Come proteggere la rete wireless

Le reti WiFi rappresentano, in molti casi, l'anello debole della propria rete casalinga (LAN, Local Area Network). Ecco alcuni consigli su come proteggerla dagli attacchi esterni

La navigazione wireless non è mai troppo sicura. Abbiamo già parlato dei rischi cui si va incontro se si decide di utilizzare **una rete WiFi pubblica** ma pericoli analoghi possono verificarsi anche in casa. Un **hacker** potrebbe entrare nel computer e impadronirsene semplicemente intercettando e "bucando" la **rete WiFi** utilizzata per l'accesso e la navigazione Internet. Esistono, tuttavia, accorgimenti che possono rendere la connessione senza fili più sicura, anche se non totalmente invulnerabile agli attacchi.

Per **proteggere la rete WiFi** è necessario, come primo passo, entrare nel proprio router e accedere alla pagina delle *Impostazioni*. Dopo aver selezionato la barra degli indirizzi del browser, inserire nell'indirizzo IP la stringa **192.168.1.1**. La maggior parte dei **modem router wireless** in commercio utilizza di default questo IP, tuttavia nel caso in cui non dovesse funzionare si può utilizzare la stringa **192.168.0.1**. Se queste alternative non dovessero andar bene, è necessario recuperare il manuale di istruzioni del proprio dispositivo e verificare qual è l'indirizzo IP utile per accedere direttamente al proprio router.

Una volta entrati nelle impostazioni del **router WiFi**, ecco alcuni semplici consigli su **come proteggere** la **rete wireless** dagli attacchi **hacker**.

Cambiare le credenziali di accesso al modem router wireless

La maggior parte dei router in commercio permette di accedere alle impostazioni solamente dopo aver inserito le credenziali di accesso. Solitamente, appena usciti di fabbrica, i dati per il login sono impostati su **admin** (amministratore) per il nome utente e **password** come parola chiave; altra possibile combinazione è quella composta dalla coppia **admin/admin**. Per un hacker il compito è sin troppo semplice. È il motivo per cui è buona norma cambiare questi dati alla prima connessione, così da rendere inaccessibile (o quasi) il dispositivo ai malintenzionati.

Impostare una chiave di sicurezza per la rete wireless

I modem router più moderni sono protetti da una chiave di sicurezza basata sul protocollo **WPA2** (*Wi-Fi Protected Access 2*), attualmente considerato il più sicuro e il meno vulnerabile ad attacchi hacker. Modelli più vecchi potrebbero

