



Im Falle eines Falles:

Sind Sie bereits Opfer einer Phishingmail geworden, informieren Sie bitte unverzüglich den betreffenden Internet-Anbieter (z. B. Bank, Kontaktportal, Versand- oder Auktionshaus) und die Kriminalpolizei. Speichern Sie die gefälschte E-Mail zur Beweissicherung. Falls noch möglich, machen Sie Ihre alte PIN für den Trickbetrüger sofort unbrauchbar, indem Sie sie durch eine neue ersetzen.

Weitere Informationen unter:

www.vr-networld.de

www.google.de (Suchkriterium: Phishingschutz)

www.stiftung-warentest.de/online/geldanlage_banken/meldung/1277969/1277969.html

www.bsi-fuer-buerger.de

Das **« Wir machen den Weg frei »** Prinzip

***Richtiger Umgang
mit gefälschten E-Mails.***

***Wichtige Tipps, wie Sie Phishing
verhindern können.***



Was ist Phishing?

Phishing ist ein Kunstwort, gebildet aus den Begriffen „Password“ und „Fishing“. Damit bezeichnet man den Trick von Betrügern, mithilfe gefälschter E-Mails vertrauliche Kundendaten zu erschleichen, um damit bei Bank-, Waren- oder Auktionshauskonten immensen Schaden anzurichten.

Waren es anfangs noch einfache Mailtexte, die in holprigem Deutsch den Empfänger zur Preisgabe seiner persönlichen Identifikations- (PIN) und Transaktionsnummer (TAN) aufforderten, so gehen die Täter heute mit mehr Raffinesse ans Werk:

Die Mails sehen aus wie offizielle Schreiben, z. B. Ihrer Bank. Sie tragen also das Firmenlogo, benutzen dieselbe Schriftart und dieselben Gestaltungsrichtlinien. Im Text ist oft die Rede von „Sicherheitsüberprüfungen“ oder anderen wichtig klingenden Maßnahmen.

Alle Phishingmails verfolgen das gleiche Ziel: Sie zu einer Formularseite weiterzuleiten, auf der Sie Ihre Geheimzahlen eintragen sollen. Diese Seiten sind ebenfalls perfekt den offiziellen Web-Seiten nachgebaut. Auch wenn Sie die Link-Adresse als die richtige identifizieren, ist Vorsicht geboten – denn sie ist trotzdem gefälscht.

Allerdings: Ganz gleich, wie geschickt die Trickbetrüger vorgehen – abwehren kann man sie mit relativ einfachen Maßnahmen.

Wie kann ich mich dagegen schützen?

Phishing nutzt wie die meisten Trickbetrügereien eine Kombination aus technischen und menschlichen Schwächen. Doch mit einer gesunden Portion Misstrauen und den folgenden Verhaltensregeln können Sie sich effektiv gegen Betrüger schützen.

- 1** Seriöse Internet-Anbieter fragen niemals nach sicherheitsrelevanten Daten! **Antworten Sie deshalb grundsätzlich nicht** auf E-Mails, bei denen – aus welchem Grund auch immer – nach Ihrer PIN oder TAN gefragt wird.
- 2** **Verwenden Sie keine Links aus Mail-Adressen**, um Ihr Onlinebanking aufzurufen. Geben Sie die Adresszeile stets von Hand ein. Oder benutzen Sie Bookmarks, die Sie selbst angelegt haben.
- 3** **Prüfen Sie**, ob die angezeigte Internet-Adresse mit der zertifizierten Adresse Ihrer Bank übereinstimmt (Doppelklick auf das Schloss-Symbol im Browser). Bei Abweichungen den Vorgang sofort abbrechen und die Bank benachrichtigen.
- 4** **Vereinbaren Sie ein Tageslimit** für Onlineüberweisungen. So kann möglicher Schaden von vornherein begrenzt werden.
- 5** **Sperren Sie Ihr Konto**, sobald Sie glauben, dass ein Dritter Ihre PIN oder TAN erlangt hat. Machen Sie dies direkt über Ihre Bank oder notfalls über die dreimalige Eingabe einer falschen PIN.