AEDIAEVUM LEITFADENREIHE

Identitätsdiebstahl: Mehr als nur ein privates Problem

Warum gestohlene Identitäten auch Ihren Arbeitsplatz gefährden können

Für Berufstätige, Selbstständige und alle, die beruflich online sichtbar sind

Herausgegeben von der aediaevum Stiftung · Mühltal · Juni 2026

Eine gefälschte Rechnung im Namen des Chefs, ein geklontes LinkedIn-Profil, ein kompromittiertes E-Mail-Konto: Identitätsdiebstahl endet längst nicht an der Haustür. Er kann den Ruf und im schlimmsten Fall den Arbeitsplatz kosten.

---

1. Wie groß ist das Problem wirklich?

61 % der Internetnutzer in Deutschland wurden in den letzten 12 Monaten Opfer von Cyberkriminalität, häufig ausgehend von gestohlenen Daten (Bitkom Research 2025). Laut Sophos „State of Identity Security 2026“ erlitten 71 % der befragten Unternehmen weltweit mindestens einen identitätsbezogenen Sicherheitsvorfall, in Deutschland 62 %.

Bemerkenswert

• Zwei Drittel (67 %) der von Ransomware betroffenen Unternehmen führten den Vorfall auf einen vorausgegangenen Identitätsangriff zurück.

2. Wie aus privat beruflich wird

Das gehackte E-Mail-Konto

Über ein gekapertes Postfach lassen sich Passwörter für zahlreiche andere Dienste zurücksetzen — auch Arbeits-Tools.

Das geklonte berufliche Profil

Gefälschte LinkedIn-Profile nutzen das Vertrauen von Geschäftskontakten aus.

CEO-Fraud und Stimmklon-Betrug

Täter geben sich als Vorgesetzte aus, heute oft mit geklonten Stimmen, und fordern dringende Überweisungen.

3. Konkrete Folgen für Berufstätige

E-Mail kompromittiert	Zugriff auf Arbeits-Accounts und Kundendaten
Profil geklont	Vertrauensmissbrauch bei Kollegen und Kunden
Stimmklon-Betrug	Finanzieller Schaden, arbeitsrechtliche Folgen

4. So schützen Sie Ihre berufliche Identität

- Berufliche und private Accounts strikt trennen.
- Zwei-Faktor-Authentifizierung für alle Arbeits-Accounts.
- Öffentlich sichtbare Informationen bewusst wählen.
- Verifikationsprozesse im Unternehmen etablieren (zweiter Kanal bei Geldforderungen).
- Regelmäßig prüfen, ob eigene Daten in Datenlecks auftauchen (haveibeenpwned.com).

5. Was tun, wenn es bereits passiert ist?

1. Betroffene Konten sofort sperren oder Passwörter ändern.
2. Arbeitgeber bzw. IT-Abteilung umgehend informieren.
3. Anzeige bei der Polizei erstatten.
4. Betroffene Plattformen kontaktieren (z. B. bei geklontem Profil).
5. Geschäftskontakte warnen, falls in Ihrem Namen Nachrichten versendet wurden.

6. Ihre Checkliste für berufliche Identitätssicherheit

■	Berufliche und private Accounts nutzen unterschiedliche Zugangsdaten.
■	Alle beruflich genutzten Accounts sind mit 2FA geschützt.
■	Es gibt einen klaren Verifikationsprozess für Zahlungsanfragen.
■	Ich habe geprüft, ob meine Daten in Lecks aufgetaucht sind.
■	Ich weiß, wen ich bei einem Vorfall sofort informieren muss.

aediaevum Stiftung · In der Röde 5 · 64367 Mühltal · Gemeinnützige Stiftung zur Förderung der Kriminalprävention
Stiftungsaufsicht: Regierungspräsidium Darmstadt · Stand: 21.06.2026 · Dieses Dokument darf kostenlos ausgedruckt und weitergegeben werden.