MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Cyber Security Brochure

Connessioni in Sicurezza

Il potere delle reti Wi-Fi



Sommario

Cosa troverai in questa brochure

01 *Introduzione*
Reti Wi-Fi: opportunità e rischi da conoscere

02 *Quali sono i rischi?*
Riconoscerli e adottare misure di difesa

03 *Come difendersi?*
Comportamenti consapevoli per una navigazione protetta

04 *Security trend*
Casi di attacchi reali

Introduzione

Le **reti Wi-Fi** costituiscono uno dei principali strumenti di **accesso a Internet** e svolgono un ruolo fondamentale nel favorire un **utilizzo più flessibile delle tecnologie digitali**, permettendo agli **utenti di accedere alla rete in qualsiasi momento e da luoghi diversi**.

Proprio per questo, le connessioni wireless sono diventate una **componente essenziale** della vita quotidiana e delle moderne modalità di lavoro.

Tuttavia, non tutte le reti Wi-Fi garantiscono lo stesso livello di **protezione**. Configurazioni inadeguate, utilizzo di reti pubbliche o comportamenti poco prudenti possono esporre utenti e dispositivi a rischi per la sicurezza, tra cui l'**intercettazione delle comunicazioni**, **il furto di dati** e **gli accessi non autorizzati**.

Conoscere le principali minacce e adottare alcune semplici precauzioni consente di utilizzare le reti Wi-Fi in modo più sicuro, contribuendo a **proteggere dati, dispositivi e identità digitali.**

+72,46%

Nel 2025, il **72,46% delle compromissioni rilevate** è stato riconducibile a una minaccia che ha coinvolto dispositivi connessi a Internet, come smart TV, tablet e dispositivi IoT. Questi dispositivi infetti, se connessi alla rete **Wi-Fi principale, possono diventare un punto debole per la sicurezza dell'intera rete domestica.**

Le fasi di un attacco tramite una rete Wi-Fi non legittima:

Configurazione della rete fraudolenta:
L'attaccante configura un punto di accesso Wi-Fi, in un luogo affollato, che imita una rete legittima (anche detta «evil twin»).

Connessione dell'utente:
L'utente si collega alla rete pensando che sia quella ufficiale disponibile nel luogo pubblico.

Intercettazione del traffico:
Le informazioni trasmesse dal dispositivo, connesso alla rete fraudolenta, transitano attraverso sistemi controllati dall'attaccante.

Raccolta delle informazioni:
Credenziali, dati di navigazione o altre informazioni sensibili possono essere intercettati o sottratti.

Fonte: CISA – America's Cyber D efense Agency – National Coordinator for Critical Infrastructure Security and Resilience; Rapporto Clusit - Operational Summary - 2026

Quali sono i rischi?

Rischi

01 Crittografia Wi-Fi obsoleta

Le connessioni Wi-Fi possono prevedere livelli di protezione differenti. Le reti configurate con protocolli di sicurezza **obsoleti** presentano maggiori **vulnerabilità** e sono particolarmente esposte agli attacchi informatici. Un malintenzionato potrebbe sfruttare tali criticità per **intercettare le comunicazioni**, **accedere alla rete** o **compromettere la sicurezza dei dispositivi connessi**.

02 Connessione automatica a reti non verificate

Molti dispositivi **memorizzano** le reti utilizzate in passato e possono **riconnettersi automaticamente** senza richiedere l'intervento dell'utente. Questo comportamento può favorire il collegamento a reti **non verificate**, aumentando il rischio di esporre dati aziendali e informazioni personali a soggetti non autorizzati.

03 Dispositivi visibili sulla rete

Quando si utilizza una **rete condivisa**, alcuni servizi attivi sul dispositivo possono renderlo rilevabile da altri utenti presenti sulla stessa infrastruttura. Questa esposizione può facilitare **tentativi di accesso indesiderati**, **raccolta di informazioni sul dispositivo** o **sfruttamento di servizi di condivisione** lasciati attivi involontariamente.

Contromisure

Utilizza reti Wi-Fi **protette** e **aggiornate**, gli standard di sicurezza più recenti rendono più difficile l'accesso non autorizzato e proteggono i dati trasmessi sulla rete.

Disattiva la **connessione automatica** alle reti non necessarie e **verifica** periodicamente l'elenco delle reti Wi-Fi salvate sul dispositivo.

Disabilita la condivisione di file e risorse quando non necessaria e **limita la visibilità del dispositivo** verso altri utenti della rete.

