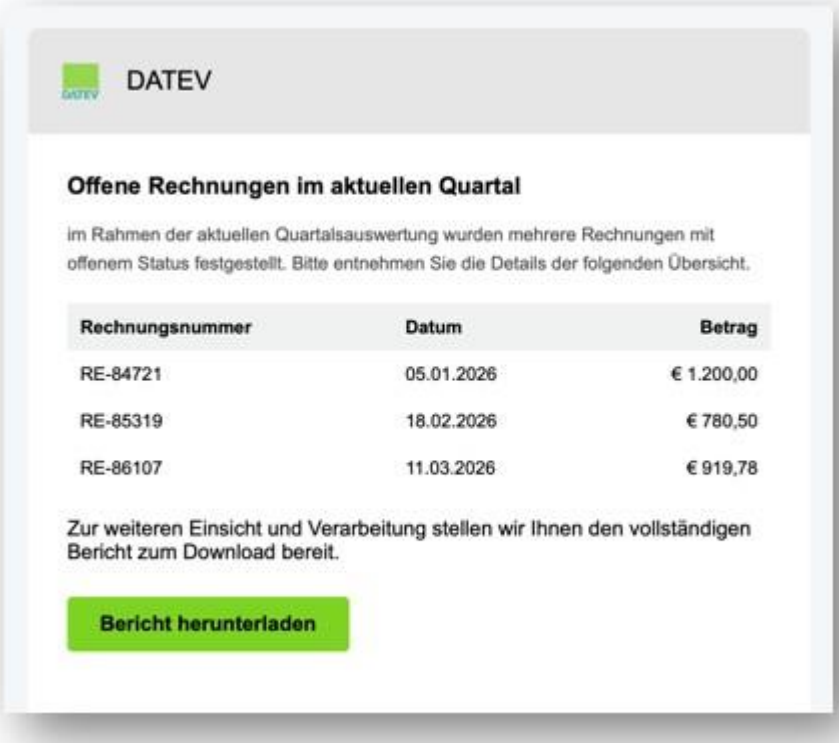
Phishing-Warnung: Gefälschte DATEV-Rechnungen

Verschiedene Anwender berichten im Mai 2026 von täuschend echt gestalteten Phishing-Mail, die angeblich von DATEV stammt und über „offene Rechnungen im aktuellen Quartal“ informieren.

Die E-Mails wirken auf den ersten Blick seriös: Sie enthalten das DATEV-Logo, konkrete Rechnungsnummern, Beträge sowie einen Button zum Herunterladen eines angeblichen Berichts. Tatsächlich handelt es sich jedoch um einen Betrugsversuch.

Aktuell scheinen diese gefälschten Rechnungen nur an Gastro-Unternehmen zu gehen – deswegen warnt speziell die DEHOGA (Deutscher Hotel- und Gaststättenverband). Es ist aber davon auszugehen, dass diese Betrugsmasche auch in anderen Branchen auftauchen wird.



DATEV

Offene Rechnungen im aktuellen Quartal

im Rahmen der aktuellen Quartalsauswertung wurden mehrere Rechnungen mit offenem Status festgestellt. Bitte entnehmen Sie die Details der folgenden Übersicht.

Rechnungsnummer	Datum	Betrag
RE-84721	05.01.2026	€ 1.200,00
RE-85319	18.02.2026	€ 780,50
RE-86107	11.03.2026	€ 919,78

Zur weiteren Einsicht und Verarbeitung stellen wir Ihnen den vollständigen Bericht zum Download bereit.

Bericht herunterladen

Besonders wichtig:
DATEV stellt Rechnungen in der Regel ausschließlich an Steuerberater, Kanzleien oder Unternehmen im Rahmen bestehender Vertragsbeziehungen. Sollten Sie kein DATEV-Kunde sein und direkte Rechnungen der DATEV empfangen, stellt sich also eigentlich nicht die Frage, ob diese Rechnungsstellung berechtigt ist.

Worauf Sie achten sollten:

Woran Sie den Betrugsversuch erkennen können:

- **Unerwartete Rechnungsinformationen:** Sie erhalten eine E-Mail zu angeblich offenen DATEV-Rechnungen, obwohl Ihnen keine offenen Posten bekannt sind oder Sie diese Kommunikation nicht erwarten.
- **Download-Aufforderung:** Die E-Mail enthält eine Schaltfläche oder einen Link, über den ein Bericht, eine Rechnung oder eine Übersicht heruntergeladen werden soll.
- **Verdächtige Absenderadresse:** Die angezeigte Absenderadresse ist keine valide DATEV-E-Mail-Adresse. Auch wenn der Absendername „DATEV“ enthält, kann es sich um E-Mail-Spoofing handeln.
- **Unklare oder generische Ansprache:** Die E-Mail ist häufig allgemein formuliert und nennt keine konkreten vertraglichen oder abrechnungstechnischen Bezüge. Meist fehlt die Beraternummer oder eine falsche wird angegeben.
- **Abweichende Links:** Die Zieladresse des Download-Links verweist beim Mouseover nicht auf eine bekannte DATEV-Domäne (datev.de), sondern auf externe oder unbekannte Domänen.

Die Gefahr:

Ein Klick auf den Download-Button kann bereits ausreichen, um Schadsoftware wie Trojaner oder Ransomware auf Ihrem System zu installieren oder Zugangsdaten abzugreifen.
Unsere Empfehlung:

1. Klicken Sie nicht auf Links oder Download-Buttons
2. Öffnen Sie keine Anhänge
3. Prüfen Sie die Absenderadresse sorgfältig
4. Kontaktieren Sie im Zweifel Ihren Steuerberater
5. Löschen oder melden Sie verdächtige E-Mails als Phishing

Bitte sensibilisieren Sie auch Ihre Mitarbeiter für diese Betrugsmasche.

Im Zweifel gilt: Lieber einmal mehr prüfen als einmal falsch klicken.

Bleiben Sie wachsam und schützen Sie Ihre Daten.