

Checkliste Erkennen von Phishing-Webseiten

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

- Eine Internetadresse der Webseite, auf der Sie zur Eingabe vertraulicher Informationen aufgefordert werden, beginnt nicht mit <https://> und das geschlossene Vorhängeschloss im Browser wird nicht angezeigt.
- Ihr Browser weist Sie beim Betreten der Webseite auf ein ungültiges Zertifikat hin und bietet Ihnen an eine Ausnahmeregelung (Sicherheitsausnahme) zu bestätigen.
- Die Internetadresse sieht der eigentlichen Zieladresse täuschend ähnlich, ist aber im Detail etwas verändert (zum Beispiel <https://www.musterbank-on1line.de> anstatt <https://www.musterbank-online.de>).
- Die Webseite enthält Grammatik- oder Rechtschreibfehler.
- Auf der Webseite werden Umlaute nicht richtig (gar nicht, falsch oder als „ae“, „oe“, „ue“) dargestellt.
- Die Webseite enthält kopierte Firmennamen oder Logos.
- Auf der Webseite wird Ihnen gedroht (zum Beispiel „Beeilen Sie sich, sonst wird Ihr Konto gesperrt“).
- Auf der Webseite wird Verbesserung/Aktualisierung der Sicherheitsmechanismen oder Zugangsdatenbestätigung bzw. Zugangsdatenpflege thematisiert.
- Die Webseite fordert Sie zum Entsperren eines Kontos oder einer Kreditkarte auf.
- Die Webseite enthält eine unpersönliche Anrede (zum Beispiel „Sehr geehrter Kunde / Lieber Kunde der Bank xyz“).
- Die Webseite enthält eine unpersönliche Grußformel (zum Beispiel „Ihr Serviceteam“ oder „Ihre xyz Bank“).
- Die Webseite enthält ein auszufüllendes Formular, das persönliche Bankdaten (PIN, TANs, Kontonummer, vollständiger Name, Banking-ID, etc.) aus angeblichen Sicherheitsgründen bestätigen soll.

- Die sensiblen Kontoinformationen wie PIN, TAN oder Login Daten werden in einem Pop-up-Fenster abgefragt.