NACHRICHTEN AG

05. März 2025

Achtung! Neue Paypal-Betrugsmaschen zielen auf Ihre Daten ab!

Neue Betrugsmaschen gegen PayPal-Nutzer: Gefälschte E-Mails und Hotlines im Umlauf – dringend Sicherheitsmaßnahmen erforderlich.

Deutschland - In der digitalen Welt sind die Gefahren durch Betrüger nach wie vor allgegenwärtig. Besonders Paypal-Nutzer werden zunehmend Zielscheibe betrügerischer Machenschaften. Aktuelle Berichte von **t-online.de** zeigen, dass Betrüger neue, raffinierte Methoden entwickelt haben, um an persönliche Daten zu gelangen.

Die Betrüger setzen hauptsächlich auf zwei Strategien: gefälschte E-Mails und manipulierte Hotlines. Diese E-Mails wirken im ersten Moment täuschend echt und scheinen von „service@paypal.com“ zu stammen. Sie informieren den Empfänger über angebliche neue Adressen in seinem Paypal-Konto oder enthalten gefälschte Kaufbestätigungen, wie etwa für ein MacBook M4 Max im Wert von über 3.000 Euro. Darüber hinaus geben die E-Mails eine falsche Service-Hotline an, die das Opfer direkt zu den Betrügern führt. Diese geben sich dann als Paypal-Mitarbeiter aus und versuchen, Zugang zu den Computern der Opfer zu erhalten.

Phishing-Mails mit verschiedenen Vorwänden

Eine weitere Betrugsvariante sind Phishing-Mails, die mit einer angeblichen Rückerstattung von 65 US-Dollar (ca. 60 Euro) locken. Diese Mails sind häufig in englischer Sprache verfasst

und enthalten unangemessene Währungsangaben sowie fehlende Anrede, was ebenfalls ein Zeichen für Betrug ist. Nutzer sollten in solchen Fällen ihre Kontobewegungen regelmäßig überprüfen und bei Verdacht Paypal über die offizielle Website oder App kontaktieren, anstatt den Links in den E-Mails zu folgen.

Zusätzlich berichten **verbraucherschutz.com** von verschiedenen Betreffzeilen, die in gefälschten E-Mails verwendet werden, wie zum Beispiel „Ihr Konto wurde gesperrt“ oder „Wichtig: Handeln erforderlich“. Auch hier gilt es, aufmerksam zu sein, da einige Mails sogar korrekte Anredeformen verwenden, die Verwirrung stiften können. Nutzer werden eindringlich gewarnt, keine Links in verdächtigen E-Mails anzuklicken und verdächtige Nachrichten an die offizielle E-Mail-Adresse von Paypal weiterzuleiten.

Sicherheitsmaßnahmen treffen

Um sich vor Phishing-Angriffen zu schützen, empfehlen Experten, wie das **BSI**, keine vertraulichen Informationen per E-Mail anzufordern. Nutzer sollten die Adressleiste im Browser überprüfen, häufig besuchte Login-Seiten als Favoriten speichern und bei Unsicherheiten direkt beim Anbieter nachfragen. Auch das Nutzen der Zwei-Faktor-Authentifizierung wird empfohlen, um zusätzliche Sicherheit zu gewährleisten.

Wichtig ist ebenfalls, auf die Sicherheit von Webseiten zu achten, da Phishing-Seiten oft nicht über HTTPS gesichert sind. Eine regelmäßige Kontrolle des Kontostands und der Transaktionen bei digitalen Zahlungsdienstleistern kann ebenfalls dazu beitragen, unbefugte Zugriffe frühzeitig zu erkennen und zu verhindern.

Zusammenfassend ist es unerlässlich, in Zeiten zunehmender digitaler Betrugsversuche wachsam zu bleiben und stets Vorsichtsmaßnahmen zu ergreifen. Nutzer sollten sich bewusst sein, dass kein seriöser Anbieter vertrauliche Daten per E-Mail

anfordert und entsprechende Sicherheitsrichtlinien strikt befolgen.

Details	
Vorfall	Betrug
Ursache	Phishing
Ort	Deutschland
Quellen	• **www.t-online.de** • **www.verbraucherschutz.com** • **www.bsi.bund.de**