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

Fri, 05/13/2022 - 10:23

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 allesamt eines gemeinsam hatten: Die Betrogenen glaubten alle, mit einer Bank oder einem Kreditkarteninstitut zu tun zu haben.

Die Bank informiert Sie per SMS, dass Ihr Konto in Gefahr ist, und fordert Sie auf, auf einen Link zu klicken und ein Formular mit Ihren Daten auszufüllen, um die Situation zu überprüfen und zu klären... Und genau damit tappt man in die betrügerische Falle.

Mitteilungen und Anrufe, die von Banken oder Kreditkarteninstituten kommen, stufen wir eigentlich immer als besonders wichtig ein und halten sie auch für seriös und vertrauenswürdig.

So auch Herr Meier, der uns Folgendes berichtet:

„Ich bekam eine SMS, die angeblich von meiner Bank kam. Darin wurde ich aufmerksam gemacht, dass bei meinem Konto Unregelmäßigkeiten festgestellt wurden. Ich sollte auf einen Link klicken, um die Situation zu überprüfen. Ich füllte das Formular mit meinen Daten aus, daraufhin rief mich ein angeblicher Bankangestellter an, dem ich meine Daten gab, um die Situation in Echtzeit zu überprüfen. So kam es, dass mein Konto leer geräumt wurde."

Der Verbraucherzentrale Südtirol (VZS) liegen Meldungen über Fälle vor, in denen Kriminelle Beträge von bis zu 10.000 Euro veruntreut haben. Wir können die in den letzten Tagen von der Polizeidirektion Bozen herausgegebenen Warnhinweise nur bestätigen.

Achtung vor OTP-Betrügereien:
Herr 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 Verbraucherzentrale Südtirol (VZS). „Unabhängig davon, ob sie anscheinend vom Gesprächspartner gesendet wurden und ganz egal, wer anruft oder sich über ein anderes Kommunikationsmittel mit Ihnen in Verbindung setzt: **OTPs werden nicht weitergeleitet** “, unterstreicht Gunde Bauhofer.

„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 Herr Meier hätten wohl auch viele andere reagiert, hätten sie sich in einer ähnlichen Situation befunden. Und trotzdem gibt es wesentliche Stellen in Herrn Meiers Erzählung, die anders ausgefallen wären, hätte er 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 Kreditkarteninsituts**.
- **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