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

Verbraucherzentrale Südtirol

Zwölfmalgreiner Straße 2
39100 Bozen
Tel. 0471 975597
info@verbraucherzentrale.it

Tatort Smartphone

Mi, 13.10.2021 - 11:10

Wenn Betrüger per SMS oder E-Mail nach Daten „fischen“ und vierstellige Beträge von Konten und Karten verschwinden

Grenzenlos sind die Möglichkeiten in der digitalen Welt, und grenzenlos sind scheinbar auch die kriminellen Aktivitäten, die sich dort entfalten. So häufen sich in diesen Tagen in der Verbraucherzentrale Südtirol (VZS) die Anrufe von teils zweifelnden und teils schon verzweifelten Verbrauchern und Verbraucherinnen. Den einen scheinen SMS und Mails, die sie erhalten haben, ziemlich suspekt; den anderen sind Summen von bis zu 5.000 Euro vom Konto oder der Kreditkarte verschwunden.

Das Ganze beginnt meist mit einer SMS: der eigene Finanzdienstleister – so scheint es – teilt mit, dass sich irgendwelche Probleme auf der Karte, auf dem Konto, mit dem Account ergeben haben. Man solle bitte diese Website aufrufen und sich einloggen, um das Problem zu beheben.

Die aufgerufene Seite sieht dann auch absolut authentisch aus, bis hin zur verschlüsselten Verbindung über https – aber wenn man genau hinblickt, merkt man, dass die Adresse nicht die gewohnte ist. Jedoch – wie vielen von uns fiele das auf die Schnelle auf – noch dazu in einer Situation, wo man ohnehin so schnell wie möglich das Konto oder die Karte überprüfen will, da doch der Anbieter ein Problem gemeldet hatte?

Und schon kann es aber geschehen sein – die Zugangsdaten sind „gefischt“, und die Betrüger haben Zugriff aufs Konto oder die Karte. Zwar sollten mit Inkrafttreten der neuen Zahlungsdienstleistungs-Richtlinie PSD2, die ein Login in zwei Schritten zur Pflicht gemacht hatte, diese Fälle eigentlich der Vergangenheit angehören – jedoch scheinen die Fälle eher zu- als abzunehmen (die VZS berichtete mehrfach).

Daher hilft eigentlich nur eins: kühlen Kopf bewahren und mit Hausverstand an die Sache herangehen. Wenn Sie Ihren Anbieter kontaktieren wollen, verwenden Sie am besten die Daten, die Sie auf dem Kontoauszug oder anderen offiziellen Dokumenten finden.

Einige Tipps:

- Grundsätzlich wird man von Banken oder Kreditkartenbetreibern nie aufgefordert, eine Website aufzusuchen und sich einzuloggen; wenn Sie eine solche SMS, E-mail oder einen solchen Anruf erhalten, ist Misstrauen erst mal angebracht.
- Wenn Sie sich einloggen, tippen Sie die Adresse der Seite von Hand ein, und verwenden Sie die offizielle Webadresse – klicken Sie nicht auf die Links, die Sie erhalten haben (wem dies zu aufwändig ist, kann für die offizielle Seite beim ersten Besuch ein digitales „Lesezeichen“ anlegen).
- Verlangt man auf irgend einem Weg von Ihnen, Einmal-Passwörter weiterzugeben (die z.B. per SMS aufs Handy kommen), sollten alle Alarmleuchten auf Rot springen – diese sind allein für Sie bestimmt!

Im Zweifelsfall sollten Sie bei Ihrem Anbieter weitere Auskünfte erhalten. Auch die Verbraucherzentrale Südtirol oder die Postpolizei stehen Ihnen mit Rat und Hilfe zur Seite.

Ausführlichere Informationen und Tipps zum Schutz gegen Phishing finden Sie unter anderem hier: https://www.kaspersky.de/blog/phishing-ten-tips/6422/

Wenn sie nicht genehmigte Geldbewegungen feststellen, gilt es, folgende Schritte zu unternehmen:

- Karte bzw. Konto sofort sperren lassen;
- bei den Behörden (Polizei/Carabinieri) Anzeige bzw. Strafanzeige erstatten;
- eine schriftliche Beschwerde an den Finanzdienstleister richten, die Bewegungen aberkennen und die Rückerstattung der betroffenen Summen fordern (Anzeige beilegen);
- sollte der Finanzdienstleister nicht bzw. negativ antworten, kann nach Ablauf der Frist von 60 Tagen ab Beschwerde vor dem Bankenschiedsgericht ABF (www.arbitrobancariofinanziario.it) Rekurs eingereicht werden.