

Achtung Paypal-Nutzer: So entlarven Sie perfide Phishing-Mails!

Achtung, PayPal-Nutzer! Eine neue Phishing-Welle zielt auf persönliche Daten ab. Schützen Sie sich mit unseren Tipps!



Berlin, Deutschland - Die digitale Welt hat längst den Alltag erobert. Für viele Menschen gehört das Onlineshopping mittlerweile zum Leben, als wäre es ein täglicher Kaffee. Zahlungsmethoden wie PayPal, Klarna oder Kreditkarten sind gängige Begleiter in der virtuellen Einkaufswelt. Doch wo es einfach wird, lauern auch neue Gefahren, die nicht unterschätzt werden sollten. Besonders Banner und Betrüger haben ein leichtes Spiel, wenn es darum geht, an persönliche Daten zu gelangen.

Eine besonders perfide Masche hat es erneut auf die Warnliste geschafft: die so genannte „Gastkonto-Masche“ bei PayPal. In diesem Betrugsversuch erhalten viele Nutzer plötzlich eine E-

Mail, die zur Bestätigung ihrer privaten Angaben auffordert. Während die Nachricht vor einer „unbefugten Aktivität“ warnt und scheinbar klare Anweisungen gibt, um das Konto wieder nutzen zu können, handelt es sich tatsächlich um einen fieseren Betrugsversuch. Die E-Mails sind Teil einer berüchtigten Phishing-Welle, die darauf abzielt, Passwörter und persönliche Informationen zu stehlen. Die Täuschung ist so gut gemacht, dass sie oft nicht von echten Nachrichten zu unterscheiden sind.

Wie man Phishing-Mails erkennt

Die Verbraucherzentrale warnt vor einer neuen Phishing-Welle, die gezielt PayPal-Nutzer ins Visier nimmt. Die betrügerischen Nachrichten behaupten, dass ungewöhnliche Aktivitäten auf dem Konto festgestellt wurden, und fordern Nutzer auf, ihre Angaben zu bestätigen. Merkmale wie unpersönliche Anredeformeln, beispielsweise „Hallo Liebe PayPal Kunde!“, sowie zahlreiche Rechtschreibfehler und fehlerhafte Formulierungen wie „Zu Ihrer gefahrlosigkeit“ sind klare Indikatoren für solche Betrügereien. Hinzu kommt, dass etwa jede dritte unerwünschte E-Mail einen Phishing-Versuch enthält, wobei über 62 Prozent der Menschen bereits solche Mails erhalten haben und viele auf gefährliche Links klickten.

Die Experten raten dazu, in solchen Fällen sehr vorsichtig zu sein. Nutzer sollten keinesfalls auf verdächtige Links klicken. Stattdessen sollte die E-Mail unverzüglich an phishing@paypal.com weitergeleitet und anschließend aus dem Posteingang gelöscht werden. Wer sich unsicher ist, sollte sich ausschließlich über die offizielle PayPal-App oder Webseite in sein Konto einloggen, um die Aktivitäten zu überprüfen.

Essenzieller Rat bei Betrugsfällen

Für den Fall, dass doch persönliche Daten preisgegeben wurden, ist schnelles Handeln gefragt. In einem solchen Fall sollte sofort das Passwort geändert werden – wenn möglich auch der Log-in-Name. Reicht der Zugriff auf den Dienst nicht mehr aus, wird

geraten, das Unternehmen zu kontaktieren und gegebenenfalls die Bank um eine Sperrung des Kontos zu bitten.

In einer Zeit, in der Online-Zahlungen und Einkäufe Alltag sind, müssen Nutzer wachsam bleiben, um nicht in die Fallen Betrüger zu tappen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hebt hervor, dass es unerlässlich ist, verdächtige Nachrichten immer kritisch zu hinterfragen.

Für weitere Informationen können die Artikel von **Berlin Live** und **T-Online** aufgerufen werden.

Details	
Vorfall	Betrug
Ursache	Phishing
Ort	Berlin, Deutschland
Quellen	<ul style="list-style-type: none">• www.berlin-live.de• www.t-online.de

Besuchen Sie uns auf: n-ag.de