MUR

CYBER
SAPERE

Cyber Security Brochure

The Art of Deception

What Social Engineering
is and how it works

Summary

What you will find in this brochure

Introduction

In recent years, the evolution of digital systems has transformed the way we communicate, work and access online services.

In this context, Social Engineering has become one of the most widespread threats because it exploits the human factor rather than technological vulnerabilities.

Through interactions that appear legitimate, attackers try to gain people's trust and induce them to perform actions that help the deception succeed. Personal details shared too lightly, or simple information made public, can be used to conduct targeted attacks capable of compromising information security.

Understanding the nature of Social Engineering and recognizing how easily it can enter digital communications is the first step toward greater awareness and safer online behavior.

Main characteristics of Social Engineering

1. **Use of public information:** Data found online are analyzed to create personalized, high-success messages.
2. **Psychological manipulation:** The attacker exploits emotions, trust and habitual behavior to induce harmful actions.
3. **Appearance of legitimacy:** Attacks appear as real, credible communications consistent with the victim's context.
4. **Compromise and persistence:** The criminal exfiltrates personal data and may reuse it for more sophisticated attacks.

Evolution of Phishing and Social Engineering attacks 2020-2024

+35%

Their spread increased by 35% in 2024 compared with previous years.

The human factor remains involved in 80-90% of cyberattacks.

Source: CLUSIT Report 2025

Do not fall for deception!

Risks

01 *Invisible and progressive information gathering*

Attackers do not strike randomly. They gather information about you step by step. Data such as your job role, habits or online content, when combined, can create a detailed profile. This invisible process makes attacks convincing and difficult to recognize.

02 *Psychological manipulation*

Attackers study your language, habits and weak points to convince you to take harmful actions. Through emails, messages or phone calls, they may push you to click suspicious links, open potentially malicious attachments, reveal personal data or grant access permissions.

03 *Credential theft*

Through carefully crafted login pages, criminals may trick you into revealing sensitive data such as access credentials, PINs and other confidential information. If the same password is reused, unauthorized access may extend to other systems and services.

Countermeasures

Avoid publishing photos of badges, documents or any content that may reveal highly confidential or private information on social networks, forums or public platforms.

When a communication appears suspicious or pushes you to act within a limited time, carefully verify the legitimacy of the request before interacting.

Do not provide passwords, codes or sensitive data by email, chat or phone. Use complex passwords and enable multi-factor authentication (MFA) whenever available.

How to protect yourself?

Limited sharing

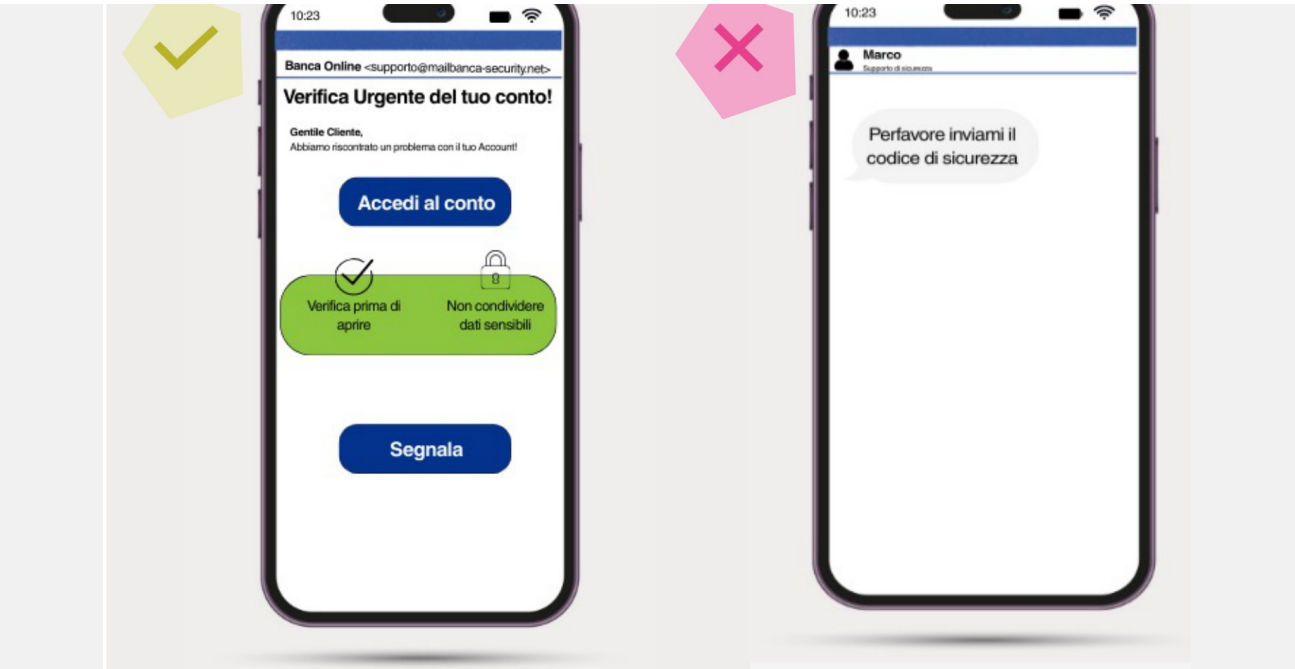
In online interactions, limit the disclosure of personal and professional information. Reducing your information exposure helps lower the risk of Social Engineering attacks and makes it harder to exploit real details to simulate legitimate requests.

Context verification

When you receive messages, emails or communications, always pay attention to the tone used. Unmotivated urgency, formal language that does not fit the context, or excessive familiarity may be warning signs of malicious communication.

Report anomalies

If you receive suspicious messages or notice unusual online behavior, do not ignore it. Alert the person involved or contact the organization or company through official channels. A timely report can prevent problems and protect data and people.



Security Trend

Malicious email campaign in the name of the ACN Director General

In July 2025, a phishing campaign was detected via email that unlawfully used the name of the Director General of the Italian National Cybersecurity Agency (ACN). To give the message an appearance of official authority, it was sent from a private email address but displayed the Director General's name and institutional title in the sender field. This is a typical identity spoofing technique intended to make the recipient consider the communication legitimate because of the role being invoked. The email claimed that the user was accused of a presumed cybercrime related to viewing illicit content, threatening judicial action if no reply was received within 24 hours. The use of a high-profile institutional figure, legal threats and a strict response deadline are clear indicators of Social Engineering.

 # July 2025

The "vote for the dancer" WhatsApp scam

In February 2026, a phishing campaign spread through WhatsApp became known as the "vote for the dancer" scam. The message appeared to come from a contact already in the address book and invited the recipient to click a link to support a child in a supposed dance contest. The link led to a web page asking for the phone number and an OTP code received by SMS. Providing this information allowed attackers to take over the victim's WhatsApp account. Once inside, they sent messages to contacts pretending to be in an emergency and asking for urgent money transfers, while the legitimate account owner could no longer warn friends and family. The case relied on trust between known contacts and emotional involvement.

 # February 2026

MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

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