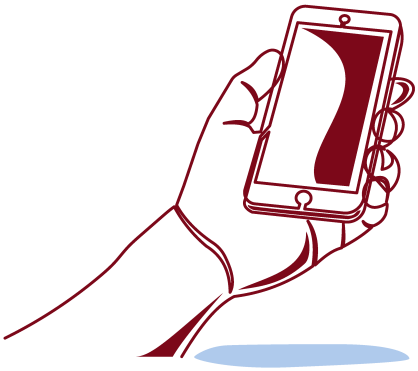
Achtung vor SMS-Betrügern!

21.10.2021
von

Ernoult, Sylvie

Schlagworte

Phishing
Cyberattacken
Verbraucher
Datenschutz
Cyberkriminalität
Verbraucherschutz
Sicherheit Verbraucher



Seit Wochen erhalten Nutzerinnen und Nutzer von Smartphones und Handys vermehrt SMS-Nachrichten, die vermeintlich über den Sendestatus von Paketen informieren sollen. Um den genauen Sendestatus abzurufen, soll der Verbraucher auf einen Link klicken. Achtung! Es kann sich hierbei um eine Betrugsmasche, genauer einen Smishing-Angriff handeln.

Das Ziel eines solchen Angriffs ist das Abfischen von persönlichen Daten. Folgt das Opfer dem Link aus der gefälschten Textnachricht, kann eine Schadstoffsoftware heruntergeladen werden oder man wird zu einer gefälschten Webseite weitergeleitet. Wird eine Telefonnummer angegeben, die man zurückrufen soll, um das eigene Konto zu „prüfen“, zu „aktualisieren“ oder zu „reaktivieren“ kann der Anruf zu einem Kriminellen, der sich als Angestellter des echten Unternehmens ausgibt, durchgestellt werden. Dabei wird das Opfer aufgefordert, seine persönlichen Daten offenzulegen. Beim vermeintlichen Abgleich der vorliegenden persönlichen Daten ergaunert sich dann der falsche Angestellte unter dem Vorwand eine erfolgreiche Paketzustellung durchführen zu wollen, wertvolle, vertrauliche Informationen.

Kriminelle setzen heutzutage vermehrt auf das **Smishing**, also das **Phishing** (Datenabfischen) per SMS: Diese Betrugsmasche ist tückisch, da das Risikobewusstsein eine

unbekannte E-Mail zu öffnen oftmals größer ist, als eine unbekannte Textnachricht zu lesen und anzuklicken.

Wie können Sie sich vor Smishing-Angriffen schützen?

- Nutzen Sie die direkte Sendungsverfolgung auf der Webseite oder in der App des Versanddienstleisters und klicken Sie keine externen Quellen an.
- Wenn Sie eine Smishing-SMS erhalten, klicken Sie nicht auf den Link.
- Installieren Sie keine Apps über Links in Textnachrichten. Apps sollten nur aus dem offiziellen App Store für Ihr Gerät heruntergeladen werden.
- Sperren Sie den Absender der SMS und löschen Sie die SMS, wenn Sie von einem Smishing-Angriff ausgehen.
- Nehmen Sie unbedingt regelmäßig die verfügbaren Updates fürs Smartphone vor, denn diese Updates dienen auch der Sicherheit vor Cyberangriffen.

Was tun, wenn Sie den Link angeklickt haben und Opfer eines Smishing-Angriffs geworden sind?

- Stellen Sie ihr Gerät sofort in den Flugmodus. Damit nehmen Sie erstmal das Gerät aus dem Mobilfunknetz und verhindern, dass Sie weitere schädliche Nachrichten erhalten oder dass sich weitere Schadprogramme auf Ihr Smartphone installieren.
- Informieren Sie Ihren Mobilfunkprovider über den Vorfall.
- Erstatten Sie Strafanzeige bei der Polizei. Nehmen Sie dazu Ihr Smartphone zur Beweissicherung mit.
- Setzen Sie Ihr Smartphone auf Werkseinstellungen zurück. Dadurch werden alle über die SMS- Nachricht verteilten Schadprogramme entfernt.
- Seien Sie besonders vorsichtig und prüfen Sie noch sorgfältiger als sonst, ob es auf Ihrem Konto

Bewegungen gegeben hat, die Sie sich nicht erklären können.