FURMICA
Treuhand & IT

SPAM und Phishing E-Mails erkennen

Phishing- oder SPAM-E-Mails wirken oft auf den ersten Blick echt, enthalten aber typische Merkmale, an denen man sie erkennen kann. Wenn eine E-Mail mindestens eines der folgenden Merkmale hat, sollte man vorsichtig sein:

1. Dringender Handlungsbedarf

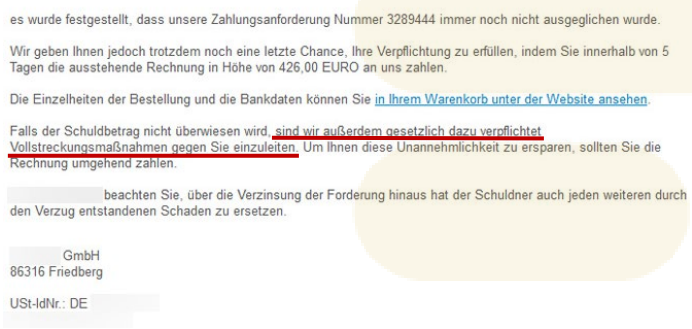
Phishing-Mails setzen häufig auf Zeitdruck, um unüberlegtes Handeln zu erzwingen.

Beispiel: „Ihr Konto wird in 24 Stunden gesperrt, wenn Sie nicht sofort Ihre Daten bestätigen!“

2. Drohungen

Oft enthalten solche Mails Drohungen oder angstmachende Aussagen, um Stress zu erzeugen.

Beispiel: „Wenn Sie nicht sofort reagieren, werden rechtliche Schritte gegen Sie eingeleitet!“



es wurde festgestellt, dass unsere Zahlungsanforderung Nummer 3289444 immer noch nicht ausgeglichen wurde.

Wir geben Ihnen jedoch trotzdem noch eine letzte Chance, Ihre Verpflichtung zu erfüllen, indem Sie innerhalb von 5 Tagen die ausstehende Rechnung in Höhe von 426,00 EURO an uns zahlen.

Die Einzelheiten der Bestellung und die Bankdaten können Sie in Ihrem Warenkorb unter der Website ansehen.

Falls der Schuldbetrag nicht überwiesen wird, sind wir außerdem gesetzlich dazu verpflichtet Vollstreckungsmaßnahmen gegen Sie einzuleiten. Um Ihnen diese Unannehmlichkeit zu ersparen, sollten Sie die Rechnung umgehend zahlen.

beachten Sie, über die Verzinsung der Forderung hinaus hat der Schuldner auch jeden weiteren durch den Verzug entstandenen Schaden zu ersetzen.

GmbH
86316 Friedberg

USt-IdNr.: DE

3. Aufforderung zur Preisgabe vertraulicher Daten

Echte Unternehmen fordern niemals per E-Mail sensible Daten wie Passwörter, Kreditkartennummern oder PINs an.

Beispiel: „Bitte geben Sie Ihre Online-Banking-PIN ein, um Ihre Identität zu bestätigen.“

Rechnung fehlgeschlagen - Konto gesperrt

NETFLLIX

Hi

Wir haben Probleme mit Ihren aktuellen Rechnungsinformationen. Wir werden es erneut versuchen, aber in der Zwischenzeit möchten Sie möglicherweise Ihre MASTERCARD in Ihren Zahlungsdetails aktualisieren.

JETZT KONTO AKTUALISIEREN

Wir sind hier, um Ihnen zu helfen, wenn Sie es brauchen. Besuche den Hilfezentrum für mehr info oder kontaktiere uns.

Deine Freunde bei Netflix

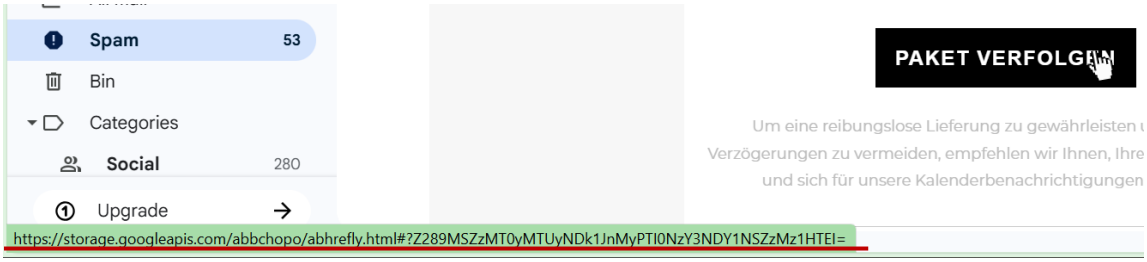
FURMICA
Treuhand & IT

4. Links oder Formulare in der E-Mail

Phishing-Mails enthalten oft gefälschte Links oder eingebettete Formulare. Die Links sehen täuschend echt aus, führen aber auf manipulierte Seiten.

Beispiel: Statt „www.post.ch“ führt der Link zu „www.post-secure-login.com“.

Tipp: Fahre mit der Maus über den Link (ohne zu klicken), um die echte Zieladresse zu sehen.



5. Ungewöhnliches Verhalten trotz bekannter Absenderadresse

Manchmal scheinen Phishing-Mails von einer bekannten Person oder Organisation zu stammen. Der Inhalt wirkt jedoch ungewöhnlich oder unlogisch.

Beispiel: Eine E-Mail angeblich von deiner Bank mit der Bitte: „Bitte laden Sie die angehängte Datei herunter und installieren Sie das Update.“

Beispiel: Ein Kollege schickt dir plötzlich einen Link zu „spannenden Bildern“ obwohl er das sonst nie macht.

6. E-Mail-Adresse und Name des Absenders

Betrüger lassen es oft so aussehen, als wäre der Anzeigename die echte Absenderadresse. Entscheidend ist jedoch die Adresse in den Klammern < >.
Wirkt diese ungewöhnlich, enthält Schreibfehler oder nutzt eine private Adresse (z. B. @gmail.com), obwohl die Nachricht angeblich von einer Firma stammt, handelt es sich sehr wahrscheinlich um eine Phishing-Mail.

Fazit:

Phishing-Mails erkennt man oft an Druck, Drohungen, Datenforderungen, dubiosen Links oder ungewöhnlichen Nachrichten von scheinbar bekannten Absendern.

Bei Fragen oder Problemen stehen wir gerne unter +41 27 510 50 95 oder itsupport@furmica.ch zur Verfügung.