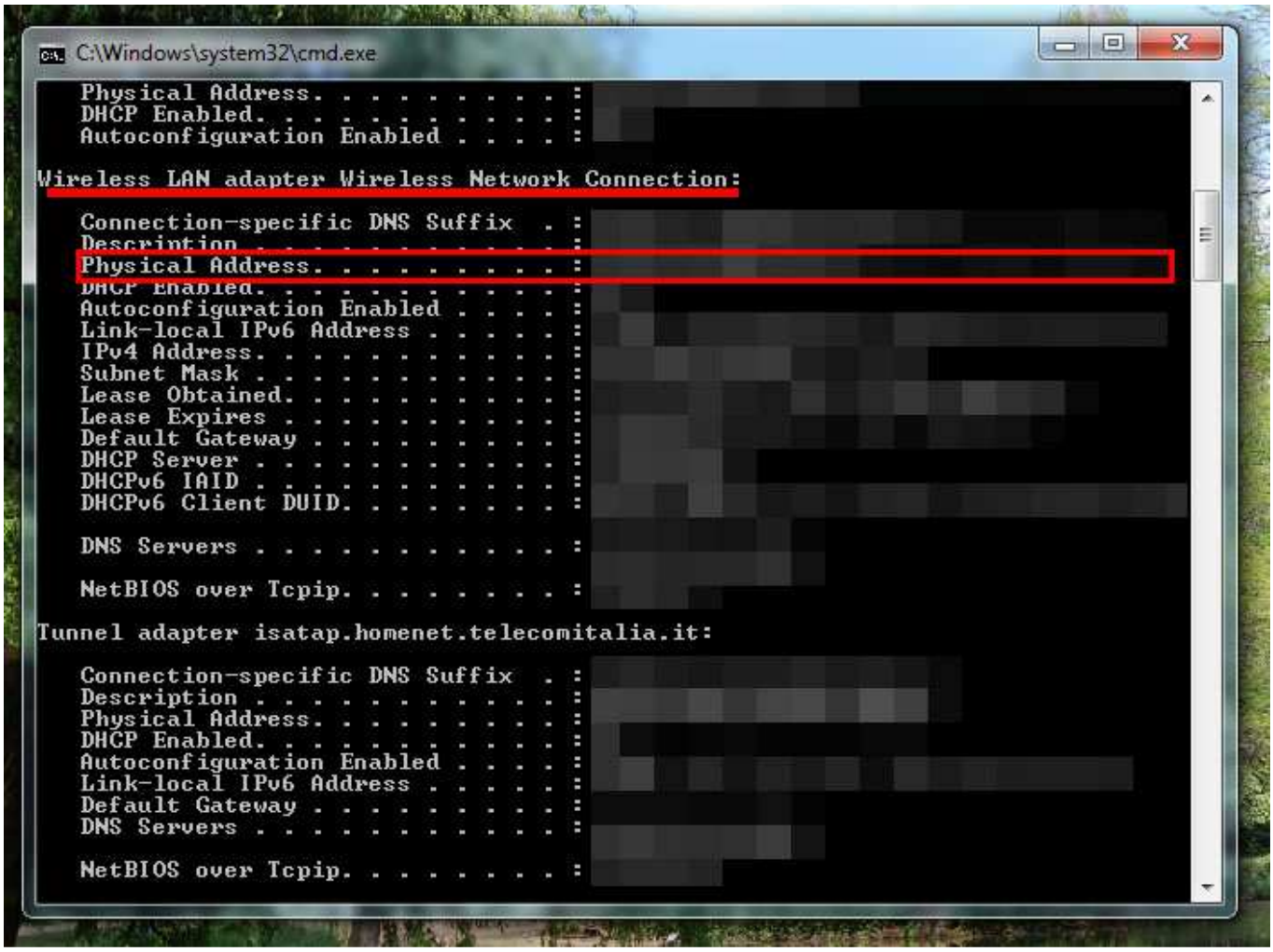
essere protetti da chiavi d'accesso generate secondo i dettami dei protocolli **WPA** e **WEP** (*Wired Equivalent Privacy*), tuttavia, queste ultime hanno mostrato di avere più di qualche pecca in fatto di sicurezza informatica. Altri modelli, addirittura, non hanno alcuna chiave di sicurezza e permettono a chiunque di connettersi. Niente di più pericoloso. Per proteggere la rete WiFi sarà quindi necessario impostare una password. Gli standard WPA2 impongono che la parola chiave scelta sia composta da **almeno 24 caratteri alfanumerici** (sia lettere sia numeri). Per impostarla o modificarla, è necessario entrare nella scheda delle impostazioni wireless e individuare il pulsante **Configura Rete WiFi** (o una dicitura simile). Una volta dentro, il pannello di amministrazione dovrebbe consentire di attivare la protezione, di scegliere il protocollo di sicurezza e impostare una nuova password o modificare quella esistente.

Cambiare nome alla rete wireless

Ogni rete WiFi è identificata da un nome (**SSID**, *Service Set IDentifier*), solitamente univoco. Anche se la sua conoscenza non ha implicazioni sul livello di sicurezza, un nome non modificato è indice di una rete con scarsa amministrazione e, quindi, con protezioni basse. In un caso del genere è altamente probabile, ad esempio, che le credenziali di accesso siano state lasciate intatte (quelle di fabbrica di cui sopra) costituendo una preda perfetta per ogni **hacker**.

