MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Cyber Security Brochure

Smishing e Vishing

Le nuove frontiere delle truffe digitali tra SMS e telefonate

Sommario

Cosa troverai in questa brochure

Introduzione

Negli ultimi anni l'aumento dei **servizi digitali** e l'uso quotidiano dello **smartphone** hanno contribuito alla diffusione di **truffe** particolarmente insidiose, quali lo **Smishing** e il **Vishing**.
Lo **Smishing**, ovvero il Phishing via SMS, si verifica quando ricevi un **messaggio** di **testo** che sembra provenire da una **fonte affidabile**, come una banca, un'Autorità o persino la tua stessa Istituzione di appartenenza. In realtà, il messaggio è stato creato da un **malintenzionato** con l'obiettivo di indurti a **cliccare** su **link fraudolenti** e/o fornire **credenziali di accesso**, come password o codici univoci.
Il **Vishing** è la variante del Phishing che usa la **telefonia**, chiamate VoIP o tradizionali, per ingannare le persone.
I criminali informatici possono ricorrere a tecniche di **falsificazione** del **numero** di **telefono**, note come **spoofing**. Con questo espediente, il **numero** visualizzato sul tuo telefono può **sembrare autentico**, rendendo difficile capire se il messaggio o la chiamata provenga davvero dalla fonte indicata. In questo modo, i cybercriminali possono indurti a **rivelare informazioni personali** oppure **registrare** la tua **voce** durante la conversazione, per poi mettere in atto **ulteriori truffe** o attacchi di Phishing sempre più mirati e sofisticati.

Attacchi Social Engineering/Phishing nel mondo

+75% Incremento di attacchi di tipo Phishing (inclusi Smishing e Vishing)

Le caratteristiche dello Smishing e del Vishing

Messaggi o chiamate urgenti: gli attaccanti creano un forte senso di urgenza, tramite SMS o telefonate che richiedono azioni immediate.

Credibilità dell'interlocutore: il malintenzionato assume una falsa identità e ti contatta fingendo di essere un soggetto affidabile.

Link o numeri fraudolenti: gli SMS possono contenere link che rimandano a siti falsi e, al pari delle chiamate, possono mostrare numeri mittenti falsificati per apparire affidabili.

Raccolta di dati sensibili: L'obiettivo di entrambi gli attacchi è quello di ottenere codici OTP, password o informazioni riservate.

Fonte: Rapporto Clusit 2025

Attento alle comunicazioni fraudolente!

Rischi

01 *Compromissione account*

Attraverso i messaggi di **Smishing**, i **malintenzionati** possono **inviare link fraudolenti** che, se eseguiti, avviano il **download** di software malevoli o indirizzare verso pagine progettate per compromettere il dispositivo. I criminali informatici sfruttano **linguaggio colloquiale**, **urgenza** e **link brevi**, aumentando la possibilità di successo anche su utenti cauti.

02 *Voice cloning*

Durante attacchi di **Vishing**, i **cybercriminali** possono **registrare** la tua **voce** anche tramite brevi risposte o durante **chiamate** apparentemente **mute**. I campioni vocali raccolti possono essere successivamente manipolati tramite tecniche di **Voice cloning** per riprodurre artificialmente la tua voce e impiegarla, a tua insaputa, in tentativi di **frode o impersonificazione**.

03 *Escalation dell'attacco*

Gli attacchi di **Smishing e Vishing** non si esauriscono spesso in un singolo episodio, ma possono rappresentare la **fase iniziale** di una **compromissione più ampia**. Le informazioni ottenute durante il primo contatto possono essere riutilizzate per rendere più credibili **tentativi di attacco successivi** o per accedere ad altri servizi digitali collegati.

Contromisure

In caso di **SMS sospetti**, **evita di cliccare su link non verificati**. Controlla sempre l'identità del mittente e valuta con attenzione la coerenza della richiesta ricevuta.

In caso di **chiamate sospette o prive di interlocutore**, **evita di parlare e interrompi** immediatamente **la comunicazione telefonica**.

In caso di comunicazioni sospette o non richieste, **evita di condividere informazioni personali**, credenziali di accesso, codici di sicurezza o altri dati sensibili.

Come difendersi?

