ESTILS

Guia pràctica contra els perills de la xarxa

Recollim els consells més bàsics que cal tenir en compte per afrontar els nous riscos que suposa l'ús massiu d'internet i les xarxes socials

NEREIDA CARRILLO
BARCELONA

¿És segur guardar les diferents contrasenyes que tenim en un únic arxiu al nostre ordinador? ¿Estem protegits si no actualitzem l'antivirus dels aparells electrònics? ¿Resulta assenyat compartir fotografies d'allà on som a les xarxes socials? ¿Baixem aplicacions de mòbil abans d'escrutar-ne l'autor i d'on provenen i valorar si són prou fiables?

Algunes d'aquestes preguntes apareixen al test en línia que la Comissió Europea ha penjat a la xarxa perquè els internautes comprovin ells mateixos els seus coneixements sobre seguretat digital. La iniciativa s'emmarca en el Mes Europeu de la Ciberseguretat, que es va celebrar a l'octubre i va dur a terme més de 240 activitats en 32 països.

"La tecnologia canvia d'una setmana per l'altra i s'ha d'estar al cas", assegura Jordi Iparraguirre, enginyer informàtic i membre del capítol català de la Internet Society. Aquest professional adverteix que cal educar en seguretat digital perquè ningú és aliè als nous perills que van associats a la tecnologia. Per conscienciar la població sobre aquests riscos i ajudar a combatre'ls se celebren a Catalunya diferents tallers i cursos, com ara els que impulsa el Col·legi Oficial d'Enginyeria Informàtica de Catalunya (COEINF) o la Crypto Party, que recorre diferents ciutats del país amb tallers gratuïts per a tot tipus de públics. A l'ARA hem volgut recopilar alguns consells en una guia pràctica per combatre els nous perills de la xarxa.

No revelar ubicacions

Les fotos donen molta informació de les nostres rutines

Els usuaris de Foursquare revelen amb freqüència on són a cada moment, mentre que en xarxes socials com Instagram o Facebook resulten habituals les fotografies de les vacances o les excursions, que, si bé permeten presumir davant dels amics i coneguts, també poden alertar els malfactors de qui no és a casa. Són efectes indesitjats del que alguns anomenen *postureig digital*. Els experts alerten de la imprudència d'aquests comportaments a les xarxes socials. "Fent una anàlisi de dades és molt fàcil extreure'n qui som, on vivim, les nostres rutines i si som a casa o no", explica Helena Rifà, directora del màster de seguretat de les TIC a la UOC.

Per evitar riscos, Rifà aconsella penjar fotos en diferit, és a dir, quan hem tornat d'aquell lloc; donar una localització aproximada en comptes de fer *check in* allà on som, i no permetre ser etiquetats a Facebook per altres persones sense donar el nostre permís previ.

La directora del màster de seguretat de les TIC explica que hi ha diverses iniciatives que intenten conscienciar els internautes d'aquests perills. El 2010 es va posar en marxa la web Pleaserobme.com, i més recentment una agència ha creat per a una empresa de seguretat un compte d'Instagram anomenat Instacacos, on uns suposats lladres es burlaven, aquest estiu, d'aquells que pengen les fotos de les vacances a la popular xarxa de fotografies. "El perill és generalitzable a qualsevol xarxa social", explica Rifà. "Podem tenir seguidors a qui no coneixem que estan veient les nostres dades", afegeix aquesta professora, que lamenta que, a internet, no som prou conscients d'aquests riscos i transmetem amb massa naturalitat informacions que mai no diríem per altres canals i d'una altra manera.

Vigilar amb el wifi

Garantir la seguretat de la xarxa al domicili

L'enginyer en telecomunicacions i professor de la Universitat Pompeu Fabra Genís Margarit vol alertar de problemes i comportaments perniciosos a les xarxes sense fils de llars particulars. "Com a pèrit, m'he començat a trobar gent que es veu involucrada en actes delictius perquè els pirategen el wifi de casa. Tothom que té wifi hauria de garantir que és prou segur", afirma Margarit.

