Smishing: 25 SMS truffa reali e come difendersi nel 2026

Maria Cattini | 27/02/2026 | Sicurezza digitale

Hai ricevuto un SMS su un pacco in giacenza che non aspettavi?
O un “avviso urgente” dalla tua banca con un link da cliccare entro 30 minuti?

Non è sfortuna. È **smishing**.

Nel 2026 gli SMS truffa sono uno dei canali più redditizi per il cybercrime. Colpiscono privati, aziende, professionisti. E lo fanno con messaggi sempre più credibili, scritti meglio di certe newsletter aziendali.

Secondo il report 2025 del Cert-AgID, in un solo anno sono state registrate 3.620 campagne malevole, con un aumento del 55% degli attacchi verso dispositivi Android. Molte infezioni partono proprio da link ricevuti via SMS .

Non parliamo di casi isolati. Parliamo di un ecosistema strutturato.

Cos’è lo smishing e perché funziona ancora

Lo smishing è phishing via SMS.
Ricevi un messaggio che sembra provenire da banca, corriere o ente pubblico. Clicchi. Inserisci dati. I criminali incassano.

La Polizia Postale lo descrive come un meccanismo che sfrutta un mittente apparentemente affidabile e un link verso un sito clone .

Funziona per tre motivi concreti:

1. L’SMS appare più “ufficiale” di una mail.
2. Sfrutta contesti reali: spedizioni, pedaggi, bonifici.
3. Lo leggiamo in mobilità, su schermi piccoli, con poca attenzione.

Oggi i testi non hanno più errori grammaticali evidenti. L’intelligenza artificiale ha alzato il livello linguistico. Il vecchio italiano sgangherato non è più il campanello d’allarme principale.

Le 25 tipologie di SMS truffa più diffuse

Nel dossier analizzato vengono elencati 25 schemi ricorrenti . Non sono teoria. Sono casi reali.

Pacchi e consegne fantasma

Il grande classico.

Messaggio:

“Poste: pacco in giacenza per tassa non pagata. Regolarizza ora: [link]”

Il Cert-AgID ha documentato campagne che imitano il portale ufficiale di Poste con pagine clone per rubare credenziali e dati di pagamento .

Pedaggi, ZTL e parcheggi

Importo basso. Pressione alta.

“Pedaggio A1 non pagato di 3,25 €. Paga subito per evitare sanzioni.”

Abuso del marchio Autostrade per l’Italia documentato in campagne recenti .

Multe e falsi PagoPA

Finta notifica con importo preciso e scadenza ravvicinata.
Link verso pagina di pagamento falsa.

Il modello è già stato ampiamente usato via mail e PEC. L’SMS è la naturale estensione .

Falsi avvisi bancari

“Attività anomala rilevata. Verifica entro 30 minuti.”

Il tema banking resta tra i più usati per distribuire malware bancari su Android e Windows .

Qui spesso entra in gioco un secondo livello: telefonata del finto operatore che chiede OTP o installazione di app remote.

Codici OTP “non richiesti”

Ricevi un codice. Non l’hai chiesto.
Subito dopo arriva un link per “proteggere l’account”.

Obiettivo: farti consegnare il vero codice di autenticazione.

Marketplace: Subito, Vinted, annunci

Hai pubblicato un oggetto. Arriva un SMS:

“Pagamento ricevuto. Conferma per incassare.”

La pagina clone chiede dati carta “per ricevere l’accredito”.
È una delle varianti più redditizie oggi.

SPID e identità digitale

“SPID sospeso per verifica documenti.”

Campagne a tema identità digitale sono state documentate in più occasioni . Il vettore può essere email o SMS.

Recupero crediti aggressivo

“Ultimo avviso per debito di 312,70 €. Procederemo legalmente.”

Qui la leva è la paura. Molti pagano pur sapendo di non avere debiti.

Crypto e trading

Promesse di rendimenti rapidi o finti blocchi wallet.
Il link punta a piattaforme non regolamentate o portali clone.

Finti supporti tecnici Apple, Google, Microsoft

“Accesso non autorizzato rilevato.”

Invito a scaricare app remote o inserire codici di ripristino.
Il controllo del dispositivo passa al truffatore.

Spoofing: quando il mittente sembra reale

Una delle varianti più insidiose è lo spoofing.

L’SMS appare nello stesso thread della banca o del corriere.
Oppure sembra arrivare dal tuo stesso numero .

Qui il mittente corretto non è garanzia di autenticità.

Come riconoscere uno smishing in 10 secondi

Non servono competenze tecniche. Serve metodo.

1. Fuori contesto

Aspetti un pacco?
Hai davvero un conto in quella banca?

Se il contesto non coincide, fermati.

2. Urgenza artificiale

“Entro 24 ore.”
“Ultima possibilità.”
“Blocco immediato.”

La fretta è una leva psicologica, non una procedura bancaria .

3. Link anomali

Domini con lettere sostituite.
Estensioni insolite (.top, .xyz).
URL accorciati.

Regola semplice: per banca e PA, apri l’app ufficiale o digita l’indirizzo a mano.

Hai cliccato? Cosa fare subito

L’errore non è cliccare. È non reagire.

