MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Cyber Security Brochure

L'uso consapevole delle piattaforme online

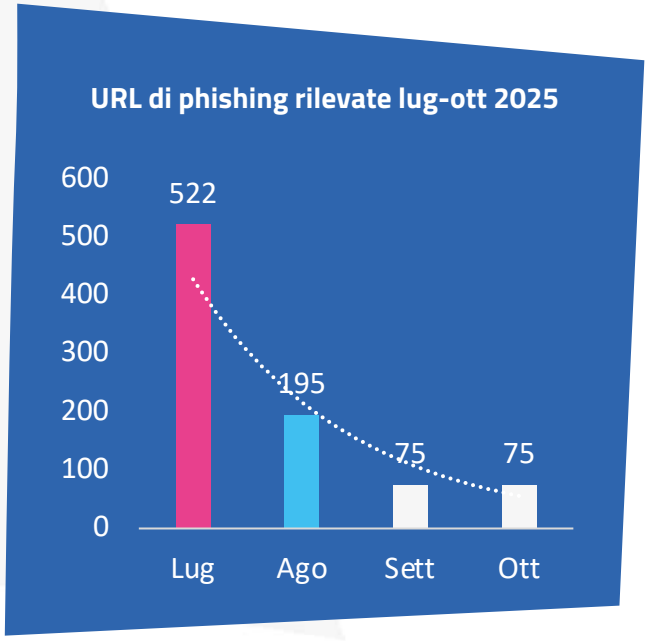
I rischi nascosti dei servizi digitali

Sommario

Cosa troverai in questa brochure

Introduzione

Le **piattaforme online** sono ormai parte integrante della **vita quotidiana**: permettono di organizzare viaggi, prenotare visite mediche e **accedere** a un'ampia gamma di **servizi in modo rapido e continuo**, rendendo molte operazioni più semplici e alla portata di tutti.
Questa comodità si inserisce però in un **contesto digitale sempre più complesso**, dove l'uso delle piattaforme e la **gestione** dei **dati personali** richiedono un'**attenzione crescente**.
Gli attacchi informatici, in particolare, tendono a **intensificarsi** nei momenti di **maggiore traffico online**, ad esempio sotto le festività, nei ponti e nei periodi estivi, quando l'aumento delle prenotazioni, la ricerca di offerte e la moltiplicazione delle transazioni espongono gli utenti a un **rischio più elevato di frodi**.



Il percorso invisibile delle truffe digitali:

Finto contatto affidabile
Il malintenzionato può contattare la vittima tramite e-mail, SMS o piattaforme, diffondendo link malevoli e spacciandosi per una fonte affidabile.

Manipolazione emotiva
Il criminale informatico induce l'utente a prendere decisioni impulsive sfruttando l'urgenza, la paura o la promessa di un presunto vantaggio.

Azione malevola
La vittima, indotta in errore, esegue l'azione richiesta, con conseguente perdita di denaro, dati o accessi.

Compromissione
I dati o gli accessi ottenuti possono essere utilizzati per ulteriori finalità fraudolente, estendendo l'impatto anche ad altri servizi o utenti.

Fonte: Rapporto Clusit - *Operational Summary II semestre - 2025*

Quali sono i rischi?

Rischi

01 Perdita di controllo dell'identità digitale

Nel caso in cui uno dei tuoi **account su piattaforme online** (ad esempio social network, servizi di prenotazione di viaggi, etc.) venga compromesso, un attaccante potrebbe utilizzare le credenziali sottratte per accedere ad altre piattaforme e servizi digitali, assumendo il **controllo** della tua **identità digitale** e operando a tuo nome senza il tuo consenso.

02 Rischio frode finanziaria

La **compromissione dei dati di pagamento** associati ai tuoi account può tradursi in **addebiti non autorizzati** e perdite economiche dirette. Il rischio si amplifica se i tuoi **strumenti di pagamento** sono **collegati al conto principale**: in questo caso, un accesso non autorizzato può prosciugare l'intera disponibilità finanziaria, con **conseguenze ben più gravi sul patrimonio.**

03 Rischio reputazionale e perdita di fiducia

Un **account compromesso** può danneggiare seriamente la tua reputazione, sia personale che professionale. Messaggi, operazioni o contenuti pubblicati da chi ha preso il controllo del tuo profilo ti verranno attribuiti, rischiando di **minare la fiducia di colleghi, clienti e contatti**.

Contromisure

Utilizza **password diverse** per ciascun account, in modo da limitare l'impatto di eventuali compromissioni e impedire che la perdita di controllo su un singolo servizio si traduca nell'accesso non autorizzato anche su altri.

Utilizza una **carta prepagata** dedicata gli **acquisti online** distinta dal conto principale, e ricaricala solo con l'importo della singola transazione per limitare il rischio di perdite economiche in caso di frodi.

Informa tempestivamente i tuoi **contatti** così da metterli in guardia da eventuali comunicazioni fraudolente riconducibili alla tua identità digitale e **prevenire** la **prosecuzione** di **tentativi** di **frode**.

Come difendersi?

