



**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

## **Smishing: i suggerimenti del Garante per proteggersi dal phishing che sfrutta SMS e messaggistica**

## **Smishing: i suggerimenti del Garante per proteggersi dal phishing che sfrutta SMS e messaggistica**

Lo Smishing (o [phishing](#) tramite SMS) è una forma di truffa che utilizza messaggi di testo e sistemi di messaggistica (compresi quelli delle piattaforme social media) per appropriarsi di dati personali a fini illeciti (ad esempio, per poi sottrarre denaro da conti e carte di credito).

### **COME FUNZIONA?**

I messaggi di smishing **invitano i destinatari a compiere azioni** (cliccare link, ecc.) **o fornire informazioni con urgenza**, per non rischiare danni (es: blocco di utenze, blocco della carta di credito o del conto) o sanzioni.

I tuffatori (“smisher”) inviano ad esempio messaggi per chiederead esempio alle vittime di:

- **cliccare un link** che conduce ad un form online in cui inserire dati personali, dati bancari o della carta di credito, ecc.. Il link da cliccare può anche essere utilizzato per installare sullo smartphone della vittima programmi malevoli capaci di carpire dati personali conservati sul dispositivo o addirittura in grado di accedere alle app e ai programmi con cui si gestiscono Internet banking, carte di credito, ecc.;
- **scaricare un allegato** che può contenere programmi malevoli capaci di prendere il controllo dello smartphone o accedere ai dati in esso contenuti;
- **rispondere ai messaggi ricevuti inviando dati personali** (il codice fiscale, il PIN del Bancomat o quello utilizzato per l’Internet banking, il numero della carta, il codice di sicurezza della carta, i dati dell’OTP cioè della password temporanea per eseguire operazioni sul conto bancario e sulla carta di credito, ecc.);
- **chiamare un numero di telefono**, dove poi un finto operatore o un sistema automatizzato chiedono di fornire informazioni di vario tipo, compresi dati bancari e/o della carta di credito.

### **PERCHÉ LO SMISHING É COSÌ PERICOLOSO?**

Gli smisher fanno leva sul timore legato ad un rischio imminente per convincere le vittime ad abbassare il livello di prudenza e a reagire d’impulso.

Meglio quindi **diffidare dei messaggi che hanno toni ultimativi e intimidatori** o che spingono ad agire con fretta e urgenza.

Ecco alcuni **esempi** di messaggi da valutare con particolare attenzione e cautela:

- **una banca o un gestore di carte di credito o una società di recupero crediti** che segnalano un account compromesso, generici problemi tecnici o anomalie sul conto bancario o sulla carta di credito, da verificare urgentemente, ecc.;
- **offerte di sconti straordinari** su beni e servizi, o anche proposte di ricariche telefoniche da effettuare subito a costi incredibilmente vantaggiosi;
- **fornitori di beni o servizi che segnalano bollette o rate non pagate** da saldare con urgenza; pacchi, lettere o raccomandate da ritirare o che si ha difficoltà a consegnare, ecc.;
- **amministrazioni pubbliche** che segnalano la necessità di fornire dati, sanzioni da pagare (multe, cartelle esattoriali), anomalie da verificare, ecc.;
- piattaforme che offrono servizi di social media o di messaggistica che segnalano una **violazione dell'account personale** e chiedono di fornire dati e/o compiere determinate azioni (cliccare link, compilare form, chiamare numeri o inviare messaggi, ecc.).

## COME DIFENDERSI?

**Non comunicare mai dati e informazioni personali o dati come codici di accesso, PIN, password, dati bancari e della carta di credito a sconosciuti.** In ogni caso, occorre ricordare che istituzioni e banche non richiedono di fornire dati personali tramite SMS o messaggistica istantanea, specie se si tratta di informazioni come PIN, password, codici di autorizzazione, ecc., che, di solito, loro stessi ci invitano a mantenere strettamente riservate.



In generale, meglio **NON conservare le credenziali** (password, PIN, codici) di dati bancari o della carta di credito sullo smartphone. In caso di intrusioni informatiche sul dispositivo (tramite malware, ad esempio), questi dati potrebbero infatti essere facilmente sottratti.

Per proteggere i conti bancari e carte di credito è bene **controllare spesso le movimentazioni ed eventualmente attivare sistemi di alert automatico che avvisano l'utente di ogni operazione effettuata.**

Se si ha il dubbio di essere stati vittime di smishing, con il furto di credenziali del conto bancario o della carta di credito, è consigliabile **contattare al più presto la banca o il gestore della carta di credito** attraverso i **canali di comunicazione conosciuti e affidabili** per segnalare la truffa e chiedere di attivare le necessarie misure di protezione.

Se si ricevono messaggi da sconosciuti, **non cliccare sui link** in essi contenuti e **non aprire eventuali allegati**: potrebbero contenere virus o programmi capaci di prendere il controllo di computer e smartphone. Stessa accortezza con i messaggi che provengono da **numerazioni anomale o particolari** (ad esempio: numeri con poche cifre), oppure da **utenze identificate da un nome con il numero nascosto**. In questi casi è sempre bene fermarsi a riflettere, prestando la massima attenzione al contenuto e al mittente del messaggio.

Può anche capitare che il truffatore abbia preso il controllo del dispositivo e/o del numero di un nostro conoscente o di un soggetto (amministrazione, impresa, ecc.) con cui abbiamo rapporti o pratiche in corso (si parla in questo caso di “**spoofing**”) e che li usi per ingannarci.

In questo caso si possono mettere in pratica alcune precauzioni:

- **verificare se il testo presenta anomalie, come errori linguistici, grammaticali, lessicali, ecc.**, che spesso sono indizi di smishing;
- **chiedersi se davvero un nostro conoscente o un soggetto con cui abbiamo rapporti (amministrazione, impresa, ecc.) farebbe certe richieste** (ad esempio: richieste di soldi via SMS) e nel caso contattarlo su canali affidabili per chiedere conferma.

**Se si ricevono messaggi che invitano a richiamare determinati numeri di aziende o istituzioni, controllare SEMPRE prima se tali numeri corrispondono a quelli ufficiali** (ad esempio consultando i siti web istituzionali). Per estrema sicurezza, invece di contattare i numeri ricevuti, ci si può rivolgere al centralino o all'URP dell'azienda o dell'istituzione chiedendo di farsi mettere in contatto con l'ufficio che dovrebbe aver inviato il messaggio.

**Se si ha il dubbio di essere stati di smishing (e in generale di phishing) riguardo dati bancari e/o della carta di credito, è consigliabile contattare immediatamente la banca o il gestore della carta di credito attraverso canali di comunicazione conosciuti e affidabili** per segnalare l'accaduto e, in caso di sottrazione di denaro, richiedere il blocco delle transazioni. In questa seconda ipotesi, si può anche segnalare la truffa subito alle [autorità di polizia](#).



## **VEDI ANCHE**

- [Phishing: pagina informativa](#)

- [Cybersecurity: pagina informativa](#)