Checkliste Phishing-E-Mails

So schützen Sie Ihre persönlichen Daten

E-Mails von Betrügern, die an Ihre persönlichen Daten wie Kontozugänge, Passwörter und Pins gelangen wollen, sind oft täuschend echt. Mit etwas Vorsicht und dem Wissen, worauf Sie achten müssen, lassen sich die sogenannten «Phishing-E-Mails» von Kriminellen aber oftmals erkennen.

1. Seien Sie besonders vorsichtig bei E-Mails, die Sie nicht erwartet haben.
2. In Phishing-E-Mails werden Sie aufgefordert, vertrauliche Daten wie Passwörter, TANs, PINs, Kunden- und Zugangsnummern im Zusammenhang mit der Angabe der eigenen Kontoverbindung zu nennen.
3. Die E-Mail beinhaltet verschiedene Schriftarten und -grössen.
4. Die E-Mail weist Grammatik- und Rechtschreibfehler auf.
5. Umlaute werden nicht richtig (gar nicht oder als ae, oe, ue) geschrieben.
6. Die Anrede ist unpersönlich (Sehr geehrte Kunden des ABC-Finanzinstituts).
7. Die Grussformel ist unpersönlich (Ihre ABC-Bank).
8. Eine Phishing-E-Mail ist nicht an Sie persönlich, sondern z. B. an eine Sammeladresse adressiert (kunden@abc-geldhaus.ch).
9. Man droht Ihnen in der E-Mail (z. B. mit Kontosperrung).
10. Der E-Mail hängt ein Formular an oder sie enthält einen Link zu einem Formular, in das Sie persönliche Daten wie PIN, TAN, Kontonummer, Kunden- und Zugangsnummern eingeben sollen.
11. Die E-Mail enthält einen Link, der auf den ersten Blick täuschend echt ist. Ungewöhnlich oder falsch geschriebene Bestandteile der URL weisen aber auf eine falsche Internet-Adresse hin.

Darauf sollten Sie noch achten:

Verwenden Sie zur Anmeldung bei Finanzinstituten niemals einen Link, der per E-Mail zugeschickt wurde oder per QR-Code eingescannt werden muss.

Geben Sie die Adresse zur Anmeldeseite ihres Finanzinstituts immer manuell ein.

Füllen Sie keine Formulare aus, die per E-Mail geschickt wurden und zur Eingabe von Anmeldeinformationen auffordern.

Geben Sie in Telefongesprächen keine vertraulichen Informationen heraus.