

Vorsicht Phishing: Betrüger-E-Mails unter dem Vorwand des Datenschutzes

17.05.2018

von



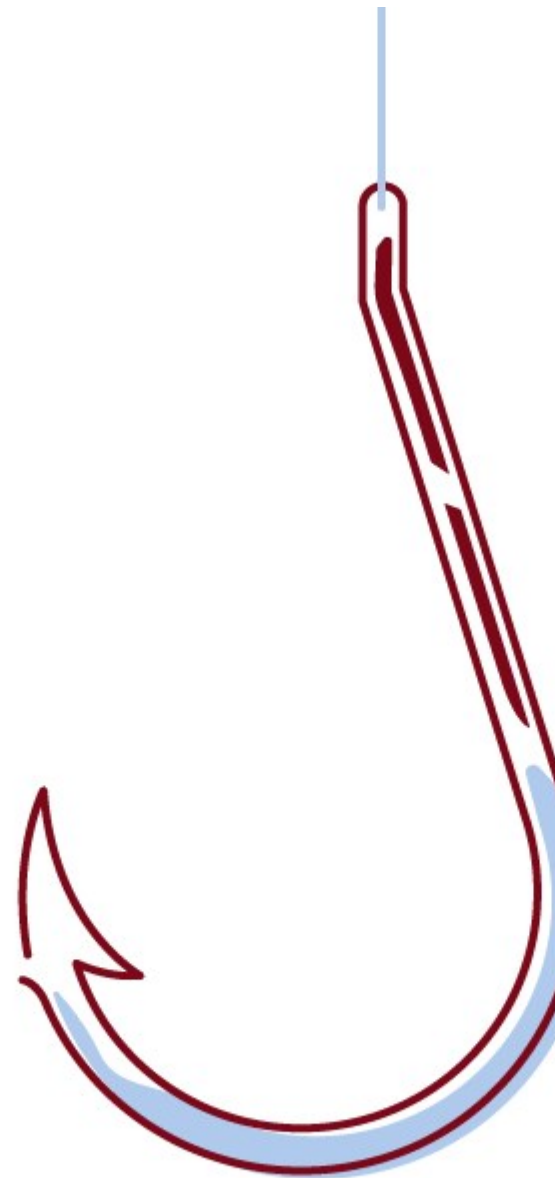
Redaktion, Verbraucher

Kurzgefasst

„Bitte akzeptieren Sie unsere aktualisierten Nutzungsbedingungen“ – viele Unternehmen versenden derzeit solche E-Mails, um der neuen EU-Datenschutzverordnung gerecht zu werden. Doch Vorsicht: Betrüger nutzen das aus, um sensible Daten abzugreifen. Wir erklären, wie Sie unseriöse Mails erkennen und was im Zweifel zu tun ist.

Schlagworte

Datenschutz
Cybersicherheit
Cyberkriminalität
Verbraucherschutz
Verbraucher



Am 25. Mai 2018 tritt die EU-Datenschutzgrundverordnung (DSGVO) in Kraft. Viele Unternehmen schreiben daher derzeit ihre Kunden per E-Mail an, um sie über die Datenschutznovelle zu informieren und sie über ihre Rechte aufzuklären. Teilweise werden Kunden gebeten, in die Nutzung ihrer Daten einzuwilligen. Oft geht es einfach nur darum, ob man einen Newsletter weiter beziehen möchte. Aber Verbraucherschützer warnen: Auf diesen Zug springen aktuell auch Betrüger auf - der Datenklau per E-Mail oder SMS unter dem Stichwort „DSGVO“ hat Hochkonjunktur. Ein falscher Klick, und eine Schadsoftware installiert sich auf Ihrem PC oder Smartphone, um nach sensiblen Daten „fischen“ zu können - daher nennt man diesen Trick auch Phishing.

Blog

Seien Sie also besonders misstrauisch, wenn Sie in den nächsten Wochen vermeintlich eine E-Mail von Ihrer Bank erhalten, in der Sie zum Beispiel aufgefordert werden, Ihre Daten preis zu geben oder auf einen „Einwilligungslink“ zu klicken. Unabhängig von der Datenschutzgrundverordnung gilt: Ihre Bank wird Sie niemals per E-Mail um Nennung oder Eingabe Ihrer persönlichen Daten wie Kontonummer, PIN oder Passwörter bitten. Ihre Bank wird auf diese Wege auch nicht von Ihnen verlangen, Ihr Konto zu aktivieren, zu „entsperren“ oder es zu „aktualisieren“. Wenn Sie Zweifel an der Echtheit einer E-Mail haben, nehmen Sie lieber direkten Kontakt zu Ihrer Bank auf.



Abonnieren Sie den Blog Verbraucher-Magazin!

Zum Abonnement

Allgemein sollten Online-Banking-Kunden eine Reihe von Sorgfaltspflichten beachten, um sich zu schützen. Dazu gehört auch die Installation von Virenschanner und Firewall auf dem heimischen Rechner. Die Software von PC und Smartphone sollte außerdem stets auf dem neuesten Stand sein. Tätigen Sie Bankgeschäfte nie über einen fremden Rechner (z.B. Internet-Café) und nutzen Sie nur autorisierte Apps Ihrer Bank.

Beim Umgang mit Passwörtern, PIN & Co. ist ebenfalls Vorsicht angesagt. Niemals sollten Sie solche geheim zu haltende Daten in Apps, der Cloud oder auf Ihrer Festplatte speichern, auch nicht als Telefonnummer verschlüsselt in den Handy-Kontakten.