



Versicherungsbetrug wird immer professioneller: So schützen sich Verbraucher

Der Oktober steht als „Cybersecurity Awareness Month“ weltweit im Zeichen digitaler Sicherheit. Das ist auch im Versicherungsumfeld relevant: Gefälschte Versicherungsunterlagen, täuschend echte Webseiten oder Personen, die sich als Versicherungsvermittler ausgeben, machen Betrugsversuche immer raffinierter. Worauf Verbraucherinnen und Verbraucher achten sollten und weshalb auch Versicherer ganz genau hinschauen.

Wer eine Versicherung abschließt oder einen Schaden meldet, verlässt sich darauf, mit einer seriösen Ansprechperson zu kommunizieren. Doch genau dieses Vertrauen nutzen Betrüger zunehmend aus. Digitale Werkzeuge ermöglichen es heute, Dokumente, Websites oder Kommunikationswege täuschend echt nachzubilden. Für Verbraucherinnen und Verbraucher wird es dadurch teilweise deutlich schwieriger, echte von gefälschten Angeboten zu unterscheiden. Die Folgen können erheblich sein: Neben finanziellen Schäden droht im schlimmsten Fall die Erkenntnis, dass ein vermeintlicher Versicherungsschutz gar nicht besteht. Umso wichtiger ist es, Warnsignale frühzeitig zu erkennen und Unterlagen sorgfältig zu prüfen.

Auch Versicherungsunternehmen selbst sind immer häufiger mit Betrugsversuchen konfrontiert. Daraus ergibt sich für sie ein Balanceakt: Einerseits erwarten Kundinnen und Kunden eine schnelle und unkomplizierte Bearbeitung ihrer Anliegen. Andererseits sind sorgfältige Prüfungen notwendig, um Betrugsversuche zu erkennen und die Interessen der Versichertengemeinschaft zu schützen.

Die Bekämpfung von Versicherungsbetrug ist eine gemeinsame Aufgabe. Neben den Prüfmechanismen der Versicherer können auch Verbraucherinnen und Verbraucher mit einfachen Vorkehrungen dazu beitragen, verdächtige Aktivitäten frühzeitig zu erkennen. „Betrüger nutzen zunehmend professionelle Methoden, um Vertrauen zu erschleichen. Umso wichtiger ist es, Informationen und Dokumente kritisch zu prüfen und im Zweifel direkt beim Versicherer nachzufragen“, rät Ilja Strunk, Abteilungsleiter Compliance und Betrugsprävention bei der HanseMerkur.

Die wichtigsten Hinweise nachfolgend im Überblick.

Checkliste: So lässt sich Versicherungsbetrug erkennen

Absender genau prüfen

- E-Mail-Adressen sorgfältig kontrollieren.
- Auf Zusätze, Schreibfehler oder ungewöhnliche Domains achten.
- Für Rückfragen ausschließlich die offiziellen Kontaktmöglichkeiten des Versicherers nutzen.

Vermittler und Berater überprüfen

- Die Vermittlerregistrierung nennen lassen.

- Prüfen, ob die Person tatsächlich für das genannte Unternehmen tätig ist.
- Bei unerwarteten Kontaktaufnahmen per Telefon, E-Mail oder soziale Medien besonders aufmerksam sein.
- Impressum, Kontaktdaten und Erreichbarkeit einer Website überprüfen.

Außergewöhnliche Versprechen hinterfragen

- Besonders hohe Beitragssparnisse oder ungewöhnlich günstige Angebote kritisch prüfen.
- Tarifwechsel und Einsparungen nachvollziehbar erläutern lassen.
- Im Zweifel eine zweite Meinung einholen.

Versicherungsunterlagen sorgfältig prüfen

- Versicherungsnummer, Namen und Vertragsdaten kontrollieren.
- Auf Rechtschreibfehler, fehlende Angaben oder ungewöhnliche Formatierungen achten.
- Dokumente mit bereits bekannten Unterlagen vergleichen.
- Im Zweifel die Echtheit von Versicherungsnachweisen direkt vom Versicherer bestätigen lassen.

Niemals vorschnell zahlen

- Keine Vorauszahlungen unter Zeitdruck leisten.
- Nicht für Leistungen zahlen, deren Inhalt oder Umfang nicht vollständig bekannt ist.
- Überweisungen erst vornehmen, wenn die Identität des Ansprechpartners geprüft wurde.
- Bei Zahlungen auf Konten unbekannter Personen besondere Vorsicht walten lassen.

Gefälschte Dokumente direkt erkennen

Folgende Merkmale können auf eine Fälschung hindeuten:

- fehlende Anschriften
- unvollständige Kontaktdaten
- ungewöhnliche E-Mail-Adressen
- nicht existente Tarife oder Leistungen
- widersprüchliche Angaben in Schreiben
- gefälschte Versicherungsbestätigungen
- auffällige Logos oder Briefköpfe
- unprofessionell wirkende Internetseiten

Die wichtigsten Warnsignale auf einen Blick

- Unbekannte Vermittler melden sich unaufgefordert.
- Es wird eine Vorauszahlung verlangt.
- Hohe Ersparnisse werden garantiert.
- Die E-Mail-Adresse passt nicht zum Unternehmen.
- Dokumente wirken ungewöhnlich oder enthalten Fehler.
- Versicherungsunterlagen stammen nicht direkt vom Versicherer.
- Es wird Druck ausgeübt, schnell zu handeln.
- Kontaktdaten oder Ansprechpartner lassen sich nicht verifizieren.

Was tun bei Verdacht?

Bestehen Zweifel an einem Angebot, einem Dokument oder einem Ansprechpartner, empfiehlt sich ein schnelles Handeln:

- Keine weiteren Zahlungen vornehmen.
- Den Kontakt zur verdächtigen Person abbrechen.
- E-Mails, Nachrichten und Dokumente sichern.
- Den Versicherer informieren.
- Bei Verdacht auf Betrug Anzeige bei der Polizei erstatten.

Ein einfacher Grundsatz schützt: Gesunde Skepsis ist oft der beste Schutz vor Betrugsversuchen. Bestehen Zweifel an der Echtheit von Dokumenten, Angeboten oder Ansprechpartnern, empfiehlt sich eine Überprüfung über die offiziellen Kontaktwege des Versicherers.

Bildquellen

- Fokussierte Büroarbeit im hellen Homeoffice.png: KI-generiertes Bild, erstellt mit ChatGPT