5 Consells bàsics sobre CIBERSEGURETAT

1 Contrasenyes segures

- Empra una **contrasenya única i segura (o frase de contrasenya)** per cada compte.
- Empra **lletres, nombres i caràcters especials**. Com **més llarga, més segura.**
- **Canvia la contrasenya** immediatament després d'una vulneració.
- **No reutilitzis contrasenyes.**
- Mai facis click a un enllaç de correu electrònic per restablir la contrasenya. Ves al lloc web del compte.
- **Evita iniciar sessió** a comptes **a través d'un wifi públic.**

Taula 1. *Temps que triga un software automàtic en esbrinar una contrasenya.*

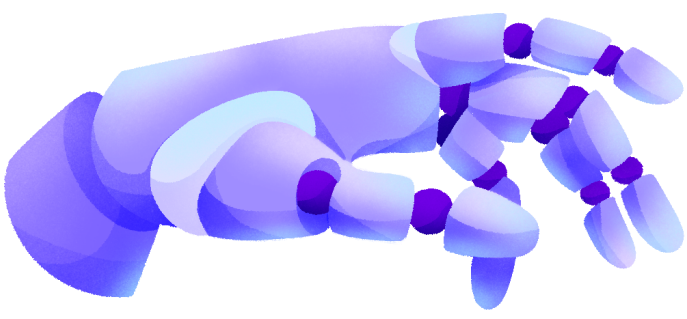
Longitud	Combinació de tot tipus de caràcters	Només minúscules
3 caràcters	0,86 segons	0,02 segons
4 caràcters	1,36 minuts	0,46 segons
5 caràcters	2,15 hores	11,9 segons
6 caràcters	8,51 dies	5,15 minuts
7 caràcters	2,21 anys	2,23 hores
8 caràcters	2,10 segles	2,42 dies
9 caràcters	20 mil·lennis	2,07 mesos
10 caràcters	1899 mil·lennis	4,48 anys
11 caràcters	180365 mil·lennis	1,16 segles

2 Useu un administrador de contrasenyes (com Bitwarden)

- Són aplicacions que poden crear, emmagatzemar i gestionar contrasenyes per a vostè.
- Adoptar un administrador de contrasenyes segur significa que **només haurà de recordar una contrasenya molt forta i llarga, anomenada contrasenya principal** o mestra. Així evitam reutilitzar claus.
- **No s'ha d'utilitzar el navegador (chrome, safari...) per desar contrasenyes.**

3 Autentificació de doble factor (2FA)

- L'autentificació de doble factor proporciona una **segona línia important** més enllà de des claus **per protegir els comptes** d'accessos no autoritzats.
- Aquests serveis us **permeten rebre un codi temporal d'inici de sessió de dos factors** a través d'una aplicació mòbil o una notificació push (notificació d'inserció) al telèfon intel·ligent.
- **Algunes opcions populars i de confiança són Google Authenticator, Authy i Duo Mobile.**



Els ordinadors Mac i Linux i els dispositius Android i iOS no porten incorporat un programari contra el malware. **Podeu instal·lar una eina de confiança i d'ús gratuït com Bitdefender o Malwarebytes** (també a ordinadors Windows). No obstant, recorda que el codi maliciós canvia tan ràpid que confiar en qualsevol eina daquest tipus no pot ser la seva única defensa.

4 Protegiu-vos contra el phishing i el malware

- És important **emprar un antivirus** en temps real.
- Emprar **bloquejadors d'anuncis**. Alguns anuncis poden contenir codi maliciós i infectar l'ordinador amb malware si fem click a l'anunci.
- Seguretat de DNS. Utilitza el sistema de noms de domini. **Molts d'atacants empren noms de domini de llocs web similars per enganar a les víctimes.** Els firewalls de DNS poden ajudar a prevenir virus i atacs de phishing ja que comproven si la IP conté codi maliciós i de ser així es bloqueja l'accés.
- **Mai fer click a links enviats per correu electrònic, reds socials o aplicaciones de mensajería instantània.**

5 Reds wifi trampa

- