NACHRICHTEN
Österreich

06. Juni 2025

Vorsicht! Cleverer Betrug in der Schweiz: So schützen Sie Ihr Konto!

Warnung vor neuer Betrugsmasche in der Schweiz: Täter nutzen gefälschte E-Mails und Anrufe zur Kontoausraubung.

Schweiz, Schweiz - Das Bundesamt für Cybersicherheit (Bacs) warnt vor einer neuen Betrugsmasche, die auch erfahrene Internetnutzer in der Schweiz betrifft. Diese Methode zielt nicht auf eine breite Masse ab, sondern ist spezifisch auf gezielt ausgewählte Personen ausgericht. Die Betrüger verwenden dafür eine raffinierte Vorgehensweise, die sowohl gefälschte E-Mails als auch Anrufe umfasst.

In einem ersten Schritt versenden die Täter E-Mails, die im Namen von Banken versendet werden. Diese Mails fordern eine angebliche „Compliance-Aktualisierung“ und leiten die Opfer auf eine täuschend echte Webseite, wo persönliche Daten wie Name, Telefonnummer und Vertragsnummer abgefragt werden.

Anschließend werden die Opfer auf die echte Bank-Website weitergeleitet, was die Glaubwürdigkeit der Masche erhöht.

Raffinierte Anrufer und extreme Vorsicht

Das zweite Element dieser Betrugsmasche sind Anrufe, die die Betrüger mit einer echten Banknummer durchführen, ein taktisches Vorgehen, das als Spoofing bekannt ist. Während des Gesprächs verfügen die Anrufer über persönliche Informationen der Opfer und schaffen so ein Vertrauensverhältnis. Das Ziel dieser Gespräche ist es, die Betroffenen zu einer angeblich verdächtigen Transaktion zu bewegen.

In einem besonders perfiden Schritt fordern die Betrüger ihre Opfer auf, einen QR-Code mit ihrer E-Banking-App zu scannen. Auf diese Weise versuchen sie, die Zwei-Faktor-Authentifizierung zu untergraben und erhalten so Zugang zu den Bankkonten der Betroffenen. Dieses Phänomen zeigt, wie kriminelle Strukturen zunehmend auch Sicherheitsmaßnahmen, die früher als wirksam galten, umgehen können, was die Gefährlichkeit dieser Betrugsmasche verdeutlicht.

Zugrunde liegende Probleme im Bereich Cybersicherheit

Die neue Masche offenbart die Schwächen in der Cybersicherheit und der Wirksamkeit von Traditionen wie der Zwei-Faktor-Authentifizierung (2FA). Diese wurde lange Zeit als zuverlässiger Schutz gegen Phishing-Angriffe betrachtet, verliert jedoch zunehmend an Effektivität. Cyberkriminelle haben ihre Taktiken weiterentwickelt und greifen auf ausgeklügelte Methoden zurück, die selbst gut geschulte Sicherheitsmitarbeiter täuschen können. Laut einer Bitkom-Studie waren im Jahr 2024 rund 25 % der befragten Unternehmen von Phishing-Schäden betroffen.

Unternehmen wird geraten, einen ganzheitlichen Ansatz zur

Bekämpfung von Phishing-Angriffen zu verfolgen. Dieser sollte regelmäßige Schulungen zur Sensibilisierung der Mitarbeiter, robuste technische Schutzvorkehrungen sowie moderne Authentifizierungsmethoden beinhalten. Innovative Ansätze wie FIDO2 und Passkeys ermöglichen passwortfreie Anmeldungen und bieten zusätzlichen Schutz gegen Man-in-the-Middle-Angriffe.

In einem von der CISA veröffentlichten Leitfaden werden spezifische Empfehlungen für die Bekämpfung solcher Phishing-Techniken bereitgestellt. Dieser Leitfaden richtet sich an alle Organisationen, darunter auch kleine und mittelständische Unternehmen, die ihre Cyber-Ressourcen schützen möchten.

Insgesamt zeigt die aktuelle Situation, dass die Methoden der Cyberkriminellen immer raffinierter werden und einfache Vorsichtsmaßnahmen nicht mehr ausreichen. Nutzer und Unternehmen müssen daher wachsam bleiben und moderne Sicherheitsstrategien anwenden, um sich vor solchen Angriffen zu schützen.

Empfehlungen des Bacs sind, niemals auf telefonische Aufforderungen zur Bestätigung über QR-Codes einzugehen, da dies zu einem Verlust des Bankzugangs führen kann. Der Rat, sich über die neuesten Techniken und Empfehlungen zur Sicherstellung der Internet-Sicherheit zu informieren, ist jetzt wichtiger denn je.

Besuchen Sie die folgenden Links für mehr Informationen: **vol.at** , **indevis.de**, **cisa.gov**.

Details	
Vorfall	Betrug
Ort	Schweiz, Schweiz
Quellen	• **www.vol.at** • **www.indevis.de** • **www.cisa.gov**