Phishing erkennen

Kaum ein Internet-Nutzer bleibt von diesen raffinierten Phishing-Mails verschont. Dieser ans englische „fishing“ (angeln, fischen) angelehnte Hacker-Begriff umschreibt den Versuch, den Mail-Empfängern sensible Daten zu entlocken, vor allem Kontonummern und Pins. Unter dem Vorwand, irgendein Fehler müsse behoben werden, wird man als (zunächst) Ahnungsloser aufgefordert, einen Link anzuklicken und die erforderlichen Daten einzugeben. Doch das Befolgen einer solchen Aufforderung, und sei sie noch so höflich eingekleidet, kann verheerende Folgen haben. Daher seien Schutzvorkehrungen zu treffen, wird immer wieder empfohlen. Ein Tipp zur Erkennung eines Phishing-Angriffs lautet, auf korrekte Rechtschreibung in den Mails zu achten. So war mir dieser Tage sofort klar, dass die „Wichtige Mittlerung“ nicht von der ING-Bank, sondern von einem Hacker stammte. Rechtschreibkontrolle genügt aber nicht immer. Phishings-Mails von Banken, die fehlerfrei und mit „echtem“ Firmenlogo daherkommen, machen sich eher anders verdächtig, etwa durch unpersönliche Anrede, wie unlängst die Phishing-Mails einer Sparkasse und der Postbank. Auf einem ziemlich weiten Feld ist fehlerhafte Rechtschreibung allerdings gar kein Indiz für Phishing. Ich denke da an gelegentliche Posts und Kommentare in Süd-Duisburger Chat-Gruppen. Ihre Texte stammen gewiss von harmlosen Mitbürgern und nicht von raffinierten Datenfischern. **HOS**