürlich beteuern wird, dass alles seine Richtigkeit hat. **Greifen Sie daher lieber zum Telefon und rufen Sie den vermeintlichen Absender unter der bekannten Nummer aus Ihrem Adressbuch an.**

Bleiben Sie wachsam!