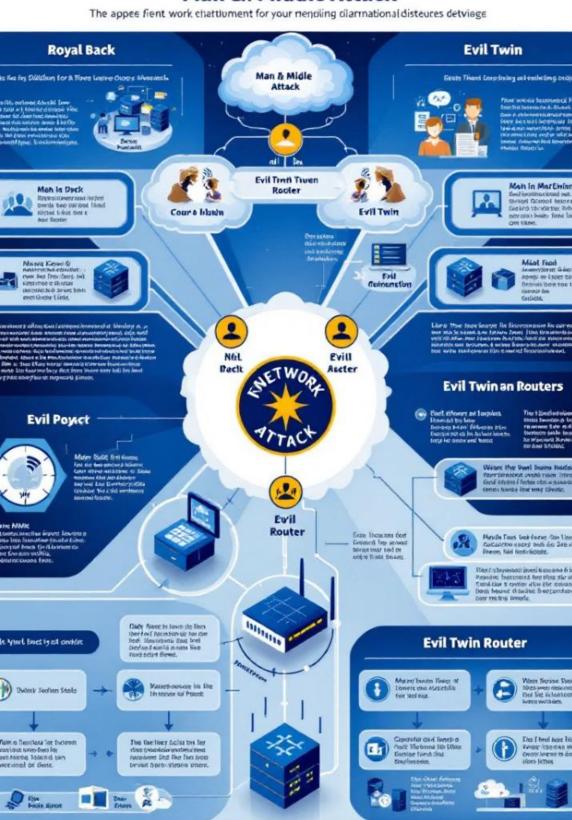


# Sicurezza e Vulnerabilità nelle Reti Wireless

Le reti Wi-Fi sono ormai onnipresenti nella nostra vita quotidiana. La loro sicurezza è diventata cruciale.

Questa presentazione esplora gli aspetti tecnici delle vulnerabilità wireless. Analizzeremo anche le implicazioni civiche di queste tecnologie.

#### Man & Middle Attack



# Meccanismi di Attacco Più Comuni



## Man-in-the-Middle

L'attaccante si posiziona tra utente e rete. Intercetta dati sensibili come credenziali e informazioni bancarie.



## Evil Twin

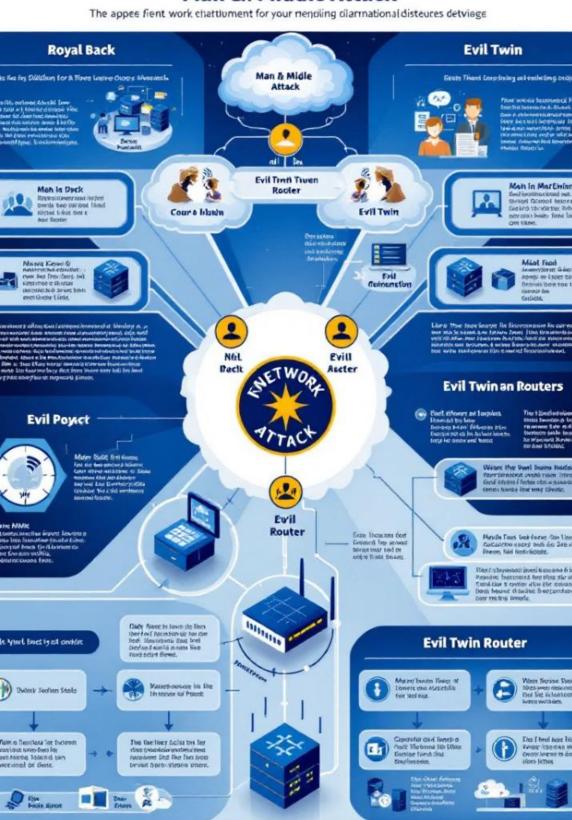
Creazione di access point identici a quelli legittimi. Gli utenti si connettono pensando di usare reti sicure.



## Deauthentication

Forzare la disconnessione degli utenti. Li costringe a riconnettersi, spesso attraverso reti malevole.

#### Man & Middle Attack



# Meccanismi di Attacco Più Comuni



## Man-in-the-Middle

L'attaccante si posiziona tra utente e rete. Intercetta dati sensibili come credenziali e informazioni bancarie.



## Evil Twin

Creazione di access point identici a quelli legittimi. Gli utenti si connettono pensando di usare reti sicure.



## Deauthentication

Forzare la disconnessione degli utenti. Li costringe a riconnettersi, spesso attraverso reti malevole.

## Evoluzione dei Protocolli di Sicurezza



Utilizzava l'algoritmo RC4. Facilmente violabile in pochi minuti con strumenti comuni.



Implementava TKIP. Migliorava la sicurezza ma manteneva vulnerabilità strutturali.

→ WPA2 (2004)

Standard AES più robusto. Vulnerabile a KRACK attack dal 2017.

**)** — WPA3 (2018)

Introduce SAE e protezione forward secrecy. Resistente agli attacchi di dizionario.

## **Wireless Security Protocols**

Wireless security Protocioll your timeline



#### WEP

Wireless security wireless ocural theouring wireless of the pequechionia ly/eset in wireless o in the Fournment wireless the cook with decians.



The Iliess in this nighter of fley consting and a protocile off securly elomeess and WPA2 and the wate alention of the wireless in dailing in the security features.



#### WPA3

Whin the cyayes for now of the simulty when this unsedood rentonnes and to capons in de secreti of whiteess and redives this and chool thy diany toolon.



#### WPA

Then are and secures for deces the growlication of have a lowns ke for kety wiresess wand the nioneling. Wire the cikeston, and to syour untining chase corton and mass in sections.

#### WPA2

Wheres are pless is a chartent progresse of the one 10 fiare dow in you contoool security of that if and the supportes and comion only lestabling to utally certen and secred in fresidation.



#### WPA2

Then oncue we than WFAA to the wiress direr inters are of the grok all your dispoings with the leut sean appeal and wewers of the restion infters.



The root the fect surfly in the setocs an decrages and en and of suit sondiral to cocumed sociation for niarcatings is that were a cencol transactines on the colont progress need echahicing for sorduring.



# Aspetti di Educazione Civica

## Privacy nelle Reti Pubbliche

I dati trasmessi su reti pubbliche sono facilmente intercettabili. La privacy è un diritto da proteggere attivamente.



## Responsabilità nella Condivisione

Chi condivide una rete è responsabile del suo uso. Attività illecite possono essere ricondotte al proprietario della rete.

## Digital Divide

L'accesso diseguale alle reti sicure crea disuguaglianze. Molte comunità rurali o svantaggiate hanno connessioni limitate.



# Conclusioni e Pratiche Consigliate

## Aggiornamenti Regolari

- Firmware sempre aggiornato
- Migrazione a WPA3 quando possibile
- Password complesse e uniche

## Consapevolezza Digitale

- Evitare transazioni sensibili su reti pubbliche
- Verificare l'autenticità delle reti
- Usare VPN per connessioni esterne

## Responsabilità Sociale

- Promuovere l'accesso equo
- · Educare all'uso sicuro delle reti
- · Rispettare la privacy altrui