PRESSEMITTEILUNG

Phishing: A-Trust warnt vor betrügerischen Nachrichten im Namen bekannter Dienste

Wien, 2. November 2026 - Eine vermeintlich notwendige Datenaktualisierung, eine drohende Zugangssperre oder ein angeblicher Sicherheitsvorfall: Phishing-Nachrichten greifen gezielt Situationen auf, die plausibel und dringend wirken. Dabei treten Kriminelle häufig im Namen bekannter Unternehmen, Behörden oder digitaler Dienste auf. A-Trust zeigt, welche Warnsignale Nutzer:innen kennen sollten und wie sie bei verdächtigen Nachrichten richtig reagieren.

Beim Phishing versuchen Angreifer:innen, über gefälschte E-Mails, SMS oder Websites an persönliche Daten, Zugangsdaten oder Zahlungsinformationen zu gelangen. Aktuell werden beispielsweise auch betrügerische Nachrichten im Namen der ID Austria versendet.

Dabei können Betrugsversuche auch mehrstufig aufgebaut sein: Auf eine vermeintliche Aufforderung zur Aktualisierung von Daten kann etwa der Anruf einer Person folgen, die sich als Bankmitarbeiter:in ausgibt. Unter einem Vorwand versuchen Täter:innen, Zugriff auf Geräte oder Online-Banking zu erhalten und anschließend betrügerische Transaktionen durchzuführen.

Markus Vesely, CEO von A-Trust: „Phishing ist gerade deshalb so gefährlich, weil eine Nachricht im ersten Moment vollkommen plausibel wirken kann. Ein bekannter Name, ein nachvollziehbarer Anlass und eine vermeintliche Frist schaffen schnell Vertrauen. Umso wichtiger ist es, bei unerwarteten Aufforderungen genau hinzusehen und nicht vorschnell zu reagieren."

Typische Warnsignale erkennen

Bestimmte Merkmale sollten Nutzer:innen besonders aufmerksam machen:

- Zeitdruck oder Drohungen: Eine Nachricht verlangt sofortiges Handeln oder kündigt Sperren und andere Konsequenzen an.
- Aufforderung zur Dateneingabe: Passwörter, Bankdaten, TANs oder andere persönliche Informationen sollen übermittelt werden.
- Auffällige Links oder Absender: Schreibweisen, Zahlen, Zusätze oder Webadressen weichen vom bekannten Absender ab.
- Ungewohnter Ablauf: Nach einer Nachricht wird beispielsweise telefonisch Zugriff auf Computer oder Smartphone verlangt.

Zusätzliche Orientierung bietet bei SMS das öffentliche Verzeichnis der Rundfunk und Telekom Regulierungs-GmbH (RTR). Seit 1. Oktober 2026 dürfen nur registrierte alphanumerische Absenderkennungen an österreichische Endnutzer:innen zugestellt werden. Ob eine Kennung im Verzeichnis eingetragen ist, kann öffentlich überprüft werden. A-Trust verwendet für seine SMS-Kommunikation immer eine solche registrierte Absenderkennung.

Im Zweifel empfiehlt es sich, einen Dienst direkt über die bekannte Website oder App aufzurufen, anstatt einem Link aus einer unerwarteten Nachricht zu folgen. Auch Absender und Webadresse sollten vor einer Reaktion sorgfältig geprüft werden.

„Ein vertrauter Name oder ein professionelles Erscheinungsbild allein sind heute kein Beleg dafür, dass eine Nachricht tatsächlich echt ist“, so Vesely. „Wer unsicher ist, sollte nicht direkt über die erhaltene Nachricht reagieren, sondern den betreffenden Dienst unabhängig davon aufrufen. Gerade bei sensiblen Daten kann ein kurzer zusätzlicher Check entscheidend sein.“

Bei Verdacht rasch handeln

Wer bereits persönliche Daten eingegeben oder Zugriff auf ein Gerät ermöglicht hat, sollte Zugangsdaten und Passwörter rasch ändern. Sind Bankdaten betroffen, empfiehlt die Polizei, Online-Banking, Konto beziehungsweise Bankkarten unverzüglich sperren zu lassen und Kontobewegungen genau zu kontrollieren. Ist bereits ein Schaden entstanden, kontaktieren Sie unverzüglich die Bank oder den Zahlungsdienstleister, um eine mögliche Rückholung des Geldes zu veranlassen. Erstatten Sie dann die Anzeige auf der nächsten Polizeidienststelle und nehmen Sie dazu dokumentierte Zahlungs- und Kontoinformationen sowie alle sonstigen gesicherten Beweise mit.

Über A-Trust
Compliance, Integrität, Komfort und vor allem Sicherheit: A-Trust ist ein zuverlässiges Partnerunternehmen, wenn es um Sicherheit im digitalen Raum geht, und steht für innovative und professionelle Zertifikats- und Signaturlösungen. Das Unternehmen ist ein qualifizierter Vertrauensdiensteanbieter für elektronische Zertifikate auf Basis der eIDAS-Verordnung und in der EU-Trusted List eingetragen. Die Teilnahme am EUDI-Wallet-Pilotprojekt POTENTIAL beweist, dass A-Trust-Know-how bei der Entwicklung innovativer Lösungen europaweit geschätzt wird.
Mit über 25 Jahren Erfahrung im Zertifikatsbereich und über 5 Millionen aktiven Nutzer:innen einer A-Trust-QES (z.B. ID Austria) steht A-Trust für Beständigkeit und Investitionssicherheit und ist im Heimatmarkt Österreich zum Branchenführer avanciert. Gemeinsam mit verschiedenen internationalen Partnerunternehmen bietet A-Trust erfolgreich sichere und komfortable Signaturlösungen für zahlreiche Kund:innen in ganz Europa an.
www.a-trust.at

Rückfragehinweis

A-Trust GmbH
Jenny Zheng, MA
Head of Marketing & PR
Landstraßer Hauptstraße 1b / E02
1030 Wien
Tel.: +43 1 713 21 51 341
E-Mail: jenny.zheng@a-trust.at

corporate identity prihoda gmbh
tatjana schnittchen, BA
pr consultant
peter-jordan-straße 74
1190 wien
tel.: +43 1 479 63 66–29
e-mail: tatjana.schnittchen@cip.at