



Sicherheitscheck für Ihr Postfach

5 Tipps, wie Sie betrügerische Mails rund um Steuern, Finanzen & Co. erkennen

Mit digitalem Spürsinn und einem wachsamen Blick: So bleiben Sie souverän im Umgang mit Phishing-Mails - wir unterstützen Sie dabei!

1. Wer ist der Absender?

- Offizielle Stellen wie das Bundeszentralamt für Steuern oder die Finanzverwaltung nutzen ausschließlich Domains wie @bzst.bund.de oder @elster.de.
- Achtung bei Abwandlungen wie @bzst-zahlungsfrist.com, @steuer-infos.net – das sind betrügerische Fantasieadressen.

2. Wozu werden Sie aufgefordert?

- Steuerbescheide mit Zahlungsaufforderungen kommen **niemals per E-Mail**, sondern per Post bzw. im Portal.
- E-Mails mit Fristdruck, Drohungen oder Forderungen zur sofortigen Zahlung sind klare Warnsignale.

3. Ist das eine echte Rechnung oder nur ein Fake?

- Offizielle Schreiben enthalten keine Begriffe wie „Rechnung“, „Stückpreis“ oder „MwSt.“ bei Steuerforderungen.
- Fehlt die Steuernummer, ist das Logo pixelig oder der Text fehlerhaft? Dann Finger weg!

4. Wohin soll das Geld gehen?

- Eine IBAN, die ins Ausland führt (z. B. Spanien), ist **definitiv kein Konto deutscher Steuerbehörden**.
- Zahlungen dürfen nur an offizielle Konten geleistet werden – im Zweifel rufen Sie uns an.

5. Der gesunde Menschenverstandstest:

- "Würde mir mein Steuerberater nicht Bescheid geben, wenn ich wirklich etwas verpasst hätte?"
- Wenn eine Nachricht beunruhigt oder unklar ist: Erst mit uns sprechen, bevor Sie handeln.