Configurare un filtro wireless MAC

Ogni scheda di rete (e di conseguenza ogni dispositivo che ne è dotato) è identificata da un **indirizzo MAC** (*MAC address*, *Media Access Control*). Si tratta di un codice di 48 bit, assegnato in modo univoco dal produttore, che difficilmente può essere modificato a livello software. In teoria, quindi, ogni dispositivo in rete può essere riconosciuto in base a questo indirizzo. Tramite questa informazione si può stabilire che l'**accesso alla rete wireless** sia consentito soltanto ad alcuni dispositivi (computer, laptop, smartphone, tablet, stampanti, NAS, hard disk di rete, ecc.) di cui conosciamo il MAC address, escludendone tutti gli altri (e quindi anche il device del nostro ipotetico hacker). Qual è l'indirizzo MAC del computer? In sistemi Windows, per scoprire qual è il MAC address è necessario aprire il prompt dei comandi digitando la stringa **cmd** nel menu di Start oppure seguendo il percorso **Start/Tutti i programmi/Accessori/Esegui**. Nella finestra, inserire la stringa **ipconfig/all** e premere invio. Nella lista che comparirà, cercare la voce relativa alla scheda di rete (wireless o ethernet) del computer (o del dispositivo che vi interessa) e, alla riga corrispondente a **Indirizzo Fisico,** troverete il vostro MAC address.



Per attivare il filtro wireless MAC, si deve entrare nella scheda delle impostazioni wireless, cercare la scheda relativa al **MAC filtering** o **Filtro MAC** e attivare l'opzione. Nel caso in cui non si riesca a trovarlo, si può provare a consultare il manuale di istruzioni che accompagna il router wireless.
Come detto, il filtro MAC identifica univocamente il dispositivo a cui è assegnato: è, quindi, una sorta di impronta digitale del computer, dello smartphone o della stampante di rete che si ha in casa. Attivando un filtro MAC solo per alcuni dispositivi a conosciuti, si rende inaccessibile la rete WiFi ad altri dispositivi sconosciuti e pertanto non autorizzati. Proseguendo nel parallelo con le impronte digitali, è come se si montasse uno scanner di impronte digitali alla porta di casa autorizzando l'ingresso solo ad alcune persone conosciute, lasciando fuori casa tutti gli altri. In sintesi, è l'impronta digitale a fare fede, così come l'indirizzo MAC per i dispositivi digitali.

Assegnare indirizzi IP statici ai dispositivi

Un'altra porta di accesso alla rete wireless è rappresentata dal **DHCP** (*Dynamic Host Configuration Protocol*), il protocollo che si occupa di assegnare in maniera automatica indirizzi IP a ogni dispositivo connesso alla rete wifi privata.
Nel caso in cui il router che gestisce la rete casalinga abbia il DHCP attivato, ogni nuovo dispositivo che si connette alla nostra rete (smartphone, laptop,

computer, stampante di rete, NAS) otterrà in maniera automatica un indirizzo IP nel range di indirizzi privati. In questo modo, diverrà uno dei nodi che compongono la rete e, teoricamente, potrebbe funzionare da portone di ingresso verso gli altri nodi o devices. Nel caso in cui il protocollo DHCP sia disattivato, invece, l'amministratore della rete dovrà assegnare manualmente un indirizzo IP a ogni nodo o dispositivo collegato della rete stessa. Questo significa che ogni altro nuovo device che dovesse collegarsi in un secondo momento (ad esempio quello del nostro solito hacker ipotetico), non avendo ottenuto un indirizzo IP apposito dall'amministratore, sarà effettivamente tagliato fuori dalla rete stessa e quindi da ogni possibilità di interagire con essa.
In questo modo, si può evitare che qualche dispositivo possa connettersi alla rete senza autorizzazione e, soprattutto, si è in grado di non rendere pubblici i propri dispositivi connessi alla rete locale. Grazie all'IP masquerading, infatti, l'indirizzo privato di ogni nodo/device collegato alla nostra rete casalinga verrà "velato" dietro l'indirizzo pubblico del router stesso e sarà pertanto virtualmente irrintracciabile da qualsiasi malintenzionato posto al suo esterno.