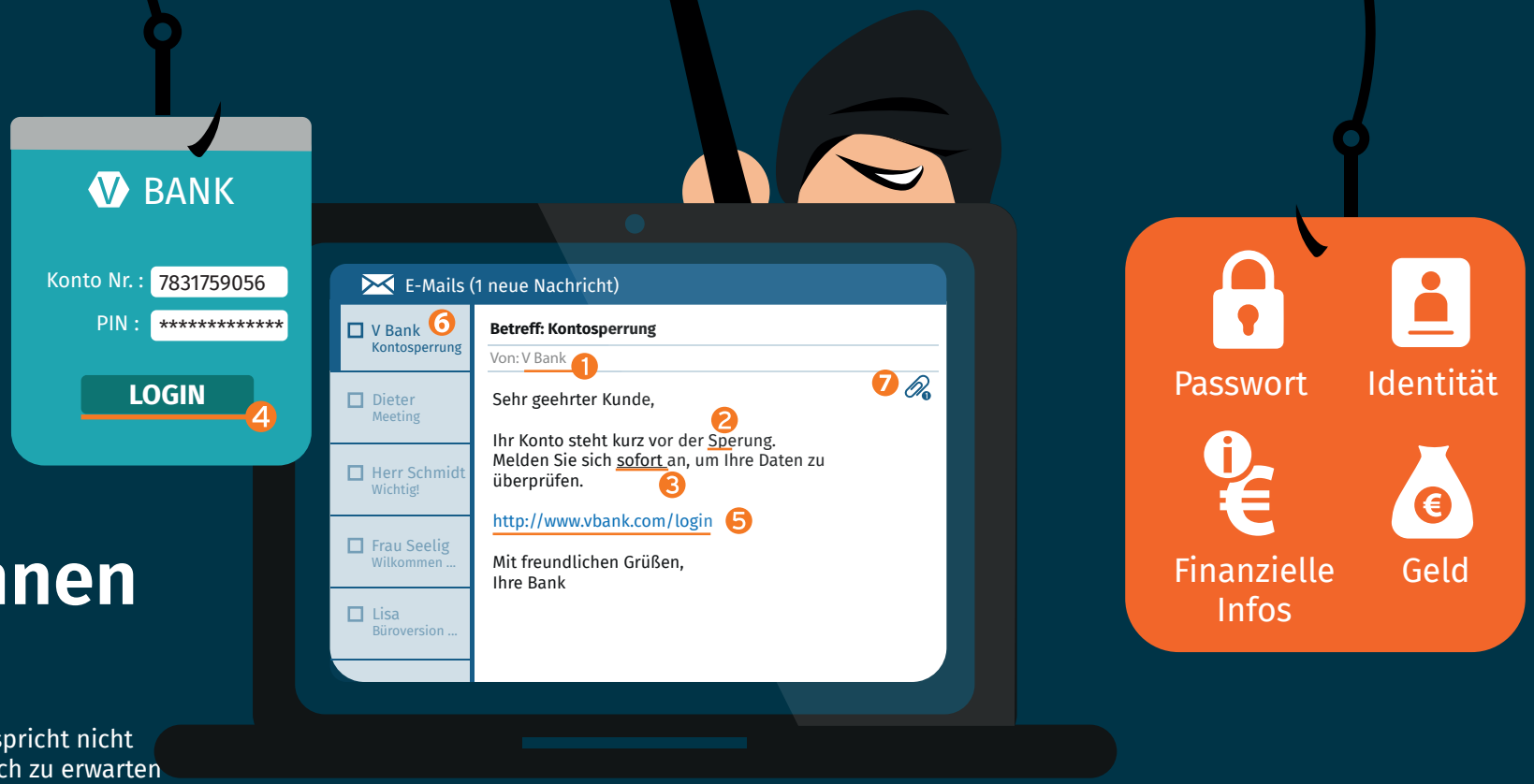

Phishing Mails erkennen

1 Absender-E-Mail Adresse

Die Adresse (nicht der Name) entspricht nicht der Absenderadresse, die eigentlich zu erwarten wäre.

2 Grammatik- und Rechtschreibfehler

Am einfachsten zu durchschauen sind E-Mails, die in fehlerhaftem Deutsch geschrieben sind. Meistens wurden sie nicht in Deutsch verfasst, sondern sind mit einem Übersetzungsdienst aus einer anderen Sprache übersetzt worden. Ein weiterer Hinweis auf solche E-Mails sind Zeichensatzfehler, wie etwa kyrillische Buchstaben oder auch fehlende Umlaute.

3 Dringender Handlungsbedarf

Wenn Sie via E-Mail aufgefordert werden, ganz dringend und innerhalb einer bestimmten (kurzen) Frist zu handeln, sollten Sie ebenfalls stutzig werden. Insbesondere, wenn diese Aufforderung mit einer Drohung verbunden ist - beispielsweise, dass sonst die Kreditkarte oder der Online-Zugang gesperrt werden.

4 Eingabe von Daten

Die Aufforderung, persönliche Daten sowie möglicherweise PIN oder TAN einzugeben, ist ein weiterer Hinweis. Banken und Online-Zahlungsdienste werden Sie um so etwas nicht per E-Mail bitten. PIN und TAN werden von Geldinstituten niemals telefonisch oder per E-Mail abgefragt; dies zählt zu den wesentlichen Sicherheitsregeln.

5 Links in der Mail

Nicht "blind" klicken, sondern den Mauszeiger darüber halten und nach einem Augenblick (zumindest in Outlook) wird angezeigt, wohin der Link eigentlich führt. Jetzt die Adresse sorgfältig prüfen, meistens ähnelt sie einer korrekten Adresse. Amacon, Amazom oder Amazonde.com statt Amazon, 189z-sparkasse.com oder .ab-bank.kundenservice.de.

6 Mail Kopfzeile (Header)

Manche Phishing Mails sind sehr gut gemacht. Die Absender-E-Mail-Adresse scheint vertrauenswürdig, der Link im Text auch, das Deutsch ist flüssig. Trotzdem muss diese E-Mail nicht echt sein. Auch Absenderangaben von E-Mails lassen sich fälschen. Wenn Sie - um letzte Zweifel auszuräumen - das prüfen wollen, müssen Sie die Mail Kopfzeile anschauen. Dort steht die IP-Adresse des Absenders. Nur diese ist fälschungssicher und gibt Aufschluss über den tatsächlichen Absender.

7 Mail Anhänge

Office Dokumente im Anhang nur öffnen, wenn das Dokument erwartet wird und von einem bekannten Absender stammt. Wenn man das Dokument doch öffnet und man dann, um die Datei ansehen zu können, in einem Dialogfenster bestätigen muss, dass Makrofunktionen aktiviert werden dürfen, wird es kritisch. Wer dem zustimmt, setzt die Infizierung in Gang. Also äußerste Vorsicht!