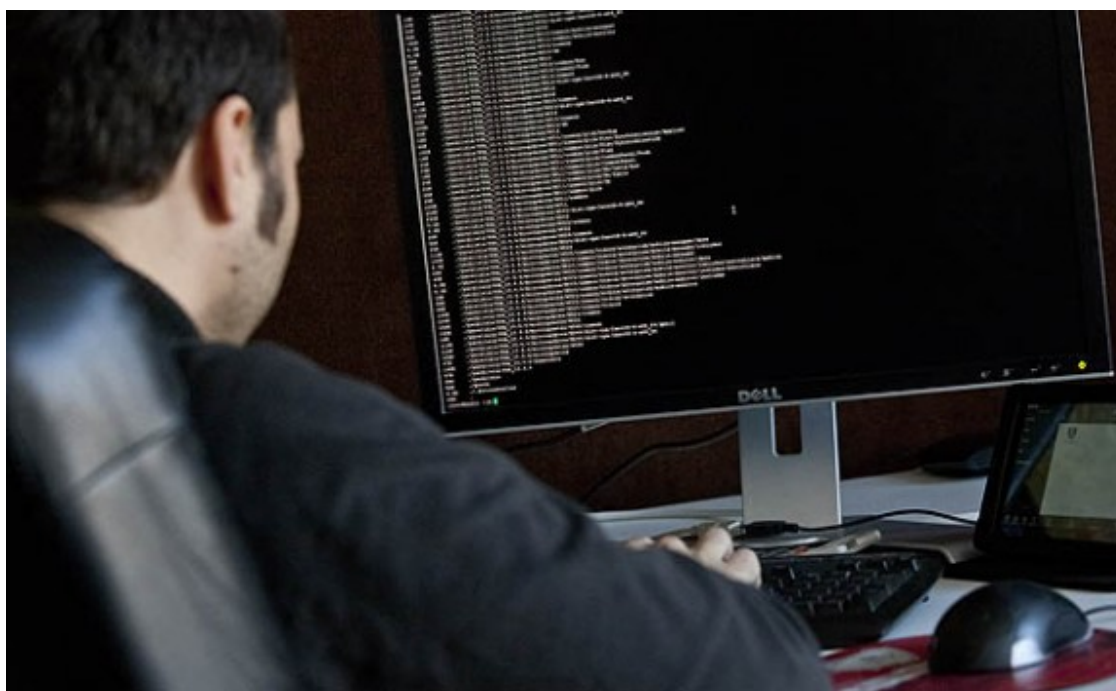


## ?Set coses que no pots fer a Internet (si vols navegar segur)

*Els experts en seguretat de "Kaspersky Lab" elaboren una llista de recomanacions de pràctiques habituals a evitar*



Set activitats que hem d'evitar a Internet | Adrià Costa

Els experts en seguretat de Kaspersky Lab (<http://www.kaspersky.es/>) han elaborat una llista de set recomanacions de pràctiques habituals a internet que s'han d'evitar per tenir una connexió segura. Són aquestes:

### 1. Confiar en els punts de wifi oberts

Els punts de wifi sense contrasenya o amb una contrasenya que tothom coneix, bars o biblioteques, són molt poc segures perquè els pirates informàtics poden utilitzar la connexió per robar-te les dades. Els experts recomanen que si les utilitzes que intentis evitar pàgines on et demanin les dades i que mai compris per internet connectat amb una xarxa tan poc segura.

### 2. Triar contrasenyes fàcils de recordar

Una contrasenya fàcil de recordar és també una contrasenya fàcil de robar o deduir. Evita referències òbvies a dies senyalats, com aniversaris, i combina majúscules, minúscules, números i senyals.

### 3. No repetir contrasenyes

No només les contrasenyes han de ser difícils, sinó que no es poden repetir, utilitzar la mateixa contrasenya per diferents comptes et fa vulnerable a un gran atac si aquesta és descoberta.

#### **4. Clicar els enllaços dels correus electrònics**

Clicant l'enllaç d'un correu electrònic és una de les maneres més fàcils de baixar-te un virus i ara que els pirates han après a crear correus que semblen corporatius o de bancs és molt important ser caut. Només clica enllaços de persones que hi tens molta confiança.

#### **5. Donar les dades d'accés dels teus comptes**

La millor manera d'evitar accidents i de mantenir un secret és no dir-ho, donar les teves dades d'accés a una altra persona t'exposes que aquesta per descuit o per malícia les distribueixi a terceres persones.

#### **6. Explicar per Internet que vas de vacances**

El típic post al Facebook d'una persona a l'aeroport, la foto d'una platja o el tuit amb el geolocalitzador activat són maneres molt ràpides d'informar els lladres que a casa teva no hi ha ningú, això és molt perillós en xarxes socials que faciliten la teva adreça o almenys la teva ciutat.

#### **7. Acceptar la privacitat per defecte de les xarxes socials**

Les opcions de privacitat de les xarxes socials canvien amb freqüència. Si no prens el temps i la paciència per desentranyar amb qui comparteixes què és molt fàcil que acabis revelant informació privada a una persona que no volies que sabés.