ESTILS

Els experts alerten que el wifi públic pot ser fàcilment clonat i, per tant, s'hi poden interceptar les comunicacions. GETTY

Vigila! En un wifi públic poden parar l'orella

Els experts recomanen navegar per pàgines segures i encriptar informació

NEREIDA CARRILLO
BARCELONA

La temptació de tenir internet de manera gratuïta ha fet que ens connectem al wifi que bars, biblioteques, centres comercials i altres llocs proporcionen. La pregunta és: és segur? ¿Els usuaris naveguem amb prudència? ¿Sabem com protegir-nos?

El grup Telecos.cat, el col·lectiu que agrupa els enginyers de telecomunicacions de Catalunya, ha advertit dels perills d'aquestes xarxes compartides. A l'informe *Societat i telecos 2015* atribuïa els riscos d'aquests espais a "la baixa seguretat de les xarxes en si mateixes", però també al desconeixement, la imprudència i "la mala fe d'alguns individus". Un estudi d'Intel Security també posa xifres a la imprudència: un 67% dels enquestats fan servir wifi públic sense contrasenya en els seus viatges a l'estranger, i un 17% hi naveguen com si ho fessin des de casa. L'estudi certificava que sobretot els joves d'entre 18 i 24 anys són els més imprudents.

Jordi Iparraguirre, enginyer informàtic i membre del capítol català de la Internet Society, explica: "El wifi públic pot ser fàcilment clonat o replicat i les comunicacions es poden interceptar". Genís Margarit, enginyer en telecomunicacions i professor de la Universitat Pompeu Fabra, alerta que l'atac a un wifi públic no és sofisticat. "Els espais sense fils són un medi compartit. Qualsevol que hi estigui enganxat pot escoltar-te", comenta Margarit, que afegeix que aquests riscos existeixen tant si el wifi té contrasenya com si no.

En l'argot de la seguretat informàtica es coneixen com a *man in the middle* molts d'aquests atacs amb el wifi. "El *man in the middle* –explica Iparraguirre– és algú que, sense que tu ho sàpigues, es posa entremig de tu i el lloc on et connectaràs. Tot el que tu estàs enviant i rebent passa per aquesta persona". Margarit i Iparraguirre diuen que de vegades els atacs es fan amb eines d'auditoria que es fan servir per analitzar xarxes; el problema són els usuaris que utilitzen aquestes eines per perjudicar els altres.

Perills
A les xarxes públiques les comunicacions es poden interceptar fàcilment

No compris ni piulis

Suplantar la teva identitat a Facebook, començar fer piulades al teu compte de Twitter o robar-te les contrasenyes del compte bancari són alguns dels contratemps amb què els usuaris es poden trobar si es connecten en un wifi compartit, sense saber-ho, amb delinqüents. "El més aconsellable seria no connectar-se enlloc que demanés un usuari i una contrasenya", recomana Iparraguirre. Consultar la previsió del temps o comprovar els horaris d'un museu formen part d'una navegació innòcua, però quan ens connectem a llocs dels quals ens poden robar dades personals, el perill augmenta.

Margarit també defensa una navegació cautelosa i recomana que es valori sempre abans la confiança que ens inspira el negoci que ens està proporcionant la connexió a internet i la gent amb qui s'estigui compartint el wifi. "El que hauríem d'intentar és que totes les aplicacions que utilitzem quedin encriptades", adverteix.

VPNs i altres proteccions

Margarit aconsella que es facin servir sempre les pàgines *https*, amb certificat de seguretat. Molts navegadors ja permeten que els configurem de manera que, per defecte, es connectin a aquestes pàgines. Un altre mètode que els experts encoratgen a fer servir si ens connectem en un espai públic és una VPN (Virtual Private Network), un instrument que xifra la comunicació entre el nostre dispositiu i la sortida de la VPN. "Tant els telèfons mòbils com les tauletes i els ordinadors estan preparats per fer servir VPNs sense gaires complicacions –diu Iparraguirre–. Només és qüestió de buscar un proveïdor que ens inspiri confiança.

Margarit aconsella també el sistema d'autentificació en dos passos: per poder iniciar sessió en un lloc no habitual, quan poses el teu usuari i contrasenya, se't demana un codi enviat al mòbil. Per a Iparraguirre, per contra, l'autentificació en dos passos no és infal·lible. Explica que hi ha casos de robatori de dades i suplantació d'identitat.

Els experts conclouen que no es tracta ara de deixar d'utilitzar un wifi públic, sinó de ser conscients dels riscos i navegar-hi de manera més cautelosa.