

Wie erkennen Sie ein Phishing-Mail?

So unterschiedlich Phishing-Attacken auch ablaufen, an diesen zehn typischen Merkmalen erkennen Sie ein Phishing-Mail:

1. Sie kennen den Absender nicht.
2. Sie werden nicht persönlich angesprochen («Sehr geehrter Kunde»).
3. Das E-Mail fordert Sie zu einer dringenden Handlung auf («Loggen Sie sich innerhalb von 2 Tagen ein.»).
4. Das E-Mail enthält Drohungen («Andernfalls wird Ihr Konto gesperrt.»).
5. Der Text ist in schlechtem oder fehlerhaftem Deutsch geschrieben.
6. Umlaute wurden vergessen oder aufgelöst (statt «ü» steht «u» oder «ue»).
7. Ihre vertraulichen Daten werden abgefragt.
8. Die URL beginnt nicht mit <https://>.
9. Die URL enthält verdächtige Zeichen (69-connecta.net oder kns-suisse.kunden.ch).
10. Auf der verlinkten Website fehlt das SSL-Sicherheitszertifikat (Secure Socket Layer).

So schützen Sie sich gegen Phishing

Die Tricks der Betrüger sind zwar raffiniert, aber wenn Sie auf die folgenden acht wichtigen Regeln zur Prävention gegen Phishing achten, dann können Sie die Betrüger umgehen:

1. Misstrauen Sie E-Mails, deren Absenderadresse Sie nicht kennen. Besonders vertrauenswürdige Unternehmen werden gerne gefälscht.
2. Seien Sie vorsichtig, wenn Sie E-Mails bekommen, die eine Aktion von Ihnen verlangen und mit Konsequenzen drohen (Geldverlust, Strafanzeige, Konto- oder Kartensperrung usw.)
3. Überprüfen Sie Zahlungsaufforderungen, die Sie per E-Mail erhalten.
4. Klicken Sie in verdächtigen E-Mails auf keine Anhänge und keinen Link.
5. Öffnen Sie keine E-Mail-Anhänge mit skurrilen Endungen (z. B. picture.bmp.vbs).
6. Besuchen Sie nur vertrauenswürdige Websites.
7. Kontrollieren Sie regelmässig Ihre Kreditkartenabrechnungen und Bankauszüge.
8. Schützen Sie Ihre Computer mit Antiviren-Programmen, und halten Sie Ihre Software immer auf dem neuesten Stand.

Nationales Zentrum für Cybersicherheit NCSC

<https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-private/aktuelle-themen.html>