



Phishing-Mails erwecken auf den ersten Blick den Anschein von Echtheit und Seriosität, bei genauerem Hinsehen sind sie aber leicht zu enttarnen.

Mehr Phishing-Fälle in Österreich

Die Zahl der Phishing-Attacken ist angestiegen. Die Beamten des Bundeskriminalamts bearbeiteten im Jänner 60 Fälle.

Es beginnt mit einer offiziell anmutenden E-Mail einer Bank oder eines Versandhauses. Der Empfänger des E-Mails wird aufgefordert, Konto- und Zugangsdaten bekannt zu geben. Hinter den Mails stecken Betrüger. Sie räumen die Konten ihrer Opfer leer, sobald sie die Informationen haben.

Die Beamtinnen und Beamten des österreichischen Bundeskriminalamts verzeichnen seit Mitte Oktober 2005 ein vermehrtes Auftreten so genannter „Phishing“-Attacken. Immer wieder fallen Menschen auf die Tricks der Betrüger herein. Im Bundeskriminalamt wurden im Jänner 2006 etwa 60 Phishing-Fälle bearbeitet.

Der Begriff „Phishing“ ist eine Kombination aus den Wörtern „Passwort“ und „Fishing“. Die Täter „fischen“ nach den Passwörtern ihrer Opfer. Die Methoden der Datenbeschaffung variieren leicht. Die Täter fordern,

getarnt als Bankinstitut, in ihrem Mail zum Besuch einer bestimmten Webseite auf, wo der Bankkunde seine Zugangsdaten für das Bankkonto hinterlassen soll. Oder sie schicken, in die Mail eingebettet, das Formular gleich mit, in das das Passwort eingegeben werden soll.

Oft verlangen sie die Eingabe von zwei Transaktionsnummern (TAN). Haben sie die Nummern bekommen, ändern sie mit der einen TAN den Zugangscod zum Konto, so dass der Eigentümer keinen Zugriff mehr hat. Mit der anderen Nummer räumen sie das Konto leer.

Leicht erkennbar. Phishing-Mails erwecken auf den ersten Blick den Anschein von Echtheit und Seriosität, bei genauerem Hinsehen sind sie aber leicht zu enttarnen. Die Anrede in den Schreiben ist unpersönlich wie „Sehr geehrter Herr“ oder „Sehr geehrter Kunde“. Im

üblichen Geschäftsverkehr wird man mit dem Namen angesprochen. Die Mailtexte beinhalten oft schwere Rechtschreib- oder Grammatikfehler. Beispielsweise werden Umlaute nicht beachtet und ungebräuchliche Wörter wie „eintasten“ anstatt „eingeben“ verwendet. Banken und Versandhäuser fordern nie per E-Mail zur Bekanntgabe persönlicher Daten auf.

Opfer eines Phishing-Angriffs sollten unverzüglich die Polizei und das entsprechende Unternehmen informieren, in dessen Namen die falsche Mail geschickt wurde. Die gefälschte Mail sollte gespeichert und für polizeiliche Ermittlungen bereitgehalten werden. Wenn möglich, sollte man die gestohlenen Passwörter sofort ändern. So werden die Originalcodes für die Betrüger unbrauchbar.

www.bmi.gv.at/kriminalpolizei/