Per això aquest professional recomana comprovar que el protocol que es fa servir és segur i aconsella, especialment en el cas d'algunes companyies, no posar-li el mateix nom i contrasenya que ve per defecte amb el *router* sinó configurar-ho d'una manera més segura amb l'ajuda d'un expert. Això es deu al fet que ja existeixen maneres per esbrinar aquestes contrasenyes i usuaris amb mala fe i alguns coneixements poden intentar piratejar aquestes xarxes.


GETTY

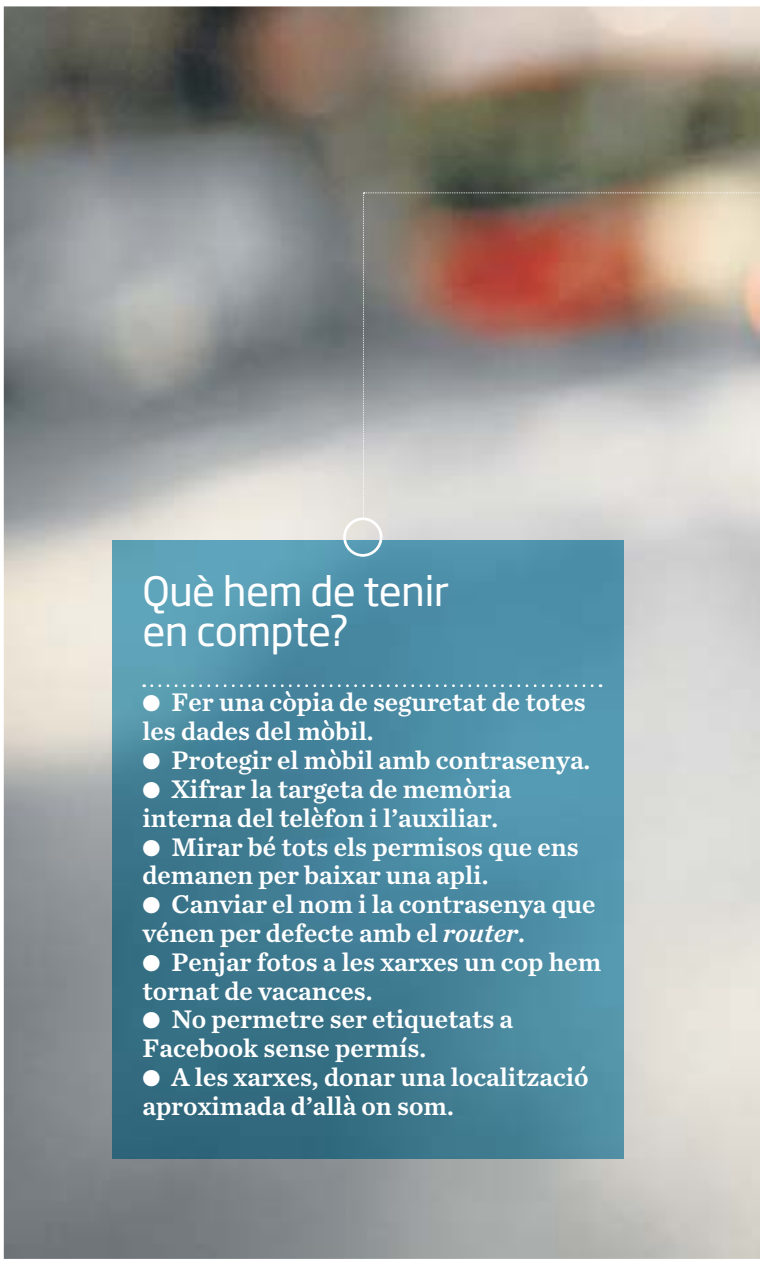
Prevenir
Els experts diuen que cal educar en seguretat digital perquè afecta tothom

