MUR

CYBER
SAPERE

Cyber Security Brochure

Smishing and Vishing

The new frontiers of digital scams through SMS and phone calls

Summary

What you will find in this brochure

Introduction

In recent years, the growth of digital services and the daily use of smartphones have contributed to the spread of particularly insidious scams such as Smishing and Vishing.

Smishing, or phishing via SMS, occurs when you receive a text message that appears to come from a trusted source such as a bank, an authority or even your own institution. In reality, the message has been created by an attacker to induce you to click fraudulent links and/or provide access credentials such as passwords or one-time codes.

Vishing is the phishing variant that uses telephone calls, either VoIP or traditional calls, to deceive people. Criminals may use phone number falsification techniques known as spoofing. The number shown on your phone may look authentic, making it difficult to understand whether the message or call really comes from the indicated source. In this way, cybercriminals can induce you to reveal personal information or record your voice during the conversation for further scams or increasingly targeted phishing attacks.

Social Engineering/Phishing attacks worldwide

+75%

Increase in phishing-type attacks, including Smishing and Vishing.

Characteristics of Smishing and Vishing

1. **Urgent messages or calls:** Attackers create a strong sense of urgency through SMS or calls that require immediate action.
2. **Credibility of the interlocutor:** The attacker assumes a false identity and contacts you pretending to be a trusted party.
3. **Fraudulent links or numbers:** SMS may contain links to fake sites and, like calls, may show falsified sender numbers.
4. **Collection of sensitive data:** The goal of both attacks is to obtain OTP codes, passwords or confidential information.

Source: CLUSIT Report 2025

Beware of fraudulent communications!

Risks

01 Account compromise

Through Smishing messages, attackers can send fraudulent links that, if opened, start the download of malicious software or redirect to pages designed to compromise the device. They use colloquial language, urgency and short links to increase their chances of success even with cautious users.

02 Voice cloning

During Vishing attacks, cybercriminals can record your voice even through brief answers or apparently silent calls. Voice samples may later be manipulated with voice cloning techniques to artificially reproduce your voice and use it in fraud or impersonation attempts without your knowledge.

03 Attack escalation

Smishing and Vishing often do not end with a single episode. They may represent the first stage of a broader compromise. Information obtained during the first contact can be reused to make later attacks more credible or to access other connected digital services.

Countermeasures

In case of suspicious SMS messages, avoid clicking unverified links. Always check the sender identity and carefully assess whether the request is consistent.

In case of suspicious or silent calls, avoid speaking and immediately end the phone communication.

In case of suspicious or unsolicited communications, avoid sharing personal information, access credentials, security codes or other sensitive data.

How to protect yourself?

Identity verification

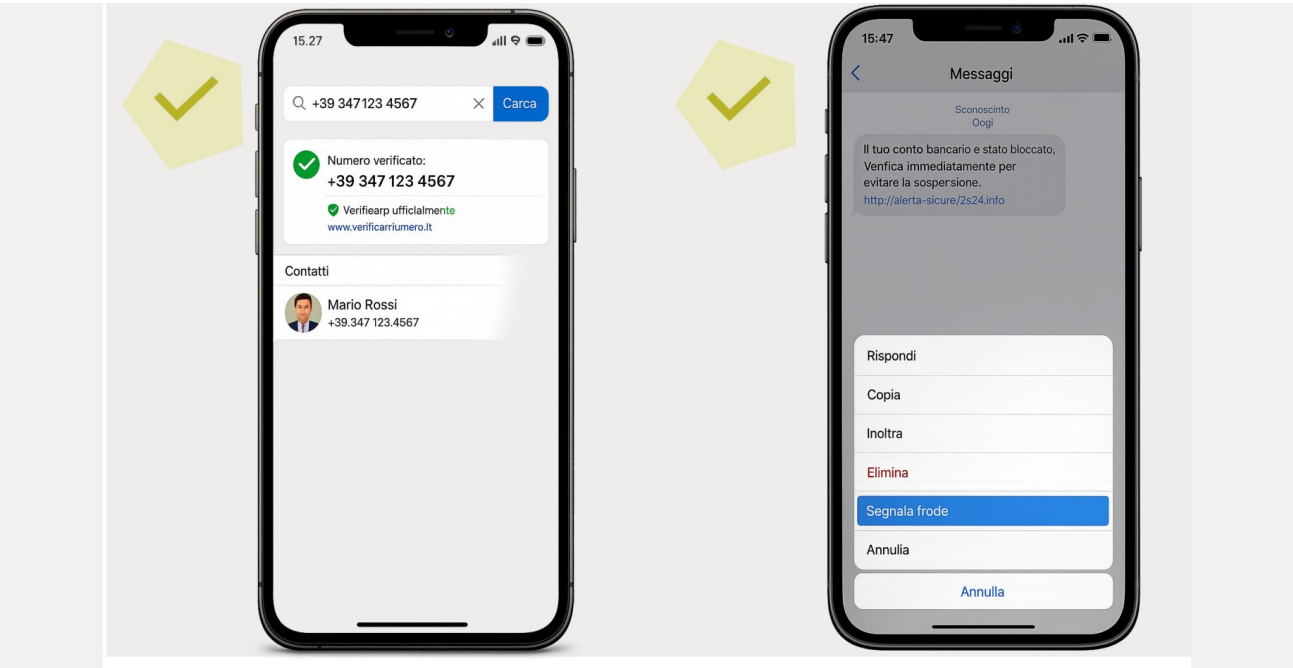
Use the organization's official contact details to call the interlocutor back when suspicious requests arrive by SMS or phone. This lets you verify the authenticity of the communication even if the displayed number has been falsified through Caller ID spoofing.

Blocking suspicious numbers

Use the built-in functions of your device or SMS/call management app to add the number to your blocked contacts. This prevents further calls or messages from the same number and reduces exposure to repeated fraudulent contacts.

Reporting events

Use your device or application functions to report suspicious SMS messages or calls as spam or attempted fraud. This supports built-in protection systems, improves automatic recognition of fraudulent communications and reduces future contact attempts.



Security Trend

Smishing: the Autostrade per l'Italia themed scam

In October 2025, CERT-AGID reported a Smishing campaign that abused the name of Autostrade per l'Italia to distribute fraudulent SMS messages. The messages referred to a supposed unpaid toll and urged the recipient to click an attached link to perform checks. The link actually led to a malicious site designed to imitate the official one and induce the user to enter personal and payment information so it could be stolen. The case shows how these campaigns exploit psychological levers such as urgency and sender credibility to increase their chances of success. A cautious and critical approach is essential to avoid sharing sensitive data and becoming a victim of fraud.

October 2025

Vishing: the Crosetto case

In February 2025, a Vishing case in Italy received wide media attention. Cybercriminals used AI-based voice cloning technologies to reproduce the voice of Defence Minister Guido Crosetto and call high-profile entrepreneurs. During the calls they described false emergency situations and requested large sums of money, presented as a supposed ransom for journalists kidnapped abroad. The case shows how Social Engineering techniques can become increasingly sophisticated through advanced technology. A good practice is to always verify the authenticity of requests, hang up and call back through official channels, and avoid transferring money based on urgent or unverifiable phone communications.

February 2025

MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Stay tuned:
new cybersecurity insights
await you
in upcoming publications.