Se hai inserito dati bancari

Chiama immediatamente il numero ufficiale della banca.
Blocca carta e credenziali.
Verifica movimenti recenti .

Se hai installato un file APK su Android

Molte campagne di smishing distribuiscono trojan bancari .

Azioni immediate:

• Disinstalla l’app sospetta
• Esegui scansione con soluzione mobile security
• Valuta ripristino alle impostazioni di fabbrica

Se hai fornito documenti

Attiva alert su bonifici e movimenti.
Valuta denuncia alla Polizia Postale .

Prevenzione: ridurre l’esposizione

Non esiste rischio zero. Esiste riduzione del rischio.

• Attiva filtri SMS su iOS e Android
• Mantieni sistema operativo aggiornato
• Usa protezione mobile con antiphishing
• In azienda, inserisci lo smishing nei programmi di awareness

Il telefono personale è ormai parte del perimetro aziendale. Ignorarlo è un errore strategico.

Pro e contro dell’SMS come canale di comunicazione

Per le aziende

Pro:

• Tasso di apertura altissimo
• Immediatezza

Contro:

• Facile spoofing
• Difficoltà di verifica per l’utente
• Erosione della fiducia

Per i criminali

Pro:

• Costi bassi
• Alta probabilità di clic
• Targeting mirato

Contro:

• Blocco progressivo dei numeri
• Tracciabilità tramite segnalazioni aggregate

È una guerra di adattamento continuo.

Perché lo smishing è un problema strutturale

Non è solo una truffa al dettaglio.

È:

• Distribuzione di malware bancari
• Accesso a conti aziendali
• Raccolta di dati per attacchi successivi
• Ingresso laterale verso infrastrutture corporate

Il confine tra vittima privata e breach aziendale è più sottile di quanto sembri.

Una domanda scomoda

Quante volte hai cliccato senza pensarci?

Lo smishing non colpisce solo chi “non è esperto”.
Colpisce chi è stanco, distratto, di fretta.

Il vero antivirus è il dubbio metodico.

Vuoi alzare il tuo livello di difesa digitale?

Se ti occupi di OSINT, cybersecurity o semplicemente vuoi proteggere il tuo ecosistema digitale:

• Studia i pattern ricorrenti
• Analizza i domini prima di cliccare
• Inserisci lo smishing nei tuoi scenari di threat modeling

Vuoi approfondire casi reali e tecniche di verifica?
Iscriviti alla newsletter su https://coondivido.substack.com/
Unisciti alla community Telegram: https://t.me/osintaipertutti

La prossima notifica potrebbe essere una trappola.
La differenza la fa il tuo metodo.
Hai ricevuto un SMS su un pacco in giacenza che non aspettavi?
O un “avviso urgente” dalla tua banca con un link da cliccare entro 30 minuti?

Non è sfortuna. È **smishing**.

Nel 2026 gli SMS truffa sono uno dei canali più redditizi per il cybercrime. Colpiscono privati, aziende, professionisti. E lo fanno con messaggi sempre più credibili, scritti meglio di certe newsletter aziendali.

Secondo il report 2025 del Cert-AgID, in un solo anno sono state registrate 3.620 campagne malevole, con un aumento del 55% degli attacchi verso dispositivi Android. Molte infezioni partono proprio da link ricevuti via SMS .

Non parliamo di casi isolati. Parliamo di un ecosistema strutturato.

Cos’è lo smishing e perché funziona ancora

Lo smishing è phishing via SMS.

Ricevi un messaggio che sembra provenire da banca, corriere o ente pubblico. Clicchi. Inserisci dati. I criminali incassano.

La Polizia Postale lo descrive come un meccanismo che sfrutta un mittente apparentemente affidabile e un link verso un sito clone .

Funziona per tre motivi concreti:

1. L’SMS appare più “ufficiale” di una mail.
2. Sfrutta contesti reali: spedizioni, pedaggi, bonifici.
3. Lo leggiamo in mobilità, su schermi piccoli, con poca attenzione.

Oggi i testi non hanno più errori grammaticali evidenti. L’intelligenza artificiale ha alzato il livello linguistico. Il vecchio italiano sgangherato non è più il campanello d’allarme principale.

Le 25 tipologie di SMS truffa più diffuse

Nel dossier analizzato vengono elencati 25 schemi ricorrenti . Non sono teoria. Sono casi reali.

Pacchi e consegne fantasma

Il grande classico.

Messaggio:
“Poste: pacco in giacenza per tassa non pagata. Regolarizza ora: [link]”

Il Cert-AgID ha documentato campagne che imitano il portale ufficiale di Poste con pagine clone per rubare credenziali e dati di pagamento .

Pedaggi, ZTL e parcheggi

Importo basso. Pressione alta.

“Pedaggio A1 non pagato di 3,25 €. Paga subito per evitare sanzioni.”

Abuso del marchio Autostrade per l’Italia documentato in campagne recenti .

Multe e falsi PagoPA

Finta notifica con importo preciso e scadenza ravvicinata.
Link verso pagina di pagamento falsa.

Il modello è già stato ampiamente usato via mail e PEC. L’SMS è la naturale estensione .