Pagamenti protetti

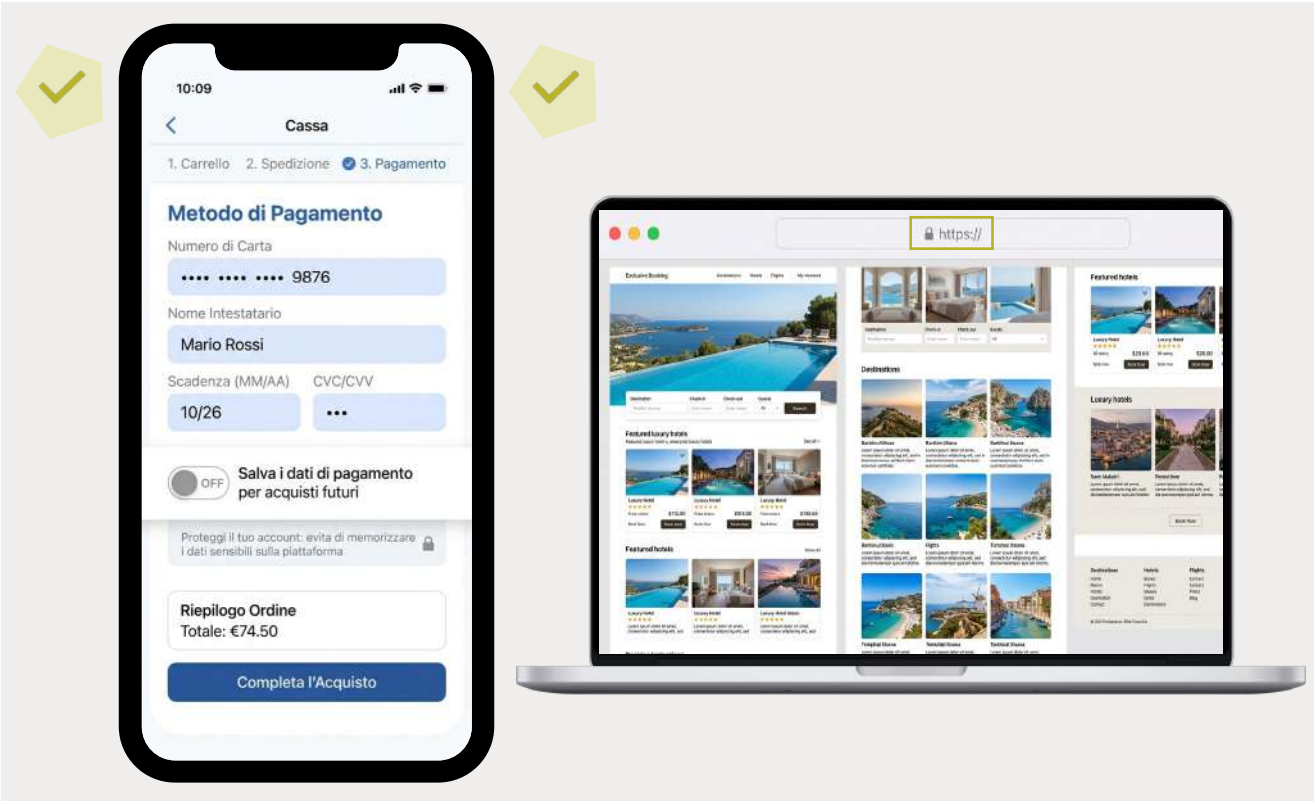
In caso di utilizzo di servizi di e-commerce, **evita di salvare** i **dati di pagamento** sulla piattaforma di utilizzo. La memorizzazione delle informazioni di pagamento può infatti aumentare il rischio che queste vengano esposte o utilizzate in modo fraudolento in caso di compromissione dell'account o della piattaforma stessa.

Verifica della fonte

Dopo aver effettuato una prenotazione, presta attenzione alle comunicazioni che ricevi. I criminali informatici possono infatti inviare messaggi che imitano quelli delle piattaforme ufficiali con l'obiettivo di richiedere pagamenti aggiuntivi o ottenere dati personali. **Verifica** con attenzione **l'autenticità** della **fonte** prima di fornire informazioni.

Protocollo di sicurezza

Prima di procedere con una prenotazione o di sottoscrivere abbonamenti, è importante accertarsi che il sito utilizzato sia **ufficiale, affidabile e sicuro.** Controlla la presenza del **protocollo https://** evitando l'utilizzo di piattaforme sconosciute.



Security Trend

Truffa del trilocale fantasma a Jesolo

Nell'agosto 2025 oltre quaranta turisti sono stati truffati dopo aver prenotato online un presunto trilocale nel centro di Jesolo.
L'annuncio, molto curato e con foto accattivanti, proponeva un appartamento mo-derno a un prezzo insolitamente conveniente per il periodo di ferragosto.
La finta proprietaria rispondeva in modo cordiale e convincente, spiegando che l'alloggio era molto richiesto e che per bloccarlo serviva una **caparra immediata**, da versare tramite bonifico o carta ricaricabile, quindi **fuori da qualsiasi piattaforma ufficiale**.
Dopo il pagamento, però, la donna spariva e smetteva di rispondere. Quando i turisti arrivavano all'indirizzo indicato, scoprivano che **l'appartamento non esisteva**: il palazzo non offriva affitti turistici e l'annuncio era stato creato ad hoc per ingannare.

Agosto 2025

Booking: quando la prenotazione diventa una truffa

Nell'aprile 2026 si è verificato un caso di **truffa digitale** legata ad una nota **piattaforma di prenotazione viaggi**. I cybercriminali hanno avviato una **campagna** di **phishing colpendo** le **strutture ricettive** registrate sulla piattaforma, inviando e-mail false per rubare le credenziali di accesso degli hotel. Una volta entrati nei sistemi, gli hacker hanno ottenuto i **dati reali** delle **prenotazioni** e li hanno usati per **contattare direttamente** i **clienti** tramite la messaggistica ufficiale. I truffatori, contattando le potenziali vittime, segnalavano loro dei problemi afferenti al pagamento dell'alloggio, invitandoli ad **inserire** i **dati della carta di credito** attraverso un link riportato in allegato all'e-mail. Molti utenti, fidandosi della comunicazione, hanno inserito le proprie informazioni bancarie, subendo frodi finanziarie.

Aprile 2026

MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Restate sintonizzati:

nuovi approfondimenti sulla cybersecurity vi aspettano nelle prossime pubblicazioni.