Verbraucherzentrale Südtirol
Centro Tutela Consumatori Utenti
Die Stimme der VerbraucherInnen
La voce dei consumatori

**VZS-name**

VZS-str
VZS-plz
VZS-tel
info@verbraucherzentrale.it

# Digitale Zahlungen

Thu, 06/10/2021 - 10:15

## Der Betrug mit den „Einmal-Passwörtern“

**Das Europäische Verbraucherzentrum (EVZ) und die Verbraucherzentrale Südtirol (VZS) haben in letzter Zeit zahlreiche Meldungen zu Betrügereien erhalten, die sich zwar in ihrer Ausführung leicht voneinander unterschieden, aber allesamt eines gemeinsam hatten: die Betrogenen glaubten alle, mit einer Bank oder einem Kreditkarteninstitut zu tun zu haben.**

Mitteilungen und Anrufe, die von Banken oder Kreditkarteninstituten kommen, stufen wir eigentlich immer als besonders wichtig ein und halten sie (leider) auch meist automatisch für seriös und vertrauenswürdig, denn: “Sie kommen ja von einer Bank!“

So auch Frau Meier, die uns Folgendes berichtet:

„*Ich bekam eine SMS, in der ich dazu aufgefordert wurde, eine Grüne Nummer zu kontaktieren, um eine Unregelmäßigkeit in Zusammenhang mit meiner Kreditkarte zu überprüfen. Im Gespräch brachte mich mein Gesprächspartner, der sich als Mitarbeiter meines Kreditkarteninstitutes ausgab, dazu, ihm den Code mitzuteilen, den ich gerade per SMS zugeschickt bekommen hatte. Ich habe also den Code mitgeteilt und hatte damit tatsächlich in eine Abbuchung über mehr als 1000 Euro eingewilligt.* „

### Achtung vor OTP-Betrügereien:

Frau Meier wurde Opfer einer von vielen sogenannten **“OTP-Betrügereien”.** OTP steht für „One-Time-Password” also „Einmal-Passwort“ und bezeichnet einen Code, der häufig bei digitalen Zahlungen per Kreditkarte oder Onlinebanking zum Abschluss der Transaktion benötigt wird. Er wird über SMS zugeschickt oder über andere Systeme erst im Moment der Zahlung generiert. Solche OTPs benötigt man nur, wenn man Geld ausgeben möchte, nicht aber, um etwa Geld zu erhalten oder Überprüfungen durchzuführen.

„*In Zusammenhang mit solchen OTPs gibt es einen Grundsatz, den man immer beherzigen sollte, um nicht in eine Falle zu tappen:* ***Diese Passwörter dürfen auf keinen Fall weitergegeben werden*****“**, erklärt Gunde Bauhofer, Geschäftsführerin der VZS. Unabhängig davon, ob sie anscheinend vom Gesprächspartner geschickt wurden und ganz egal wer anruft, schreibt, simst oder Whatsappt: **OTPs werden nicht weitergeleitet.** „*Keine Bank, kein Kreditkarteninstitut oder sonstige vertrauenserweckende Institution wird danach fragen: der einzige Ort, an dem das OTP verwendet wird, ist die – schon geöffnete - Website für die Zahlung des Onlinekaufs, oder die Seite des Onlinebankings*“, bekräftigt Julia Rufinatscha, E-Commerce-

Expertin im Europäischen Verbraucherzentrum.

So wie Frau Meier hätten wohl auch viele andere reagiert, hätten sie sich in einer ähnlichen Situation befunden. Und trotzdem gibt es wesentliche Stellen in Frau Meiers Erzählung, die anders ausgefallen wären, hätte sie folgende Tipps und Informationen bereits gehabt:

- Wenn Sie ein Kreditkarteninstitut oder eine Bank kontaktieren, verlassen Sie sich niemals auf die Telefonnummern, die Sie über soziale Medien und Suchmaschinen finden, oder die Ihnen per SMS oder WhatsApp mitgeteilt werden. Überprüfen Sie diese immer zuerst und **entnehmen Sie alle Kontaktdaten ausschließlich der offiziellen Internetseite des Bank- oder Kreditkarteninsitutes**

- **Klicken Sie niemals auf Links** die angeblich von Ihrer Bank oder Ihrem Kreditkarteninstitut kommen: sie können zu einer **betrügerischen Abbuchung** führen

- **Kontrollieren** Sie immer den **Inhalt der SMS** und geben Sie niemals die mitgeteilte Zahlenkombination ein, ohne die SMS geöffnet zu haben

- Gehen Sie davon aus, dass Banken und Finanzdienstleister **keine vollständigen persönlichen Codes oder Kartennummern** per SMS oder telefonisch abfragen

- Sollten Sie dennoch Opfer eines OTP-Betrugs geworden sein, erstatten Sie **Anzeige** und reichen Sie eine **Beschwerde bei Ihrem Finanzdienstleister** ein.

Weitere Informationen zu diesem Themen finden Sie hier:

https://www.euroconsumatori.org/de/gefahren_im_netz_phishing