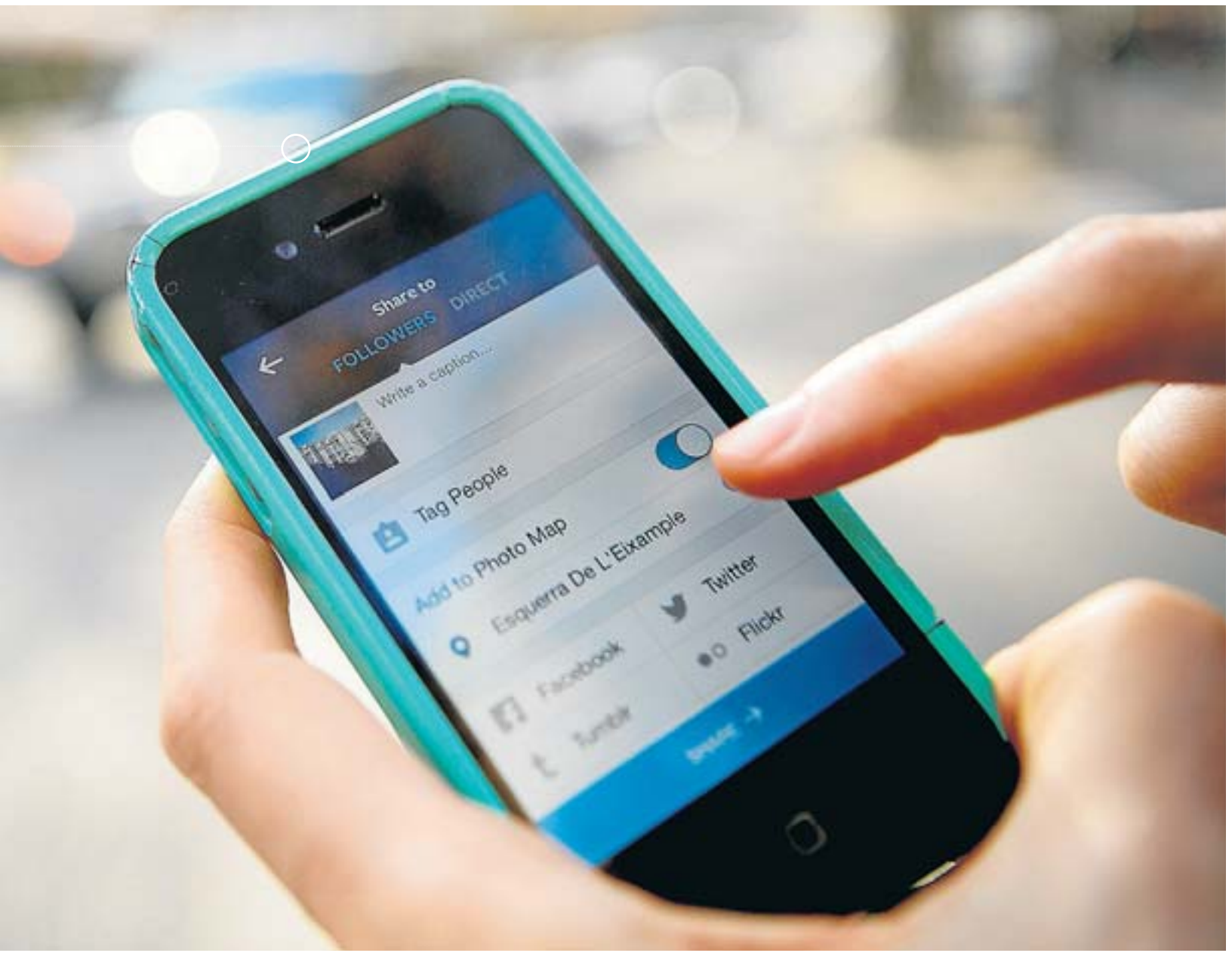
I si ens roben el telèfon?

