MUR

CYBER
SAPERE

Cyber Security Brochure

Responsible Use of Online Platforms

The hidden risks of digital services

Summary

What you will find in this brochure

Introduction

Online platforms are now an integral part of everyday life. They allow us to organize trips, book medical appointments and access a wide range of services quickly and continuously, making many operations simpler and accessible to everyone.

This convenience, however, is part of an increasingly complex digital context, where the use of platforms and the management of personal data require growing attention.

Cyberattacks, in particular, tend to intensify during periods of higher online traffic, such as holidays, long weekends and summer periods, when more bookings, searches for deals and transactions expose users to a higher risk of fraud.

Phishing URLs detected July-October 2025

522

Peak number detected in July, followed by 195 in August and 75 in both September and October.

The invisible path of digital scams

1. **Fake trusted contact:** The attacker may contact the victim by email, SMS or platforms, spreading malicious links while pretending to be a trusted source.

2. **Emotional manipulation:** The cybercriminal pushes the user into impulsive decisions by exploiting urgency, fear or the promise of a supposed benefit.

3. **Malicious action:** The victim, deceived, performs the requested action, leading to loss of money, data or access.

4. **Compromise:** The data or access obtained can be used for further fraudulent purposes, extending the impact to other services or users.

Source: CLUSIT Report - Operational Summary, second half 2025

What are the risks?

Risks

01 *Loss of control over digital identity*

If one of your accounts on online platforms, such as social networks or travel booking services, is compromised, an attacker could use stolen credentials to access other platforms and digital services, taking control of your digital identity and acting in your name without consent.

02 *Financial fraud risk*

Compromise of payment data associated with your accounts can result in unauthorized charges and direct economic losses. The risk increases if payment instruments are linked to your main account: unauthorized access could drain the available funds, with far more serious consequences.

03 *Reputational risk and loss of trust*

A compromised account can seriously damage your personal and professional reputation. Messages, operations or content published by whoever has taken control of your profile will be attributed to you, undermining the trust of colleagues, clients and contacts.

Countermeasures

Use different passwords for each account to limit the impact of compromise and prevent loss of control over a single service from becoming unauthorized access to others.

Use a dedicated prepaid card for online purchases, separate from your main account, and top it up only with the amount required for each transaction to limit losses in case of fraud.

Promptly inform your contacts so they can watch for fraudulent communications linked to your digital identity and prevent further scam attempts.

How to protect yourself?

Protected payments

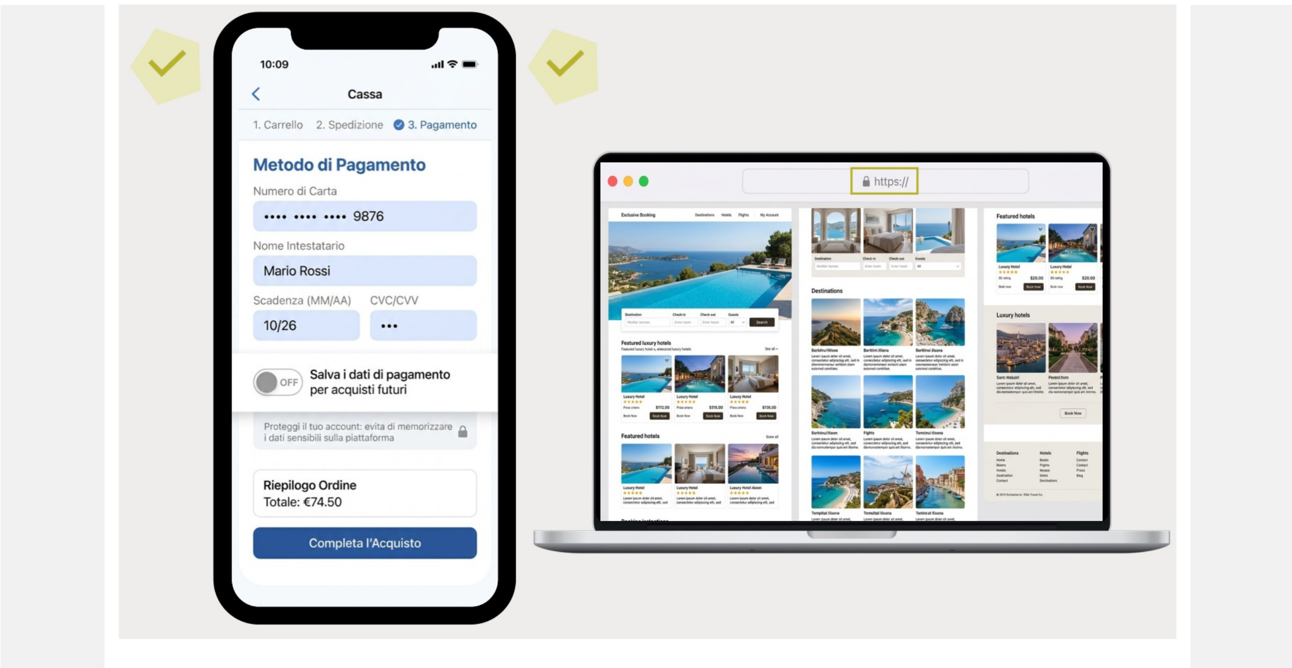
When using e-commerce services, avoid saving payment data on the platform. Storing payment information can increase the risk that it will be exposed or used fraudulently if the account or the platform is compromised.

Source verification

After making a booking, pay close attention to the communications you receive. Cybercriminals can send messages that imitate official platforms to request additional payments or obtain personal data. Carefully verify the authenticity of the source before providing information.

Security protocol

Before making a booking or subscribing to a service, make sure the site is official, reliable and secure. Check for the https:// protocol and avoid using unknown platforms.



Security Trend

The ghost three-room apartment scam in Jesolo

In August 2025, more than forty tourists were scammed after booking online a supposed three-room apartment in the center of Jesolo. The listing was well designed, with attractive photos, and offered a modern apartment at an unusually convenient price for the mid-August period. The fake owner replied in a friendly and convincing way, explaining that the accommodation was in high demand and that an immediate deposit was needed to reserve it, to be paid by bank transfer or prepaid card and therefore outside any official platform. After payment, she disappeared and stopped replying. When the tourists arrived at the address, they discovered that the apartment did not exist: the building did not offer tourist rentals and the listing had been created specifically to deceive.

 # August 2025

Booking: when a reservation becomes a scam

In April 2026, a digital scam involving a well-known travel booking platform occurred. Cybercriminals launched a phishing campaign against accommodation facilities registered on the platform, sending fake emails to steal hotel access credentials. Once inside the systems, the attackers obtained real booking data and used it to contact customers directly through the official messaging system. They told victims there were payment problems and invited them to enter credit card data through a link. Many users trusted the communication, entered their banking information and suffered financial fraud.

 # April 2026

Ministero dell'Università e della Ricerca

CYBER
SAPERE

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