

## Phishing-Opfer erhält 13.700€ zurück

Do, 29.05.2025 - 09:59

### Erfolg der VZS vor Bankenschiedsgericht

### Vorsicht vor Online-Investitionen in sozialen Netzwerken

Herr B. erhielt einen Anruf von Telefonnummer, die er der seiner Bank zuordnete. Der Anrufer – ein Betrüger – forderte den Kunden dazu auf, Änderungen am Authentifizierungssystem vorzunehmen. Der Betroffene gab an, sich in die Applikation eingeloggt zu haben, konnte aber nicht mehr genau nachvollziehen, was er in der Applikation unter Anleitung des Betrügers genau gemacht hatte. Es wurde jedoch eine Überweisung von 13.700 Euro durchgeführt. Herr B. bemerkte alsbald, einem Betrüger aufgesessen zu sein, aber das Geld war weg. Die VZS brachte diesen klassischen Phishing-Fall nach einer erfolglosen Beschwerde vor das Bankenschiedsgericht.

#### Was ist Phishing?

Bei Phishing wird man von Betrügern gezielt über E-Mail, SMS, Telefonanrufe oder andere Kommunikationswege kontaktiert. Ziel dieser Phishing-Nachrichten ist es, die betroffene Person zu einer bestimmten Handlung zu bewegen – beispielsweise zur Preisgabe sensibler Informationen wie finanzieller Daten, Login-Daten oder anderer persönlicher Informationen.

Die Täter greifen nicht direkt das Sicherheitssysteme von Banken an, sondern sie setzen auf Social Engineering: Durch psychologische Manipulation und Täuschung, unterstützt von Phishing-Elementen (z.B. gefälschten E-Mails, SMS oder Anrufen), und geben sich als die Hausbank aus. Auf diese Weise bringen sie ihre Opfer dazu, bestimmte Handlungen auszuführen, wie etwa auf Links zu gefälschten Webseiten zu klicken, schädliche Dateien herunterzuladen oder private Informationen wie Kontodaten oder Kreditkarteninformationen preiszugeben. Mit diesen Daten bzw. durch diese Handlungen können dann die Betrüger Bankoperationen durchführen und so das Geld der Opfer entwenden.

## Die Zwei Faktor-Authentifizierung

Der europäische und nationale Gesetzgeber haben festgelegt, dass bei jeder Bank-Transaktion oder Operation aus der Ferne, die potenziellen Schaden für den Kunden verursachen könnte, eine Zwei-Faktor-Authentifizierung durchgeführt werden muss. Sollte die Bank keine Zwei-Faktor-Authentifizierung durchgeführt haben, hat der Kunde das Anrecht für eine vollständige Rückerstattung des Schadens.

## Was ist die Zwei-Faktor-Authentifizierung?

Die Zwei-Faktor-Authentifizierung ist ein Sicherheitsverfahren, bei dem der Zugriff auf ein System oder die Durchführung einer Transaktion nur durch die Kombination von zwei unabhängigen Faktoren verifiziert wird. Ziel ist es, die Identität des Nutzers eindeutig zu bestätigen und die Sicherheit zu erhöhen.

Die beiden Faktoren stammen aus unterschiedlichen Kategorien:

1. **Wissen:** Etwas, das nur der Nutzer weiß, z. B. ein Passwort oder eine PIN.
2. **Besitz:** Etwas, das der Nutzer besitzt, z. B. ein Smartphone, eine Bankkarte oder ein TAN-Generator.
3. **Biometrie:** Etwas, das der Nutzer ist, z. B. ein Fingerabdruck, Gesichtserkennung oder die Stimme.

## Wie der ABF entschied

In diesem Fall konnte die Bank nicht nachweisen, dass beim Login ins Online-Banking eine Zwei-Faktor-Authentifizierung durchgeführt wurde. Fehlt auch nur ein Nachweis in sämtlichen Phasen des Zahlungsvorgangs, also bereits beim Zugang zum System, kann die Bank für den Schaden verantwortlich gemacht werden.

Da der Nachweis gemäß ABF nicht erbracht wurde, entschied man zugunsten des Kunden und forderte die Bank auf, den gesamten entstandenen Schaden zu ersetzen.

„Dieser Fall ist für den Kunden erfreulich ausgefallen. Doch nicht jeder darf mit einem ähnlichen Urteil rechnen“, erklärt VZS-Geschäftsführerin Gunde Bauhofer. „Wenn die Bank zweifelsfrei belegen kann, dass eine sogenannte starke Zwei-Faktor-Authentifizierung erfolgt ist, könnte die Entscheidung auch anders ausfallen.“

## Wie sollte man sich verhalten, wenn man Opfer eines Betrugs geworden ist?

- Karte bzw. Konto sofort sperren lassen
- bei den Behörden (Polizei/Carabinieri) Anzeige bzw. Strafanzeige erstatten;
- eine 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 vor Schlichtungsstelle der Banca d'Italia, dem Arbitro Bancario Finanziario ([www.arbitrobancariofinanziario.it](http://www.arbitrobancariofinanziario.it)) Rekurs eingereicht werden (Verbraucherorganisationen wie die VZS helfen bei einem solchen Rekurs).

### **Vermehrte Anfragen zu betrügerischem Online-Trading**

In den letzten Monaten erhielt die Verbraucherzentrale Südtirol (VZS) auch wieder vermehrt Anfragen zu Betrugsfällen im Zusammenhang mit Online-Trading. In den bekannten Fällen erfolgte die erste Kontaktaufnahme meist über soziale Netzwerke wie Facebook. Dabei werden auch Videos eingesetzt, in denen bekannte Persönlichkeiten – unter anderem auch Ministerpräsidentin Meloni – scheinbar Investitionen empfehlen. Diese Videos wurden jedoch mithilfe von Künstlicher Intelligenz manipuliert. Ist der erste Kontakt einmal hergestellt, werden die Betroffenen über persönliche Nachrichten, häufig per WhatsApp, dazu verleitet, vermeintlich lukrative Investitionen zu tätigen. Tatsächlich handelt es sich aber um Zahlungen, die nicht in Wertpapiere angelegt werden, sondern direkt bei den Betrügern landen.

Deshalb rät die Verbraucherzentrale dringend davon ab, auf vermeintlich lukrative Investmentmöglichkeiten einzugehen, die über soziale Netzwerke angeboten werden – zumindest nicht ohne vorherige sorgfältige Prüfung. Die dem VZS gemeldeten Beträge belaufen sich teils auf mehrere tausend Euro und überschreiten in nicht wenigen Fällen sogar die 100.000-Euro-Marke.

Die Berater:innen der Verbraucherzentrale Südtirol stehen für Informationen und Rat zur Verfügung (Tel. 0471-975597).