



Phishing

„Phishing“ ist ein englisches Kunstwort, das sich an Fishing („Angeln“) und Passwort, also das „Angeln nach Passwörtern“, anlehnt.

Beim Phishing versuchen Internet-Betrüger mittels gefälschten E-Mails und Websites an die Passwörter der Internetnutzer zu gelangen.

Bevorzugte Angriffsziele für Phishing-Betrüger sind: Banken (Onlinebanking), Bezahlsysteme (PayPal, etc.), Versandhäuser, Auktionshäuser oder Singlebörsen.

- Wie kann man sich davor schützen?
Banken, Bezahlsysteme oder Versandhäuser werden Sie niemals per E-Mail nach Ihrem Passwort fragen
- Was tun, wenn man sich nicht sicher ist, ob es sich um Phishing-Mail handelt?
Am Besten fragen Sie telefonisch bei der jeweiligen Bank, Online-Shop, etc. nach
- Wie erkennt man Phishing-Mails oder Webseiten rechtzeitig?
 - Mittlerweile bieten laufend aktualisierte Antivirenprogramme einen guten Schutz gegen Phishing-Attacken. Auch einige E-Mail-Programme und Browser, wie Internet Explorer 8 und Mozilla Firefox, warnen vor Phishing-Seiten
 - Wenn Sie eine E-Mail von Ihrer Bank bekommen und Sie mit „Sehr geehrter Kunde“ angesprochen werden, obwohl Ihr Name der Bank bekannt ist, ist dies eine weitere Möglichkeit Phishing-Mails zu erkennen.
 - Sie werden aufgefordert eine Webseite zu besuchen, welche der „echten Webseite“ täuschen ähnlich sieht, und zur Eingabe Ihrer Zugangsdaten aufgefordert.
 - Achten Sie auf eine korrekte Rechtschreibung in E-Mails und auf Webseiten.

Beispiel für eine Phishing-Webseite:

