WLAN

A casa, al lavoro o in uno spazio pubblico, grazie ai dispositivi mobili oggi è possibile essere online praticamente ovunque e in qualsiasi momento. Per farlo spesso si usa una WLAN.

Proteggetevi così:

- Utilizzate reti WLAN sconosciute solo in misura limitata o, se possibile, evitatele del tutto.
- Non eseguite nessuna operazione di e-banking tramite reti WLAN pubbliche e non inviate in generale nessun dato riservato quando siete connessi a una rete di questo tipo.
- Se possibile, collegatevi soltanto a WLAN cifrate.
- Per il vostro punto d'accesso utilizzate un metodo di crittografia moderno (WPA) con una password sicura.

Funzionamento

Grazie all'uso della tecnologia radio, le WLAN sono un modo estremamente flessibile e comodo per connettersi a una rete e a Internet da un dispositivo mobile. Il tutto senza doversi preoccupare di cavi fastidiosi. Per i dispositivi mobili, come i tablet, spesso è tra l'altro l'unica possibilità per collegarsi a una rete. Anche negli smartphone questa modalità di connessione spesso è attivata per impostazione predefinita.

L'uso e la gestione di queste reti radio, tuttavia, portano con sé anche certi rischi di cui molte persone non sono consapevoli.

Come usare le WLAN in modo sicuro

Abbiate una «sana» dose di sfiducia quando utilizzate una WLAN che non conoscete.

Se possibile, collegatevi soltanto a WLAN cifrate (WPA2 o WPA3).

Non eseguite nessuna operazione di e-banking e non inviate dati riservati tramite reti mobili pubbliche, come gli «hotspot» nei locali pubblici (città, stazioni ecc.) oppure negli hotel.

Utilizzate la crittografia end-to-end per i dati riservati, a prescindere dalla tecnologia di trasmissione scelta.

Disattivate sul vostro dispositivo mobile, se possibile, la funzione di «connessione automatica» per le WLAN sconosciute e non protette.

Come gestire le WLAN in modo sicuro

Attivate un'opzione di crittografia robusta, almeno WPA, o meglio ancora WPA2 o WPA3, e impostate assolutamente una chiave di rete o password sicura.

Modificate l'SSID della rete, se contiene dati relativi a una persona, come il cognome, o informazioni sul router, p. es. il tipo.

Sostituite le password del router impostate in fabbrica con password personali e sicure.

Attivate il filtro MAC.

Se possibile, riducete la potenza di trasmissione del vostro router WLAN e spegnetelo quando la rete mobile locale non viene utilizzata.

Adottate precauzioni simili anche quando attivate un hotspot privato sullo smartphone, così da evitare abusi della vostra connessione mobile a Internet.

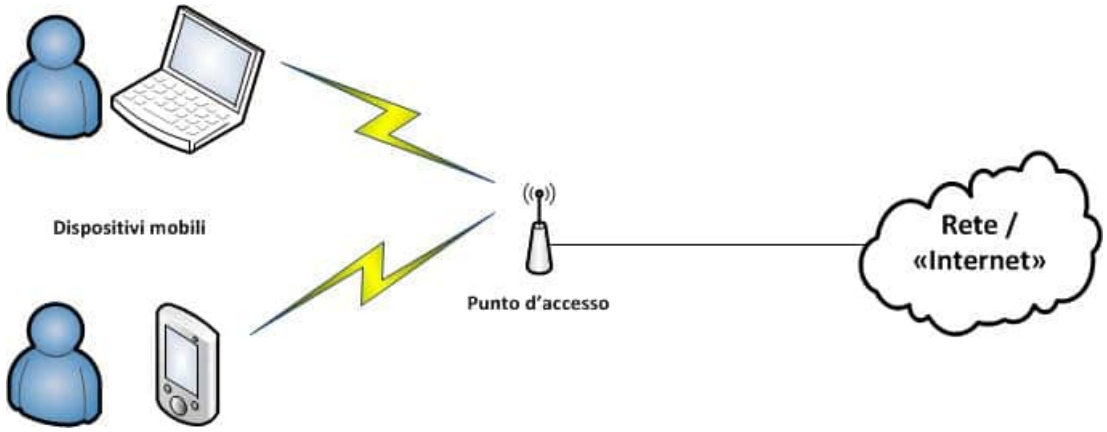
WLAN significa Wireless Local Area Network, in italiano «rete locale senza fili». La comunicazione wireless è estremamente flessibile, comoda e quindi molto diffusa al giorno d'oggi.

