

Gefahren beim Onlinebanking: So schützen Sie sich!

Bankgeschäfte über das Internet werden täglich millionenfach ohne Probleme getätigt. Das geht schnell, bequem und unkompliziert – ist aber auch interessant für Betrüger. Mit raffinierten Tricks versuchen sie, an die Zugangsdaten Ihres Kontos zu gelangen. Eine beliebte Methode ist Phishing.

Was ist Phishing?

- Phishing setzt sich zusammen aus den englischen Wörtern für Passwort und Fischen. Betrüger versuchen dabei, mit gefälschten E-Mails geheime Zugangsdaten abzufragen.
- Phishing-Mails sehen aus wie offizielle Schreiben, zum Beispiel Ihrer <<Name der Bank>>: Täuschend echt – mit Logo und gleicher Schrift.
- Im Text ist oft die Rede von „Sicherheitsüberprüfungen bzw. Sicherheitstechnischen Standards“. Sie werden aufgefordert, Ihre PIN und TAN einzugeben.
- Alle Phishing-Mails verfolgen das Ziel, Sie zu einer Internetseite mit Formular weiterzuleiten, auf der Sie Ihre Geheimzahlen eintragen sollen. Diese Seiten sind eins zu eins den offiziellen Webseiten Ihrer Bank nachgebaut.

Wie Sie sich vor Datenmissbrauch schützen:

- Antworten Sie grundsätzlich nicht auf Phishing-Mails. Stattdessen löschen Sie diese ungeöffnet aus Ihrem Postfach – auch aus dem Papierkorb.
- Benutzen Sie keine Links aus Mail-Adressen, um Ihr Onlinebanking aufzurufen. Geben Sie die Adresse <<Internetseite der Bank>> immer selbst ein.
- Verwenden Sie für Onlinebankgeschäfte nur verschlüsselte Internetverbindungen. Sie erkennen sie an dem Schlosssymbol im Browser und daran, dass die Adresse mit „https//“ beginnt.



Was bei Datenmissbrauch zu tun ist:

- ➔ Haben Sie aus Versehen Daten preisgegeben? Dann ändern Sie wenn möglich sofort Ihre PIN und informieren Sie die <<Name der Bank>>.
- ➔ Sperren Sie umgehend Ihr Konto, wenn Sie glauben, dass ein Dritter Ihre PIN/TAN hat oder Ihnen beim Onlinebanking etwas ungewöhnlich erscheint. Benachrichtigen Sie dazu die <<Name der Bank>>.
- ➔ Löschen Sie die E-Mail nicht, die Sie zur Eingabe der Daten veranlasst hat! Stellen Sie diese der <<Name der Bank>> und der Polizei zur Verfügung.

Allgemeine Sicherheitstipps fürs Onlinebanking:

- ➔ Geben Sie nie sicherheitsrelevante Daten per E-Mail an Dritte weiter. Kein Bankmitarbeiter wird nach Ihren PINs oder TANs fragen.
- ➔ Verwenden Sie beim Onlinebanking nur Computer, von denen Sie wissen, dass sie frei von schädlichen Programmen sind. Achten Sie darauf, dass Sie aktuelle Antiviren- und Firewallprogramme im Einsatz haben.
- ➔ Bevor Sie das Onlinebanking auf dem Rechner starten, schließen Sie alle anderen Browserfenster.
- ➔ Speichern Sie vertrauliche Daten wie PIN, Passwörter oder Kreditkartennummern niemals auf Ihrem Computer!
- ➔ Ändern Sie regelmäßig Ihre PIN und Passwörter. Bei der Wahl Ihres selbst gewählten Kennworts sollten Sie vermeiden, was einfach zu erraten ist: Geburtstage, Telefonnummern, aber auch bekannte oder regelmäßige Zahlenkombinationen zum Beispiel „0815“ oder „12345“.
- ➔ Überprüfen Sie Ihre Kontoumsätze. Neue Transaktionen sollten sofort sichtbar sein. Melden Sie Unregelmäßigkeiten der <<Name der Bank>>.
- ➔ Vereinbaren Sie ein Tageslimit für Onlineüberweisungen. So kann möglicher Schaden von vornherein begrenzt werden.