Come difendersi?

Presta attenzione alla rete Wi-Fi a cui ti connetti

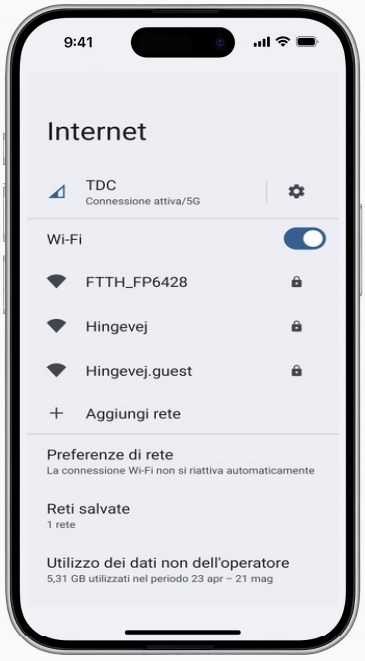
Prima di collegarti a una rete Wi-Fi pubblica, **verifica** che si tratti della **rete ufficiale** messa a disposizione dalla struttura e, in caso di dubbi, rivolgiti al personale. Reti Wi-Fi fraudolente possono essere create con nomi simili a quelli delle reti legittime, inducendo gli utenti a connettersi e aumentando il rischio di intercettazione di dati e credenziali.

Non inserire informazioni sensibili

Quando utilizzi una rete Wi-Fi aperta o condivisa, **evita** di effettuare operazioni che richiedono l'inserimento di **informazioni riservate**, come l'accesso a servizi bancari, pagamenti online o consultazione di dati sensibili. Quando possibile, utilizza sempre la rete dati del tuo dispositivo mobile.

Utilizza protocolli di sicurezza

Utilizza siti e servizi che presentano il **protocollo HTTPS**, il quale garantisce la connessione criptata. Quando disponibile, l'utilizzo di una **VPN** aggiunge un ulteriore livello di protezione alle comunicazioni effettuate attraverso reti Wi-Fi pubbliche.



Security Trend

Attacco Evil Twin negli aeroporti australiani

Nel **2024**, le autorità australiane hanno individuato una **campagna finalizzata al furto di dati**, che ha coinvolto viaggiatori in aeroporti e su voli nazionali. L'attacco è stato scoperto dopo che il personale di una compagnia aerea ha individuato una **rete Wi-Fi sospetta** durante un volo domestico in Australia.

L'attaccante utilizzava un dispositivo portatile in grado di creare falsi hotspot Wi-Fi con nomi identici o molto simili a quelli delle reti ufficiali presenti negli aeroporti e a bordo degli aeromobili.

Una volta stabilita la connessione, gli utenti venivano **reindirizzati** verso pagine di accesso false che **imitavano** quelle ufficiali della rete Wi-Fi.

Le credenziali inserite venivano memorizzate dall'attaccante, che successivamente accedeva ad account email, profili social e altri servizi online.

Le successive indagini hanno portato all'**arresto** e alla **condanna** dell'autore nel 2025. L'episodio ha evidenziato come la semplice connessione a una rete apparentemente affidabile possa rappresentare un rischio per la sicurezza delle informazioni.

gennaio 2024

Compromissione di reti Wi-Fi nel settore alberghiero

Nel **corso del 2026** è stato identificato un **attacco cyber** che ha preso di mira le **infrastrutture Wi-Fi** e i **portali di accesso** utilizzati da **hotel** e **strutture ricettive** frequentate da professionisti in viaggio.

Gli attaccanti non hanno compromesso direttamente i dispositivi delle vittime, ma i sistemi che gestivano l'accesso alle reti wireless degli ospiti.

Una volta ottenuto il controllo di tali infrastrutture, i cybercriminali hanno **modificato le configurazioni di rete** per manipolare il traffico Internet degli utenti collegati. In questo modo, durante il tentativo di accesso a servizi aziendali e piattaforme di produttività online, le vittime venivano reindirizzate verso **pagine di autenticazione fraudolente** progettate per imitare quelle legittime. Le credenziali e i token di autenticazione inseriti dagli utenti venivano così acquisiti dagli attaccanti, consentendo potenzialmente l'accesso non autorizzato ad account di posta elettronica, documenti aziendali e altri servizi professionali.

maggio – luglio 2026

MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Restate sintonizzati:

nuovi approfondimenti sulla cybersecurity vi aspettano nelle prossime pubblicazioni.