



079... un prefisso familiare, ma sempre più spesso falsificato

10 giugno 2025 | Beatrice Kübli

Sul display del telefono compare un numero sconosciuto. Il prefisso è però familiare: 079. Si tratta di un numero Swisscom? Oppure no? Ci si può fidare della chiamata? Non necessariamente, perché il prefisso non significa nulla. Esistono infatti diversi modi per falsificare i numeri di telefono.

In passato, il prefisso consentiva di identificare chiaramente il Paese e la regione di provenienza di una chiamata telefonica. Nel frattempo, in seguito alla progressiva digitalizzazione queste informazioni non sono però più affidabili. I numeri di telefono possono infatti essere registrati sotto falsi nominativi o essere oggetto di spoofing. Anche un account TWINT o una telefonata tramite WhatsApp con un prefisso svizzero noto possono essere falsificati.

False registrazioni

In caso di false registrazioni, i numeri di telefono vengono intenzionalmente registrati sotto nominativi inesistenti oppure a nome di persone o aziende reali ma ignote. Questi numeri di telefono vengono poi utilizzati per compiere dei reati. Le o i criminali creano account TWINT o bancari, oppure registrano il numero su piattaforme di social media come WhatsApp, Signal, Telegram, Viber, ecc. Spacciandosi poi per un cittadino o una cittadina residente in Svizzera, il o la criminale entra in contatto con una potenziale vittima. Di regola, però, chi si nasconde dietro il numero di telefono non risiede in Svizzera, bensì si trova in un Paese straniero lontano. L'uso di un numero di telefono o di un indirizzo e-mail apparentemente svizzeri e di un nome e un cognome scelti di conseguenza permette alle e ai criminali di trasmettere un senso di sicurezza. La vittima si fida del suo interlocutore o della sua interlocutrice, effettua pagamenti o rivela persino informazioni bancarie confidenziali. Così facendo, i o le criminali riescono a svuotare completamente conti bancari. Talvolta, i conti bancari piratati sono anche utilizzati per riciclare denaro. Attualmente è in discussione in Parlamento **una protezione efficace contro le false registrazioni.**

Spoofing

Lo spoofing è una particolare tipologia di attacco che consente ad un/a criminale di spacciarsi per un/a mittente autentico che in realtà non esiste per risultare “degno di fiducia” e carpire alla vittima designata informazioni confidenziali e dati sensibili. Nel caso dello spoofing dell’ID chiamante (telefoni), chi chiama fa apparire intenzionalmente un falso numero sul display del telefono della persona chiamata. Questa tecnica può essere utilizzata legalmente, come nel caso delle chiamate aziendali effettuate da un telefono cellulare privato. È però spesso usata dai e dalle criminali per far sembrare affidabile la chiamata, come se a telefonare fosse un’azienda nota, un’autorità o persino un amico. Le e i criminali utilizzano questa tecnica per appropriarsi di informazioni personali, mettere a segno delle truffe o esercitare pressioni. Dato che il numero visualizzato è manipolato, è difficile risalire al o alla mittente. Attualmente è in discussione in Parlamento anche **una protezione efficace contro lo spoofing dell’ID chiamante.**

Cosa potete fare?

- Effettuate un test di plausibilità ogni volta che ricevete una telefonata da un numero sconosciuto: quanto è probabile che la storia raccontata dal o dalla mittente sia vera?
- Non fidatevi mai di un metodo di pagamento che non conoscete e di cui non padroneggiate completamente il funzionamento.
- I dati di pagamento che appaiono vi sembrano plausibili? (In caso di truffa, il numero di WhatsApp e i numeri di telefono utilizzati per il pagamento, per esempio Twint, spesso non coincidono).
- Non divulgate mai dati sensibili. Nessuna banca né tantomeno la polizia vi chiedono i dati d’accesso della carta di credito, di Twint o dell’e-banking.
- In caso di dubbio, riagganciate e contattate la persona che vi ha chiamato (familiare, consulente bancario, polizia, ecc.) utilizzando il numero ufficiale che avrete avuto la premura di cercare prima voi stessi.
- Attivate il filtro delle chiamate presso il vostro operatore di telecomunicazioni.
- Bloccate i numeri sospetti.

La Prevenzione Svizzera della Criminalità (PSC) è un servizio intercantonale specializzato nel settore della prevenzione della criminalità e si adopera per migliorare il sentimento di sicurezza nella popolazione. Il servizio è sostenuto dalla Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia (CCDGP). Fra i compiti più importanti della PSC rientra il rafforzamento della cooperazione intercantonale fra forze di polizia nel settore della prevenzione della criminalità. Un altro importante compito è quello di informare la popolazione sui fenomeni criminali, sulle possibilità di prevenzione e sulle offerte di aiuto in quest’ambito.