



Aktuelle Phishing-Welle: Erhöhte Aufmerksamkeit in Steuerkanzleien erforderlich

RA Christian Michel, Referatsleiter Recht und Berufsrecht, DStV, Berlin

Aus dem Kreis der regionalen Steuerberaterverbände und zahlreicher Steuerberatungskanzleien erreichen uns derzeit Hinweise auf vermehrte **Phishing-Angriffe und kompromittierte E-Mail-Konten**.

Besonders tückisch: Nicht immer stammen verdächtige Nachrichten von unbekannten Absendern. Werden E-Mail-Konten von Kanzleien oder Geschäftspartnern kompromittiert, können betrügerische Nachrichten unter einem **bekannten und vermeintlich vertrauenswürdigen Absender** versendet werden. Aktuell wurde uns beispielsweise von E-Mails berichtet, in denen Empfänger unter einem geschäftlich plausiblen Vorwand – etwa zur Klärung von Kapitalkonten – zum Öffnen eines Anhangs oder Anklicken eines Links aufgefordert werden. Unter anderem kursieren auch **professionell gestaltete Fake-Mails im Namen von ELSTER** ([siehe Muster mit entfernten betrügerischen Links](#)). Darin werden angebliche Einkommensteuererstattungen angekündigt. Für die Auszahlung sollen die Empfänger über einen Link eine „digitale Identitätsprüfung“ durchführen und sich dabei mit einem Zahlungsmittel legitimieren. Auch vermeintliche Rechtsgrundlagen sollen der Nachricht Seriosität verleihen.

Unsere dringende Empfehlung:

Bitte öffnen Sie keine Links und geben Sie keine persönlichen Zahlungsdaten ein. Sensibilisieren Sie außerdem Ihr gesamtes Kanzleiteam.

Rufen Sie die wichtigsten **Grundsätze zur Cybersicherheit** in Erinnerung:

- **Auch bekannte Absender kritisch prüfen.** Ein vertrauter Absender ist keine Garantie für die Echtheit einer Nachricht.
- **Unerwartete Links und Anhänge nicht vorschnell öffnen.** Besser zunächst nachfragen, insbesondere wenn die Nachricht ungewöhnlich, dringlich oder nicht eindeutig einem bekannten Vorgang zuzuordnen ist.
- **Im Zweifel eine Bestätigung über einen zweiten Kommunikationsweg einholen.** Zur Sicherheit die bekannte Telefonnummer des Absenders nutzen, anstatt auf die verdächtige E-Mail zu antworten.
- **Verdächtige Nachrichten intern melden** und einen klaren Ansprechpartner bzw. Prozess für solche Fälle festlegen.
- **Mitarbeitende regelmäßig sensibilisieren und schulen.** Phishing ist nicht allein ein technisches, sondern auch ein organisatorisches Risiko.

Cybersicherheit im Fokus:

Schaffen Sie in Ihrer Kanzlei eine Kultur, in der Mitarbeitende bei Unsicherheit lieber einmal mehr nachfragen und verdächtige Nachrichten melden. Gerade bei professionell gestalteten Angriffen kann Aufmerksamkeit im Team eine entscheidende zusätzliche Schutzebene sein.

Hier setzen wir auch beim diesjährigen **Deutschen Steuerberatertag vom 4. bis 6. Oktober 2026 in Bonn** an. Unter dem Titel „**Cyberangriff in der Kanzlei: Was wirklich passiert – und wie Sie richtig reagieren**“ beleuchten Experten aus den Bereichen Cybersecurity, Cyberversicherung sowie Berufsangehörige aktuelle Bedrohungen, wirksame Präventionsmaßnahmen und die entscheidenden Schritte im Ernstfall. Freuen Sie sich auf praxisnahe Einblicke, spannende Impulse und konkrete Handlungsempfehlungen für mehr Cybersicherheit in Ihrer Kanzlei.

Melden Sie sich gleich an unter www.steuerberatertag.de
[Deutscher Steuerberatertag – 04. bis 06. Oktober 2026 in Bonn](#)