Phishing

Darunter versteht man das „Abfischen“ von Passwörtern durch Kriminelle mithilfe von gefälschten Webseiten oder betrügerischen E-Mails.

Vorgehensweise

Nicht umsonst klingt der Begriff „Phishing“ nach Angeln: Das Kunstwort aus „Password“ und „Fishing“ bezeichnet das kriminelle Abfischen von sensiblen Zugangsdaten für das Internet-Banking oder andere persönliche Online-Geschäfte. Die Betrüger werden dabei meist auf folgendem Weg aktiv: Gefälschte E-Mails, die angeblich von Banken oder Firmen stammen, fordern Nutzer dazu auf, über bestimmte Links Webseiten zu öffnen und dort ihre Benutzerdaten einzugeben. Als Gründe werden oft dringende Sicherheitsprobleme oder drohende Sperrungen von Konten angegeben. Folgendie Adressaten den angegebenen Links, so landen sie auf gefälschten Seiten – und die Kriminellen „fischen“ Passwörter und sonstige Benutzerdaten ab.

Sicherheitsmaßnahmen gegen Phishing

Computer und Smartphones sollten gleichermaßen mit einer aktuellen Virenschutzsoftware ausgerüstet sein und diese sollte auch immer wieder aktualisiert werden.

Mit Passwörtern und Benutzerdaten sollte man generell sehr vorsichtig umgehen und sie nicht leichtfertig preisgeben.

E-Mails von Banken und Unternehmen, die eine Aufforderung zum Einloggen unter einem bestimmten Link enthalten, können gefälscht sein. Im Zweifelsfall sollte man lieber direkt nachfragen.

Wer bei Online-Banking oder anderen sensiblen Geschäften die Internetadresse manuell neu eingibt und die Seiten nicht einfach durch den Klick auf Links öffnet, vermeidet Risiken.

Weiterführende Informationen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet online weitere Hinweise und Hintergrundinformationen rund um Phishing.

Zurück