079... vertraut, aber vermehrt gefälscht

10. Juni 2025 | Beatrice Kübli

Auf dem Telefondisplay leuchtet eine unbekannte Nummer auf. Aber zumindest die Vorwahl ist vertraut: 079. Das ist eine Nummer der Swisscom, oder? Kann man dem Anruf also vertrauen? Nicht unbedingt, denn die Vorwahl hat nichts zu bedeuten. Es gibt verschiedene Möglichkeiten, wie Telefonnummern gefälscht werden können.

Früher konnte man aufgrund der Vorwahl klar zuweisen, aus welchem Land und welcher Region ein Telefonanruf stammt. Mit der fortschreitenden Digitalisierung kann man inzwischen diesen Angaben aber nicht mehr vertrauen. Telefonnummern können unter falschen Namen registriert oder gespooft sein. Auch ein TWINT-Account oder eine Kommunikation per WhatsApp mit einer bekannten Schweizer Vorwahl kann gefälscht sein.

Falschregistrierungen

Bei Falschregistrierungen werden Rufnummern vorsätzlich auf inexistente, oder auf fremde, aber reale Personen oder Firmen, registriert. Diese Rufnummern werden dann für kriminelle Geschäfte verwendet. Die Täterschaft erstellt damit Bankaccounts, registriert die Nummer bei Social-Media-Anbietern wie WhatsApp, Signal, Telegram, Viber, etc. oder erstellt einen TWINT-Account. Als vermeintliche/r Bürger/in mit Schweizer Wohnsitz tritt die Täterschaft mit dem potenziellen Opfer in Kontakt. Der Täter oder die Täterin hinter der Telefonnummer sitzt in der Regel jedoch nicht in der Schweiz, sondern im fernen Ausland. Mit der scheinbar schweizerischen Telefonnummer oder E-Mail-Adresse und entsprechend gewählten Vor- und Nachnamen vermitteln die Kriminellen Sicherheit. Die betroffene Person vertraut dem Gegenüber, löst Zahlungen aus oder gibt gar geheime Bankinformationen preis. Damit kann die Täterschaft komplette Bankkonten plündern. Teilweise werden die so übernommenen Bankkonten auch für Geldwäsche benutzt. Ein wirksamer **Schutz vor Falschregistrierungen** wird derzeit im Parlament behandelt.

Spoofing

Spoofing, also das Vortäuschen eines falschen Absenders, gibt es für E-Mails und auch für Telefonanrufe. Beim Call-ID-Spoofing (Telefone) lässt der/die Anrufer/in absichtlich eine falsche Rufnummer auf dem Display der angerufenen Person anzeigen. Das kann legal eingesetzt werden, beispielsweise für Firmenanrufe über das private Handy. Oft wird es aber von Kriminellen verwendet, um den Anruf vertrauenswürdig wirken zu lassen, etwa als käme er von einer bekannten Firma, einer Behörde oder sogar einem Freund. Kriminelle nutzen diese Technik, um persönliche Daten zu ergaunern, Betrug zu begehen oder Druck auszuüben. Da die angezeigte Nummer manipuliert ist, ist die Rückverfolgung schwierig. Auch ein wirksamer **Schutz vor Call-ID-Spoofing** wird aktuell im Parlament diskutiert.

Was können Sie tun?

- Machen Sie bei jedem Kontakt den Plausibilitätstest: Wie wahrscheinlich ist es, dass die Geschichte stimmt?
- Vertrauen Sie grundsätzlich keiner Zahlungsmethode, die Sie nicht bereits kennen und deren Handling Sie nicht komplett im Griff haben.
- Erscheinen die Zahlungsangaben für Sie plausibel? (WhatsApp Nr. und für Zahlung verwendete Rufnummern (Twint) sind bei Delikten oft nicht identisch.)
- Geben Sie keine sensiblen Daten bekannt. Keine Bank und auch nicht die Polizei fragen nach Ihren Kreditkarten-, Twint- oder E-Banking-Zugangsdaten.
- Legen Sie im Zweifelsfall auf und kontaktieren Sie die betroffene Person (Familienmitglied, Bankberater, Polizei etc.) über die offizielle, selbst recherchierte Nummer.
- Aktivieren Sie den Call-Filter bei Ihrem Telekom-Anbieter.
- Blockieren Sie verdächtige Nummern.

Die Schweizerische Kriminalprävention (SKP) ist eine interkantonale Fachstelle im Bereich Prävention von Kriminalität und Kriminalitätsfurcht. Sie wird von der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) getragen. Zu den wichtigsten Aufgaben der Schweizerischen Kriminalprävention gehören die Stärkung der interkantonalen Polizeizusammenarbeit im Bereich Kriminalprävention und die Aufklärung der Bevölkerung über kriminelle Phänomene, Präventionsmöglichkeiten und Hilfsangebote.