

# Datenschutz-Panne bei PayPal: Kontostand und Kundendaten durch Unbefugte abrufbar

☒ Wie die Initiative "Falle Internet" und das ZDF berichten, existierte bis gestern Abend (19. August 2008) eine Sicherheitslücke bei dem Bezahlendienst PayPal, die es möglich gemacht haben soll, fremde Kontostände auszuspähen. Über eine Servicenummer konnten Unbefugte den Kontostand und die Kontobewegungen fremder PayPal-Kunden abfragen.

## Lesen Sie mehr über die Panne bei der eBay-Tochter PayPal.

Auf diese Weise hätten auch die Kunden von Onlineshops, die mit PayPal bezahlt haben, in Erfahrung gebracht werden können. PayPal hat den telefonischen Service in dieser Form mittlerweile eingestellt. Trotz Sicherheitsvorkehrungen wie verschlüsselter Datenspeicherung sei es simpel gewesen, Guthabenstand sowie Details zu Zahlungstransfers zu ermitteln, und zwar mit Hilfe der automatisierten PayPal-Servicehotline, so die [Initiative "Falle Internet" auf ihrer Website](#):

*"Zur Identifizierung des Anrufers fragt PayPal dessen Telefonnummer und die letzten vier Ziffern der hinterlegten Bankkontonummer ab. Eine 'Telefon-PIN', ein Passwort oder ein anderes Sicherheitsmerkmal wird hingegen nicht verlangt."*

## Sicherheitsleck für Internethändler

Das Sicherheitsleck stellte gerade für Internethändler ein Risiko dar, da diese nach der überwiegenden deutschen Rechtsprechung gesetzlich verpflichtet sind, eine Telefonnummer im Rahmen der Anbieterkennzeichnung ihres Webshops anzugeben ([anders kürzlich der EuGH-Generalanwalt](#)).

Auch die Kontodaten ließen sich von Betrügern einfach durch eine Vorkasse-Testbestellung ausfindig machen, sofern sie nicht ebenfalls auf der Website des Shops veröffentlicht sind.

Wenn nun die selben Daten im Umgang mit PayPal verwendet wurden, was bei vielen Shopbetreibern der Fall sein dürfte, waren dem Missbrauch durch Unbefugte Tür und Tor geöffnet, so "Falle Internet" weiter:

*"Persönliche Finanzdaten gehören zu den sensibelsten privaten Informationen. Im Falle einer Firma sind sie sogar wichtiges Geschäftsgeheimnis. **Zusätzlich sind über das Datenschutz-Leck bei PayPal die Namen aller Transaktionspartner abrufbar - und damit der Kundenstamm eines Unternehmens.**"*

## Kundendaten konnten ausspioniert werden

Darüber hinaus sei es außerdem vorstellbar, dass PayPal-nutzende Internethändler Opfer von Phishing-Attacken geworden sein könnten, mutmaßen die Sicherheitsexperten von [falle-internet.de](#). Die dafür benötigte eMail-Adresse befände sich mit hoher Wahrscheinlichkeit ebenfalls im Impressum und mögliches Misstrauen des Empfängers sei durch PayPal unfreiwillig gedämpft worden:

*"In vielen PayPal-Mails sind Links enthalten, bei deren Anklicken man zum Einloggen in sein PayPal-Konto aufgefordert wird. Unter anderem betrifft das jede Zahlungsbestätigung - eine bedenkliche Praxis, die aus Sicherheitsgründen bei allen Banken seit Jahren abgeschafft ist."*

# Auch Phishing-Angriffe möglich

Einmal eingeloggt, hätten Betrüger das fremde PayPal-Guthaben beliebig verwenden können, denn "auch ein obligatorisches TAN-Verfahren zur Absicherung einzelner Transaktionen - ebenfalls der Mindeststandard seit den Anfangstagen des Online-Bankings - fehlt im PayPal-System ganz".

Bereits vor Wochen habe falle-internet.de PayPal auf den Missstand hingewiesen, allerdings sei erst nach Öffentlichmachung im Internet reagiert worden, indem der automatische Telefoncomputer durch lebendige Mitarbeiter ersetzt worden sei, was einen Missbrauch in Zukunft verhindern soll.

## PayPal: Sicherheitsproblem behoben

Auf Anfrage von heute.de bestätigte ein eBay-Sprecher das Vorhandensein des Sicherheitsproblems, gleichzeitig schloss er aber eine missbräuchliche Nutzung in der Vergangenheit grundsätzlich aus.

☒ Tipp: Um unbefugten Zugriff auf ein PayPal-Konto zu erschweren, bietet PayPal einen [Sicherheitsschlüssel zum Bestellen](#) an. Weitere Sicherheitstipps finden Sie am Ende des [falle-internet.de-Artikels](#).

## Falle im Internet: Missbrauch nun noch leichter?

Die Initiative "Falle im Internet" schreibt in einem [Update des Artikels vom 20.8.2008](#):

*"Eine Prüfung durch »falle-internet.de« ergab, dass die schwache Legitimation der automatisierten Konto-Abfrage nach deren Abschaltung durch eine möglicherweise noch schwächere Legitimation bei einem PayPal-Mitarbeiter ersetzt wurde.*

*Tests von »falle-internet.de« ergaben, dass die PayPal-Mitarbeiter ausführlich über den Status eines PayPal-Kontos Auskunft erteilen, wenn sich der Anrufer mit der E-Mail-Adresse, dem Namen und der Adresse, auf die das PayPal-Konto angemeldet ist, und mit den letzten vier Ziffern des Bankkontos legitimiert. Die meisten dieser Angaben finden sich in den in Deutschland gesetzlich vorgeschriebenen Impressumsangaben gewerblicher Verkäufer. Bei der Abfrage der letzten vier Ziffern der Kontonummer hat sich nichts geändert.*

***Die Datenlücke bei PayPal wurde durch die Abschaltung der automatisierten Konto-Abfrage nicht geschlossen, der Zugang zu Auskünften zu fremden PayPal-Konten ist nun eher noch leichter als bisher."***

Quellen:

["Falle Internet"](#), [ZDF heute.de](#), eigene Recherchen