

Was ist Phishing? - Methoden der Betrüger - Schutz - Was tun? - Quellen

Was ist Phishing?

Wiederholt machen Warnungen vor Phishing-attacken die Runde und Kreditinstitute müssen vorsorglich Ihr Angebot vom Web nehmen, um grösseren Schaden für Ihre Kunden abzuwehren.

Der Begriff Phishing setzt sich aus den englischen Wörtern "Password" und "Fishing" zusammen. Mittels verschiedener Tricks versuchen Betrüger Passwörter von Internetbenutzern zu „fischen“, um sich damit unerlaubt Zugang zu deren Konten von Kreditkarten, Internet Banking oder Auktionen zu beschaffen. Auch könnten sich Betrüger in Online-Dienste einloggen und unter falscher Identität Schaden anrichten.

Methoden

Früher gab es bereits ähnliche Betrügereien, wie z.B. der „Enkeltrick“. Hier versuchten die Betrüger auf telefonischem Weg, sich das Vertrauen der Opfer zu erschleichen und ihnen vertrauliche Informationen zu entlocken.

Im Internet sind solche Tricks einfacher zu erstellen und haben eine weitaus grössere Verbreitung. In Form einer meist offiziell gestalteten E-Mail, inklusive Logo einer bekannten Firma, versenden die Betrüger Aufforderungen nach Eingabe von persönlichen Daten. In der Email ist meist ein Link eingebaut, der einem zu einer täuschend echt

- **Versenden Sie niemals persönliche Angaben wie Benutzernamen, Kontonummern und Passwörter per Email.**
- **Öffnen Sie kritische Webseiten, wie z.B. Ihre Onlinebank nur über einen selbstangelegten Bookmark/Favorit oder über manuelle Eingabe der Adresse im Browser.**
- **Stellen Sie sicher, dass persönliche Daten nur über verschlüsselte Webseiten verschickt werden.**
- **Überprüfen Sie Ihre Bankauszüge und informieren Sie Ihr Kreditinstitut oder die Behörden, falls Missbrauch Ihrer Daten vorliegt.**

gemachten Website führt, die fast identisch aussieht, wie z.B. die Website Ihrer Bank, Post oder anderen Institution.

Unter Vorwand von z.B. Sicherheitsproblemen, verlangen die Betrüger die Eingabe von Passwörtern und drohen bei Verweigerung mit Sperrung des Kontos. Die Eingabe der Passwörter gelangt natürlich nicht an Ihre Bank, sondern in die Hände der Betrüger.

Eine Andere Variante bindet ein Formular direkt in die Email ein, wo die persönlichen Daten hinterlegt und abgeschickt werden sollen.

Schutz – Was tun?

- Seriöse Banken, Auktionshäuser oder andere Institutionen werden Sie nie über E-Mail, Telefon oder per Post nach ihrem Passwort fragen.
- Passwörter sind persönlich und nur Ihnen und dem System für das sie gedacht sind bekannt. Selbst Mitarbeiter Ihrer Bank können Ihre Passwörter nicht einsehen und werden niemals danach fragen.
- Löschen Sie ein verdächtiges Email umgehend und kontaktieren Sie Ihre Bank, falls Sie nicht sicher sind, wer Sie kontaktiert hat. Melden Sie Missbrauch der angegriffenen Institution, damit diese Gegenmassnahmen einleiten und Ihre Kunden aufklären können.
- Schützen Sie Ihren Rechner mit einem aktuellen Virens scanner und einer Firewall.

Quellen

Meldestelle Bundesamt: <http://www.cybercrime.admin.ch/>
Beispiel Phishingattacke: <http://www.securityinfo.ch/migros-phishing.html>
Anti Phishing Plattform: <http://www.antiphishing.org/>