SACHSEN-ANHALT

Pressemitteilung: 24 / 2025
Magdeburg, den 04.06.2025

Ministerium der Finanzen

Warnung vor Betrugsversuchen

Immer wieder kommt es vor, dass im Namen der Steuerverwaltung, bspw. eines Finanzamtes, des Finanzministeriums oder des Bundeszentralamtes für Steuern, Betrugs-E-Mails versendet werden (sog. Pishing-Mails). Bitte beachten Sie unbedingt, dass die Steuerverwaltung niemals in einer E-Mail Informationen, wie die Steuernummer, Kontoverbindungen, Kreditkartennummern, PIN oder die Antwort auf Ihre Sicherheitsabfrage, anfordert. Auch Zahlungsaufforderungen erhalten Sie niemals über diesen Weg.

Beispiele für diese Schreiben finden Sie auf den Seiten des Bundeszentralamtes für Steuern.

Hier eine Übersicht über gängige Betrugsmethoden im Namen von Steuerbehörden und ELSTER:

- Gefälschte Steuerbescheide per Post: Kriminelle versenden täuschend echte Steuerbescheide, in denen zur Überweisung auf ein betrügerisches Konto aufgefordert wird.
- Phishing-E-Mails im Namen von ELSTER, Finanzämtern oder dem Bundeszentralamt für Steuern: Die Empfänger werden aufgefordert, auf Links zu klicken, Formulare auszufüllen oder persönliche Daten einzugeben, etwa zur angeblichen Steuererstattung oder Nachzahlung.
- Gefälschte Webseiten: Über Links in E-Mails oder SMS gelangen Betroffene auf täuschend echte, aber betrügerische Seiten, auf denen sensible Daten abgefragt werden.
- Betrügerische SMS oder automatisierte Anrufe: Es wird behauptet, eine Kontoverifizierung oder Steuererstattung sei nötig, oft verbunden mit der Aufforderung, Daten preiszugeben oder Zahlungen zu leisten.
- Falsche Hilfeangebote: Anrufe oder E-Mails, in denen vermeintliche Mitarbeitende der Finanzverwaltung Unterstützung anbieten und dabei gezielt nach sensiblen Daten fragen.
- QR-Code-Betrug: E-Mails oder Briefe enthalten QR-Codes, die auf gefälschte Webseiten führen, um Daten abzugreifen.
- Gefälschte Webseiten 2: Im Zusammenhang mit gefälschte Rechnungen im Namen des Bundeszentralamts für Steuern gibt es täuschend echte Phishing-Webseiten, die bei Google-Suchen ganz oben in der Trefferliste erscheinen und mit Bank- und Filialauswahl sowie Eingabemaske gezielt sensible Daten abfragen.

Woran erkennt man die Betrugsversuche?

- Unpersönliche Anrede: Echte Behörden verwenden Ihren Namen und Ihre Steuer-ID, Betrüger oft allgemeine Formulierungen wie „Sehr geehrte Damen und Herren“.

- Fehlerhafte oder widersprüchliche Angaben: Unterschiedliche Daten, fehlerhafte Steuernummern, Rechtschreibfehler oder unpassende Fachbegriffe im Schreiben.
- Aufforderung zu schnellen Zahlungen: Besonders bei angeblich dringenden Nachforderungen mit kurzer Zahlungsfrist ist Vorsicht geboten.
- Ungewöhnliche Zahlungswege: Forderung nach Überweisung auf ausländische Konten oder per Link in einer E-Mail – echte Behörden nutzen in der Regel nur inländische Konten und keine Zahlungslinks.
- Fehlende oder falsche Kontaktdaten: Kein Ansprechpartner, keine Telefonnummer oder E-Mail-Adresse des zuständigen Sachbearbeiters.
- Unerwartete Kontaktaufnahme: Behörden fordern nie per E-Mail, SMS oder Telefon zur Preisgabe sensibler Daten oder zur Zahlung auf.
- Überprüfung der Absenderadresse: E-Mail-Adressen, die offiziellen Adressen nur ähneln, aber kleine Abweichungen enthalten.“

Impressum:

Ministerium der Finanzen Pressestelle

Editharing 40
39108 Magdeburg

Tel: (0391) 567-1105
Fax: (0391) 567-1390

Mail: presse.mf@sachsen-anhalt.de