Fer còpies de seguretat de totes les dades importants

Una distracció al metro o al restaurant, on ens podem deixar el telèfon mòbil damunt la taula mentre anem al lavabo, pot ser fatal. Els usuaris s'adonen de la importància de tota la informació que emmagatzemen a l'*smartphone* quan el perden o els hi roben. Els experts donen alguns consells per minimitzar el dany quan passa això, una sèrie passos que cal seguir tant preventivament com a posteriori.

Iparraguirre recomana "tenir còpia de seguretat de totes les dades del mòbil que ens interessen: els contactes, les fotografies, els enllaços a webs, etc., i idealment haver comprovat que aquesta còpia és útil". Tant Iparraguirre com Rifà expli-





quen que també pot frenar els lladres, almenys en un primer moment, el fet de protegir la pantalla del telèfon o tauleta amb una contrasenya de xifres o de les de seguir un patró amb el dit. "Això no evitarà que algú amb més coneixements pugui arribar a les dades", puntualitza Rifà.

A més d'aquestes dues prevencions, Iparraguirre afegeix un tercer comportament prudent: "Si no ve per defecte, cal xifrar tant la targeta de memòria auxiliar que puguem posar com la memòria interna del telèfon". Rifà creu que només s'ha de guardar al telèfon informació no xifrada si no és sensible. Si ho hem de fer, diu, almenys que n'hi hagi com menys millor. Finalment, cal tenir apuntat el número IMEI, una xifra que es proporciona al client a l'hora d'adquirir l'aparell i a la qual

Es recomana no oferir ubicacions exactes a les xarxes socials.
PERE TORDERA

sovint no es fa gaire cas però que resulta molt útil en situacions de robatori o de pèrdua del telèfon. És un codi que identifica l'aparell i que permet que l'operadora el bloquegi si l'usuari ho demana.

A més de bloquejar l'aparell, Iparraguirre també aconsella "canviar les contrasenyes" de tots els llocs on s'entrava mitjançant el telèfon. I si es pot, fer-ho tan aviat com sigui possible per impedir que el lladre pugui entrar a les xarxes socials o al correu i suplantar la identitat de l'usuari. En aquest sentit, Rifà adverteix que no és sensat estar identificat per defecte a Facebook, Twitter i altres aplicacions dels telèfons mòbils. Tot i això, és un comportament força habitual.

Riscos amb la connexió

Utilitzar el 3G del mòbil per evitar intromissions

Els riscos que comporta connectar-se a una xarxa sense fils pública –com ara que ens pirategin els comptes de les xarxes socials o que accedeixin a informació personal– desapareixen, en gran mesura, si fem servir el 3G del mòbil. Això implica, però, esgotar més ràpid la tarifa de dades, que molts usuaris volen allargar al màxim de temps possible. Tot i això, Iparraguirre assegura que els telèfons que solem portar a la butxaca tampoc estan exempts d'atacs. Explica que existeixen dispositius que poden desviar el trànsit dels mòbils per la seva antena telefònica; és a dir, si són més a prop del nostre mòbil que l'antena de la companyia telefònica, pot ser que el telèfon es connecti a aquesta mena de dispositius, amb més potència però menys segurs, que aprofiten per interceptar dades.

A més d'anar amb compte amb els problemes que pugui ocasionar la connectivitat, Iparraguirre també alerta d'altres riscos relacionats amb les aplis que els usuaris descarreguen als seus dispositius. "Quan et descarregues aplicacions, has de mirar quins permisos t'estan demanant i pensar si realment els necessiten o no", adverteix aquest enginyer informàtic. Iparraguirre subratlla que els usuaris es poden trobar amb aplicacions malignes que són gratuïtes i que serveixen per apropiar-se de dades dels propietaris d'aquests terminals. Per això, recomana no ser confiats i examinar detingudament les aplis abans de descarregar-les.