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

Die Verbraucherzentrale Südtirol warnt vor neuen Betrugsmaschen und gibt nützliche Tipps

Fr, 07.11.2025 - 09:47

In den letzten Wochen konnte bei der Verbraucherzentrale Südtirol (VZS) eine Zunahme von neuen Betrugsmaschen, die per E-Mail oder SMS eintrudeln, festgestellt werden. Verbraucher:innen erhalten zur Zeit häufiger solche E-Mails oder SMS, die angeblich vom eigenen Finanzdienstleister, Bank, Telefonanbieter oder auch von einem Patronat oder einer Behörde kommen. Gemeinsamer Nenner ist dabei eine (gefälschte) Mitteilung, mit welcher die Verbraucher:innen zur Zahlung eines bestimmten Betrags oder zur Übermittlung von persönlichen Daten aufgefordert werden. Die VZS gibt hier einige nützliche Tipps, um diese Art von Mitteilungen sofort zu erkennen und sich vor solchen Betrugsversuchen zu schützen.

Ein konkretes Beispiel
Vor kurzem haben sich mehrere Verbraucher:innen an die VZS gewandt, weil sie angeblich eine E-Mail von der „Bundespolizei Österreich“ mit einer Gerichtsvorladung erhalten haben. Nach einem kurzen Blick auf die E-Mail und das Dokument im Anhang konnten die Berater:innen der VZS feststellen, dass es sich um einen klaren Fall von „Authority Scam“ bzw. um einen Phishing-Versuch handelte.

Wie erkennt man gefälschte Mitteilungen per E-Mail oder SMS und was kann man im Zweifelsfall tun?

Absender kontrollieren

- **Die Absenderadresse wirkt unseriös.** Die betrügerischen E-Mail-Adressen enthalten oft Namen, Ziffern und stammen von einer generellen Domain (gmail.com, outlook.com usw.) oder imitieren nur teilweise eine offizielle (unternehmenseigene) Domain bzw. Adresse.

- **Bei einer SMS steht als Absender nur eine Handynummer**, statt des Namens des Unternehmens bzw. der Behörde.

Die VZS rät: Im Zweifelsfall kann man die Absenderadresse oder die Telefonnummer mit den offiziellen Kontaktdaten auf der Online-Seite des Unternehmens oder der Behörde vergleichen.

Inhalt auf verschiedene Aspekte überprüfen

- **Unpersönliche Anrede und Fehler:** Sie werden nicht persönlich mit Ihrem Namen angesprochen, sondern mit einer allgemeinen Formulierung, und Sie finden Fehler im Text.
- **Dringende Zahlungsaufforderungen:** es wird eine sofortige Zahlung gefordert, oft auch unter Androhung von Strafen.
- **Forderung nach persönlichen Daten:** es wird nach persönlichen Daten wie Passwörtern, Kontodaten oder Ausweisnummern gefragt.
- **Forderung, dringend eine Handynummer anzurufen:** seriöse Unternehmen verweisen auf eigene Online-Portale oder Apps.
- **Ungewöhnliche Anhänge oder Links:** diese sollten besser nicht geöffnet werden, da sie Schadprogramme enthalten könnten.
- **Fehlerhafte Logos oder Siegel:** die Logos, Stempel oder Siegel können ähnlich aussehen, entsprechen dem Original aber nicht und werden missbräuchlich verwendet. Auch diese können online auf den offiziellen Seiten verglichen werden.
- **Mehrkosten-Nummern:** sie werden zu einem kostenpflichtigen Rückruf verleitet. Auch SMS mit kostengünstigen Angebote können Sie zu teuren Nummern führen. Um sich zu schützen, rufen Sie unbekannte Nummern mit verdächtigen Vorwahlen (oft aus dem Ausland oder Premium-Dienste wie "89") niemals zurück und blockieren Sie die Nummer.

Wichtig: Echte Gerichts- und Behördenschreiben und weitere wichtige Mitteilungen kommen per Post und niemals per E-Mail oder SMS. Außerdem fordern Behörden niemals persönliche Daten oder Zahlungen über E-Mail an.

Die VZS empfiehlt: Besser offizielle Kontaktdaten (online oder auf Dokumenten) suchen und diese nutzen, um direkt Informationen zur erhaltenen Mitteilung zu erfragen.

Was tun, wenn sie eine solche gefälschte Mitteilung erhalten?

- **Nicht reagieren:** Gehen Sie auf keine E-Mail oder SMS ein und öffnen Sie keine Anhänge.
- **Nicht bezahlen:** Bezahlen Sie keine vermeintlichen Forderungen, die per E-Mail kommen. Erkundigen Sie sich eventuell zuerst über offizielle Kontaktdaten.
- **Beweise sichern:** Verdächtige E-Mails können hier gemeldet werden: https://www.commissariatodips.it/segnalazioni/segnala-online/index.html. Für den oben genannten Fall können Sie die erhaltene E-Mail hingegen dem Bundeskriminalamt Österreich

unter against-cybercrime@bmi.gv.at weiterleiten.
- **Computer überprüfen:** Überprüfen Sie Ihre Geräte regelmäßig mit einem aktuellen Anti-Virus-Programm und ändern Sie regelmäßig Ihre Passwörter.

Wenn Sie Phishing-Betrügern zum Opfer gefallen sind

1. Karte bzw. Konto sofort sperren lassen

2. bei den Behörden (Polizei/Carabinieri) Anzeige bzw. Strafanzeige erstatten;

3. eine Beschwerde an den Finanzdienstleister richten, die Bewegungen aberkennen und die Rückerstattung der betroffenen Summen fordern (Anzeige beilegen);

4. sollte der Finanzdienstleister nicht bzw. negativ antworten, kann vor Schlichtungsstelle der Banca d'Italia, dem Arbitro Bancaio Finanziairo (www.arbitrobancariofinanziario.it) Rekurs eingereicht werden (Verbraucherorganisationen wie die VZS helfen bei einem solchen Rekurs).

Wichtig: Die Beschwerde sollte innerhalb von 13 Monaten erfolgen, da andernfalls die Beweispflicht auf den Kunden übergehen könnte – was, schlicht gesagt, sehr nachteilig für diesen ist.

Im Zweifels- oder Verdachtsfall können sich Verbraucher:innen an die VZS (info@verbraucherzentrale.it Tel. 0471-975597) wenden, um eine fachkundige Beratung zu erhalten.

Beispiel_Benachrichtigung_über_die_Anhörung.pdf75.37 KB