Verifica dell'identità

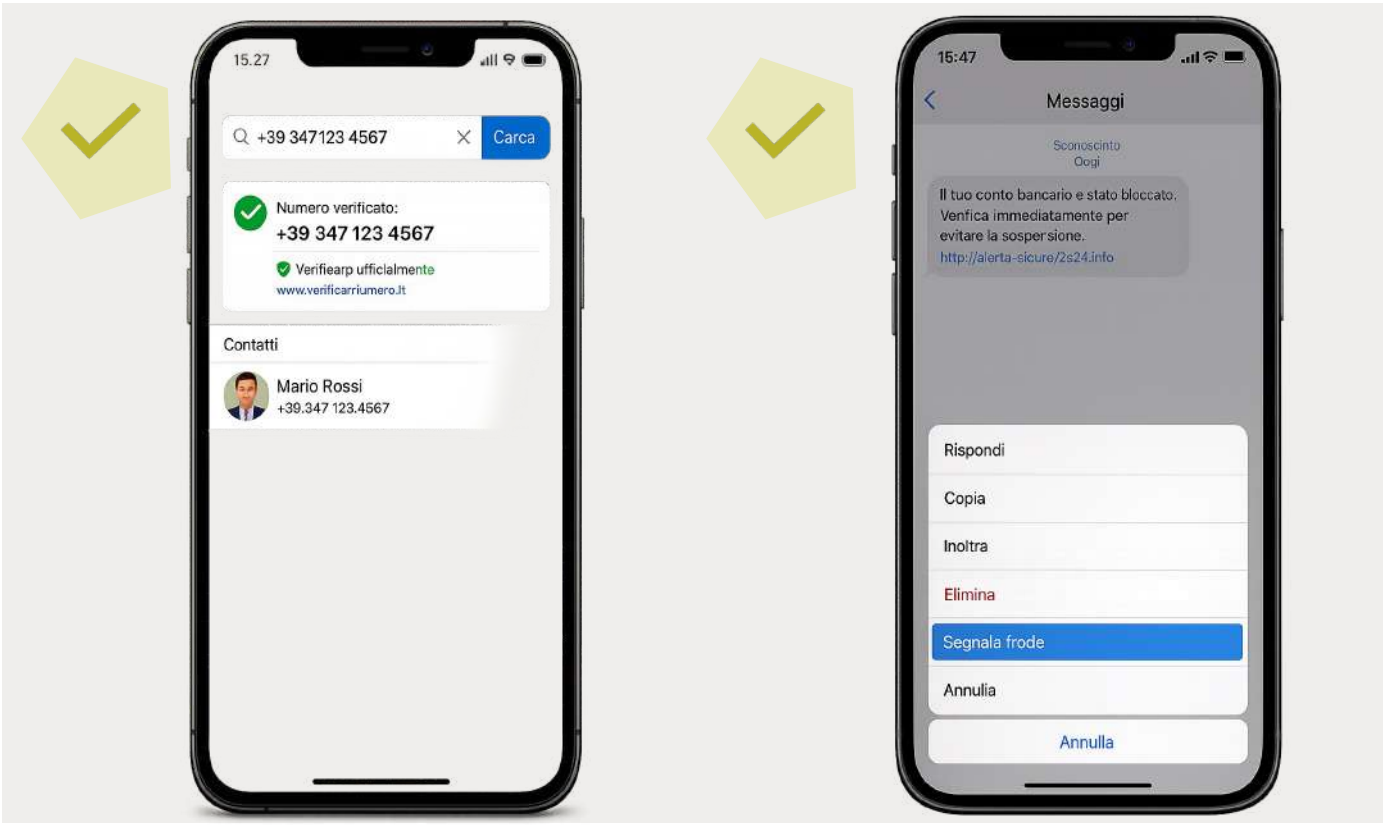
Utilizza i **recapiti ufficiali** dell'Ente per ricontattare l'**interlocutore** in caso di **richieste sospette** avvenute tramite SMS o chiamate telefoniche. Questa operazione ti consente di verificare l'autenticità della comunicazione anche nel caso in cui il numero visualizzato sia stato falsificato tramite tecniche di **Caller ID spoofing.**

Blocco di numeri sospetti

Utilizza le funzionalità integrate nel dispositivo o nell'applicazione di gestione delle chiamate e degli SMS per inserire il **numero nell'elenco** dei **contatti bloccati**. Questa operazione ti consente di **impedire ulteriori chiamate** o **messaggi** provenienti dallo **stesso recapito**, riducendo l'esposizione a tentativi ripetuti di contatto fraudolento.

Segnalazione degli eventi

Utilizza le funzionalità del dispositivo o dell'applicazione per **segnalare SMS** o **chiamate** sospette come spam o **tentativi** di **frode**. Questa operazione contribuisce al corretto funzionamento dei sistemi di protezione integrati, favorendo il riconoscimento automatico delle comunicazioni fraudolente e **riducendo** il rischio di ulteriori **tentativi** di **contatto**.



Security Trend

Smishing: la truffa a tema Autostrade per l'Italia

Nell'ottobre 2025 il CERT-AGID ha segnalato una **campagna di Smishing** che ha sfruttato il nome di **Autostrade per l'Italia** per diffondere **SMS fraudolenti**.
I messaggi inviati alle vittime facevano riferimento a un presunto **pedaggio non saldato** ed esortavano il destinatario a **cliccare** su un **link** allegato, con il pretesto di effettuare alcune **verifiche**.
Il **collegamento** conduceva in realtà a un **sito malevolo**, progettato per imitare quello ufficiale e indurre l'utente a **inserire dati personali** e **informazioni** di **pagamento**, con l'obiettivo di **sottrarli** in modo **illecito**.
L'episodio evidenzia come queste campagne sfruttino leve psicologiche come **l'urgenza** e la **credibilità** del **mittente** per **aumentare** le **probabilità** di **successo.**
A tal proposito, risulta fondamentale adottare un **approccio prudente e critico**, per evitare di condividere dati sensibili e di cadere vittima di eventuali truffe.

ottobre 2025

Vishing: Il Caso Crosetto

Nel febbraio 2025 è stato segnalato in Italia un caso di **Vishing** che ha ricevuto ampia attenzione mediatica. Alcuni cybercriminali hanno utilizzato tecnologie di **voice cloning** basate sull'Intelligenza Artificiale per riprodurre la voce del **Ministro della Difesa Guido Crosetto** e contattare telefonicamente imprenditori di alto profilo.
Durante le chiamate venivano descritte false **situazioni** di **emergenza** e richieste ingenti somme di denaro, presentate come presunto **riscatto** per **giornalisti rapiti** all'estero.
L'episodio evidenzia quanto le tecniche di ingegneria sociale possano risultare sempre più sofisticate grazie all'impiego di strumenti tecnologici avanzati. Una buona pratica consiste nel **verificare** sempre **l'autenticità** delle **richieste, attaccando e richiamando** tramite canali ufficiali, ed **evitando** di effettuare **trasferimenti** di **denaro** sulla base di **comunicazioni telefoniche urgenti** o **non verificabili**.

febbraio 2025

MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Restate sintonizzati:

nuovi approfondimenti sulla cybersecurity vi aspettano nelle prossime pubblicazioni.