

## Betrugsmaschen: Finanzagent oder Enkeltrick?



Ihnen wird ein Job als so genannter „Finanzagent“ angeboten. Sie werden von einem Techniker angerufen, der Ihnen anbietet, mit einer Fernwartungssoftware die Leistung Ihres Computers zu verbessern oder Sicherheitslücken zu schließen. Ein „offizielles“ Schreiben Ihrer Bank kündigt Ihnen einen Mitarbeiter an, der am nächsten Tag Ihren Online-Banking-Zugang überprüfen will. Ein vermeintlicher Mitarbeiter einer Lottogesellschaft gratuliert Ihnen und bittet Sie um Ihre Zugangsdaten zum Online-Banking, damit er Ihnen den Gewinn zukommen lassen kann.

Betrüger lassen sich ständig neue Tricks einfallen, um das Vertrauen ihrer potenziellen Opfer zu gewinnen - und die Methoden werden immer raffinierter.

So vielfältig die Betrugsmaschen sind, eines ist ihnen gemein: Trickreich versuchen Betrüger, Kontodaten abzugreifen oder Schadsoftware auf dem Computer des Betroffenen zu installieren, um so an die persönlichen Daten zu gelangen. Auf dem Schaden bleiben die Opfer solcher krimineller Handlungen oft sitzen. Bei einer Tätigkeit als Finanzagent machen Sie sich selbst sogar strafbar.

Schützen Sie sich, indem Sie regelmäßig Ihr Konto checken. Auch unerwartete Gutschriften sollten Sie stutzig machen. Geben Sie niemals Ihre PINs und TANs (Transaktions-

21.09.2018

von



Altmann, Kathleen

### Kurzgefasst

Ihnen wird ein Job als so genannter „Finanzagent“ angeboten. Sie werden von einem Techniker angerufen, der Ihnen anbietet, mit einer Fernwartungssoftware die Leistung Ihres Computers zu verbessern oder Sicherheitslücken zu schließen. Ein „offizielles“ Schreiben Ihrer Bank kündigt Ihnen einen Mitarbeiter an, der am nächsten Tag Ihren Online-Banking-Zugang überprüfen will. Ein vermeintlicher Mitarbeiter einer Lottogesellschaft gratuliert Ihnen und bittet Sie um Ihre Zugangsdaten zum Online-Banking, damit er Ihnen den Gewinn zukommen lassen kann.

### Schlagworte

Konto  
Verbraucher  
Dossier Betrugsmaschen  
PIN

## Blog

nummern) an Dritte weiter, egal wie vertrauenswürdig Ihnen der Anrufer erscheint. Prüfen Sie alle Angebote kritisch, bei denen Ihr Konto zur Abwicklung von Zahlungen für Firmen oder Personen dienen soll.

Bei Zweifeln an der Seriosität des Gesprächspartners lassen Sie sich nicht überrumpeln – bitten Sie einfach um Namen und Telefonnummer, um zurückzurufen. Überprüfen Sie vor dem Rückruf die Telefonnummer, indem Sie auf die Webseite des Unternehmens gehen, rufen Sie die Auskunft an oder schauen Sie im Telefonbuch nach.

Einen absoluten Schutz vor Betrugsmaschen gibt es natürlich nicht. Wichtig ist jedoch, wachsam zu bleiben und sich der Gefahren bewusst zu sein.

Mehr zu der **Betrugsmasche Techniker-Anruf in unserem Blog**. Wie Sie sich vor unterschiedlichen Betrugsmethoden im Internet schützen, haben wir in unserem **Lexikon Cyberkriminalität** zusammengefasst.