Falsi avvisi bancari

“Attività anomala rilevata. Verifica entro 30 minuti.”

Il tema banking resta tra i più usati per distribuire malware bancari su Android e Windows .

Qui spesso entra in gioco un secondo livello: telefonata del finto operatore che chiede OTP o installazione di app remote.

Codici OTP “non richiesti”

Ricevi un codice. Non l’hai chiesto.
Subito dopo arriva un link per “proteggere l’account”.

Obiettivo: farti consegnare il vero codice di autenticazione.

Marketplace: Subito, Vinted, annunci

Hai pubblicato un oggetto. Arriva un SMS:

“Pagamento ricevuto. Conferma per incassare.”

La pagina clone chiede dati carta “per ricevere l’accredito”.
È una delle varianti più redditizie oggi.

SPID e identità digitale

“SPID sospeso per verifica documenti.”

Campagne a tema identità digitale sono state documentate in più occasioni . Il vettore può essere email o SMS.

Recupero crediti aggressivo

“Ultimo avviso per debito di 312,70 €. Procederemo legalmente.”

Qui la leva è la paura. Molti pagano pur sapendo di non avere debiti.

Crypto e trading

Promesse di rendimenti rapidi o finti blocchi wallet.
Il link punta a piattaforme non regolamentate o portali clone.

Finti supporti tecnici Apple, Google, Microsoft

“Accesso non autorizzato rilevato.”

Invito a scaricare app remote o inserire codici di ripristino.
Il controllo del dispositivo passa al truffatore.

Spoofing: quando il mittente sembra reale

Una delle varianti più insidiose è lo spoofing.

L’SMS appare nello stesso thread della banca o del corriere.
Oppure sembra arrivare dal tuo stesso numero .

Qui il mittente corretto non è garanzia di autenticità.

Come riconoscere uno smishing in 10 secondi

Non servono competenze tecniche. Serve metodo.

1. Fuori contesto

Aspetti un pacco?
Hai davvero un conto in quella banca?

Se il contesto non coincide, fermati.

2. Urgenza artificiale

“Entro 24 ore.”
“Ultima possibilità.”
“Blocco immediato.”

La fretta è una leva psicologica, non una procedura bancaria .

3. Link anomali

Domini con lettere sostituite.
Estensioni insolite (.top, .xyz).
URL accorciati.

Regola semplice: per banca e PA, apri l’app ufficiale o digita l’indirizzo a mano.

Hai cliccato? Cosa fare subito

L’errore non è cliccare. È non reagire.

Se hai inserito dati bancari

Chiama immediatamente il numero ufficiale della banca.
Blocca carta e credenziali.
Verifica movimenti recenti .

Se hai installato un file APK su Android

Molte campagne di smishing distribuiscono trojan bancari .

Azioni immediate:

• Disinstalla l’app sospetta
• Esegui scansione con soluzione mobile security
• Valuta ripristino alle impostazioni di fabbrica

Se hai fornito documenti

Attiva alert su bonifici e movimenti.
Valuta denuncia alla Polizia Postale .

Prevenzione: ridurre l’esposizione

Non esiste rischio zero. Esiste riduzione del rischio.

• Attiva filtri SMS su iOS e Android
• Mantieni sistema operativo aggiornato
• Usa protezione mobile con antiphishing
• In azienda, inserisci lo smishing nei programmi di awareness

Il telefono personale è ormai parte del perimetro aziendale. Ignorarlo è un errore strategico.

Pro e contro dell’SMS come canale di comunicazione

Per le aziende

Pro:

• Tasso di apertura altissimo
• Immediatezza

Contro:

• Facile spoofing
• Difficoltà di verifica per l’utente
• Erosione della fiducia

Per i criminali

Pro:

• Costi bassi
• Alta probabilità di clic
• Targeting mirato

Contro:

• Blocco progressivo dei numeri
• Tracciabilità tramite segnalazioni aggregate

È una guerra di adattamento continuo.

Perché lo smishing è un problema strutturale

Non è solo una truffa al dettaglio.

È:

• Distribuzione di malware bancari
• Accesso a conti aziendali
• Raccolta di dati per attacchi successivi
• Ingresso laterale verso infrastrutture corporate

Il confine tra vittima privata e breach aziendale è più sottile di quanto sembri.

Una domanda scomoda

Quante volte hai cliccato senza pensarci?

Lo smishing non colpisce solo chi “non è esperto”.
Colpisce chi è stanco, distratto, di fretta.

Il vero antivirus è il dubbio metodico.

Vuoi alzare il tuo livello di difesa digitale?

Se ti occupi di OSINT, cybersecurity o semplicemente vuoi proteggere il tuo ecosistema digitale:

• Studia i pattern ricorrenti
• Analizza i domini prima di cliccare
• Inserisci lo smishing nei tuoi scenari di threat modeling

Vuoi approfondire casi reali e tecniche di verifica?
Iscriviti alla newsletter su https://coondivido.substack.com/
Unisciti alla community Telegram: https://t.me/osintaipertutti

La prossima notifica potrebbe essere una trappola.
La differenza la fa il tuo metodo.