Cybercrime: Phishing und Co.

06.09.2018
von

Altmann, Kathleen

Kurzgefasst

Weit verbreitet ist immer noch der Datenklau - das sogenannte Phishing: Betrüger verpacken Links in E-Mails oder SMS, die Ihnen dann vermeintlich von Ihrer Bank geschickt werden. Ein falscher Klick, und eine Schadsoftware installiert sich auf Ihrem PC oder Smartphone, um nach sensiblen Daten „fischen“ zu können (Phishing).

Weit verbreitet ist immer noch der Datenklau - das sogenannte Phishing: Betrüger verpacken Links in E-Mails oder SMS, die Ihnen dann vermeintlich von Ihrer Bank geschickt werden. Ein falscher Klick, und eine Schad-software installiert sich auf Ihrem PC oder Smartphone, um nach sensiblen Daten „fischen“ zu können (Phishing).

Wichtig zu wissen: Ihre Bank wird Sie niemals per E-Mail um Nennung oder Eingabe Ihrer persönlichen Daten wie PIN oder Passwörter bitten. Ihre Bank wird auch nicht von Ihnen verlangen, Ihr Konto zu aktivieren, zu „entsperren“ oder es zu „aktualisieren“. Seien Sie grundsätzlich misstrauisch, wenn Sie solche oder ähnliche Nachrichten erhalten.

Für Online-Banking-Kunden gehört die Installation von Virenscanner und Firewall grundsätzlich zu den Sorgfalts-pflichten. Die Software von PC und Smartphone sollte außerdem stets auf dem neuesten Stand sein. Tätigen Sie Bankgeschäfte nie über einen fremden Rechner (z.B. Internet-Café) und nutzen Sie nur autorisierte Apps Ihrer Bank.

Beim Umgang mit Passwörtern, PINs und co. ist ebenfalls Vorsicht angesagt. Niemals sollten solche Daten in Apps, der Cloud oder auf Ihrer Festplatte gespeichert werden, auch nicht als Telefonnummer verschlüsselt in den Handy-Kontakten.

Schlagworte

Phishing
Verbraucher
PIN
Onlinebanking
Verbraucherschutz
Dossier Cybercrime

Blog

Damit Bankkunden ihre Transaktionen sicher und ohne Sorge durchführen können, ist es wichtig, diese und weitere Regeln zu befolgen.