ACHTUNG,

PHISHING

SO ERKENNEN SIE BETRÜGERISCHE E-MAILS

RECHTSCHREIB- UND GRAMMATIKFEHLER

- Schlechtes Deutsch oder eine fremde Sprache können auf Phishing hindeuten.

DATEIANHÄNGE ODER UNBEKANNTE LINKS

- Öffnen Sie keine unbekannten Anhänge und Links.

HANDLUNGSDRUCK UND DROHUNGEN

- Die E-Mail fordert Sie zu sofortigem Handeln auf und droht mit Konsequenzen? Seriöse Anbieter setzen Sie nie unter Druck.

UNPERSÖNLICHE ODER FALSCHE ANREDE

- Achtung: Manchmal wird trotzdem Ihr richtiger Name verwendet - das macht die Mail nicht automatisch echt.

AUFFORDERUNG ZUR DATENEINGABE

- Kein seriöser Anbieter fragt per E-Mail nach PIN, Passwort oder anderen sensiblen Daten.

UNGEWÖHNLICHER ABSENDER

- Achten Sie auf Absenderadressen – schon kleinste Abweichungen können auf Betrug hindeuten.

SO KÖNNEN SIE REAGIEREN

Lassen Sie sich die Echtheit einer E-Mail im Zweifel telefonisch bestätigen

Aktivieren Sie die Zwei-Faktor-Authentifizierung für Ihre Benutzerkonten

Installieren Sie Virenschutz-Programme, die vor unseriösen Links warnen

Löschen Sie verdächtige Mails oder melden Sie sie der Verbraucher-zentrale

QUELLEN: VERBRAUCHERZENTRALE & BUNDESAMT FÜR SICHERHEIT