Vorsicht vor „Techniker“-Anrufen

08.10.2020

von

Altmann, Kathleen

Schlagworte

ECSM
Verbraucher
PIN
Onlinebanking
Sicherheit
Verbraucherschutz
Cybersicherheit
Cyberkriminalität

Kriminelle nutzen gerade das Sicherheitsbedürfnis vieler Menschen gern für Betrügereien aus. Zu den vielfältigen

Betrugsmaschen gehört auch der „Techniker"-Anruf. Wie diese Masche funktioniert, und wie Sie sich davor schützen können.

So funktioniert die Masche

Das Telefon klingelt, in der Leitung ist ein Techniker eines Ihnen bekannten Unternehmens – angeblich! Unter dem Vorwand, die Leistung Ihres Computers zu verbessern oder Sicherheitslücken schließen zu wollen, fordert er Sie dazu auf, eine Fernwartungssoftware herunterzuladen und anschließend zu starten. Lassen Sie sich darauf ein, kann der kriminelle Anrufer ohne Ihr Wissen und weiteres Zutun beispielsweise eine Spionagesoftware auf Ihrem Gerät installieren. Damit kann er im Grunde alle Ihre persönlichen Daten, die sich auf dem Computer befinden, ausspähen.

Unter Umständen werden Sie anschließend sogar noch aufgefordert, umgehend per Onlinebanking eine Servicepauschale zu überweisen. Dabei zockt der Betrüger Sie erneut ab: Während der Transaktion ändert er den Betrag, ohne dass Sie es merken. Alternativ können Sie dazu aufgefordert werden, eine fremde Webseite aufzurufen und dort Ihre Kreditkartendaten oder andere sensible Zahlungsdaten einzugeben.

***Weitere Betrugsmaschen per Telefon und wie Sie sich dagegen schützen können, finden Sie im Blogbeitrag** Betrugsmaschen: Finanzagent oder Enkeltrick?*

So können Sie sich schützen

Gesundes Misstrauen hilft! Es ist sehr wahrscheinlich, dass der kriminelle Anrufer versucht Sie unter Druck zu setzen. Zum Beispiel, indem er behauptet, Sie müssten mit finanziellen Einbußen oder anderen Schäden rechnen, wenn Sie einen bestimmten Link nicht unverzüglich aufrufen oder Ihre persönlichen Daten nicht in eine bestimmte Anwendung eingeben.

Auch andere Druckmittel werden gern gebraucht: Zum Beispiel mit einer Kontosperre zu drohen oder damit, ein Inkassobüro oder einen Rechtsanwalt einzuschalten. Aber: Lassen Sie sich nicht einschüchtern, sondern legen Sie im Zweifel einfach auf!

Allgemein gilt: Gehen Sie verantwortungsvoll mit allen Ihren persönlichen Daten um. Dazu gehören neben Ihren Kartendaten, PINs und TANs, auch Ihre Adresse, Ihre Telefonnummern oder Ihr Geburtsdatum. Überlegen Sie stets, ob diese Informationen für den beabsichtigten Vorgang überhaupt benötigt werden.

Sie sollten sich auch den Namen und die Rückrufnummer des Anrufers geben lassen, wenn Sie Zweifel an der Seriosität des Gesprächspartners haben. Versprechen Sie einen Rückruf und legen Sie vorsichtshalber auf. Bevor Sie zurückrufen, schauen Sie doch mal auf der angeblichen Unternehmenswebseite, fragen die Auskunft oder suchen im Telefonbuch nach dem Anrufer.

Wichtig: Wenden Sie sich bei jeglichem Missbrauch Ihrer Bankdaten – und auch schon bei einem Verdacht – umgehend an Ihre Bank. Kontaktieren Sie zudem die Polizei und erstatten Sie Strafanzeige. Nur wenn der versuchte oder tatsächliche Betrug angezeigt wurde, kann er auch strafrechtlich verfolgt und den Kriminellen das Handwerk gelegt werden.