L'uso e la gestione delle WLAN, tuttavia, portano con sé anche certi rischi. Con i provvedimenti giusti potete aumentare notevolmente la vostra sicurezza.

Maggiori informazioni

Struttura di una WLAN

L'elemento centrale di una WLAN è rappresentato dal punto d'accesso, che costituisce il collegamento tra l'interfaccia aerea dei terminali mobili da un lato e la rete cablata e Internet dall'altro. Il punto d'accesso «crea» la rete WLAN trasmettendo segnali radio in tutte le direzioni attraverso la sua antenna.



Perché i dispositivi possano «vedere» la WLAN, solitamente il punto d'accesso invia un identificativo di rete, il cosiddetto SSID (Service Set Identifier o «identificatore del set di servizi»). In questo modo l'utente può riconoscere le WLAN disponibili in un determinato luogo e scegliere la connessione desiderata.

Crittografia

L'uso di una trasmissione radio ha uno svantaggio: è relativamente semplice intercettare i dati trasmessi. In sostanza, a tutti i dispositivi che si trovano nel raggio di copertura di una WLAN viene inviato l'intero traffico dati. Per questo motivo la connessione tra i dispositivi mobili e il punto d'accesso andrebbe cifrata. Ciò non impedisce che le comunicazioni vengano ricevute, ma per lo meno nessuno può farci niente.

Esistono diverse procedure che si possono seguire per crittografare le trasmissioni.

- **WEP**
  Il Wired Equivalent Privacy è stato il primo protocollo di crittografia utilizzato come standard nelle WLAN. Ora però viene considerato non sicuro ed è relativamente facile da forzare. Quindi è consigliabile non utilizzarlo più.
- **WPA**
  Il WiFi Protected Access è l'evoluzione del protocollo WEP. Meccanismi di protezione migliorati garantiscono una sicurezza maggiore. Per esempio, è stata migliorata la procedura di autenticazione dei membri della rete ed è stata introdotta una chiave dinamica per la trasmissione.
- **WPA2**
  Il WPA2 si basa sul WPA ma utilizza il forte algoritmo AES per cifrare i dati trasmessi.
- **WPA3**
  WPA3 è il più recente standard di crittografia per le reti wireless. Rispetto al WPA2 complica in misura sostanziale soprattutto gli attacchi alla password usata per la crittografia.

Ogni volta che sia possibile, per le reti WLAN è consigliabile ormai utilizzare soltanto il protocollo WPA2 e dove disponibile il WPA3. La Preshared Key o «chiave precondivisa», che in un certo senso è la password per acce-

dere alla rete, deve essere impostata con un grado di sicurezza adeguato. Dovrebbe contenere almeno 16 caratteri e avere le caratteristiche di una password sicura (https://www.ebas.ch/it/4-proteggere-gli-accessi-online/) .

A questo riguardo va osservato anche che viene protetto solo il passaggio dal dispositivo al punto d'accesso: dal punto d'accesso in poi, i dati viaggiano nuovamente senza protezione. I contenuti riservati andrebbero quindi crittografati end-to-end indipendentemente dalla tecnologia di trasmissione impiegata, p. es. con crittografia TLS/SSL (https, icona a forma di lucchetto) quando si naviga in Internet o si accede all'e-banking.

Filtro MAC

Tutti i dispositivi di rete, e quindi anche tutti i dispositivi mobili, possiedono un indirizzo MAC che permette di identificarli in modo univoco. I punti d'accesso offrono la possibilità di impostare un filtro MAC. In questo modo possono accedere alla rete soltanto i dispositivi mobili registrati con un indirizzo MAC conosciuto.

Tuttavia gli indirizzi MAC dei dispositivi non sono a prova di contraffazione. Con gli strumenti giusti, infatti, è possibile «dissimulare» un indirizzo MAC autorizzato ed eludere il filtro. Ciò nonostante, per porre comunque un ulteriore ostacolo per un potenziale intruso, è una funzione che è consigliabile attivare.