

Checkliste Erkennen von Phishing-E-Mails

Diese Checkliste hilft Ihnen, Phishing-E-Mails zu erkennen. Jeder einzelne Punkt kann ein Hinweis auf einen Phishing-Angriff sein.

- In der E-Mail fragt ein Online-Dienst-Anbieter (Online Banking, Online-Shopping, etc.) nach vertraulichen Daten.
- Die E-Mail enthält Grammatik- oder Rechtschreibfehler
- In der E-Mail werden Umlaute nicht richtig (gar nicht, falsch oder als „ae“, „oe“, „ue“) dargestellt.
- Der Absender der E-Mail hat den Firmennamen oder die Absender-Adresse gefälscht.
- Die E-Mail enthält eine unpersönlicher Anrede (zum Beispiel „Sehr geehrter Kunde / Lieber Kunde der Bank xyz“).
- Die E-Mail enthält eine unpersönliche Grußformel (zum Beispiel „Ihr Serviceteam“ oder „Ihre xyz Bank“).
- Die E-Mail ist nicht direkt an Sie beziehungsweise nicht an Ihre E-Mail-Adresse adressiert.
- In der E-Mail wird Ihnen gedroht (zum Beispiel „Beeilen Sie sich, sonst wird Ihr Konto gesperrt“).
- In der E-Mail wird Verbesserung der Sicherheitsmechanismen oder Zugangsdatenbestätigung bzw. Zugangsdatenpflege thematisiert.
- Die E-Mail fordert Sie zum Eingeben oder Senden sensibler Informationen zur angeblichen Entsperrung Ihres Kontos oder Ihrer Kreditkarte auf.
- Die E-Mail enthält ein auszufüllendes Formular, das persönliche Bankdaten (PIN, TANs, Kontonummer, vollständiger Name, Banking-ID, etc.) aus angeblichen Sicherheitsgründen bestätigen soll.
- Die E-Mail enthält einen Link der zu einem auszufüllenden Formular, das angeblich persönliche Bankdaten (PIN, TANs, Kontonummer, vollständiger Name, Banking-ID, etc.) aus Sicherheitsgründen bestätigen soll.
(Bei HTML-E-Mails kann der Link durch zusätzliche Formatierung verschleiert werden.)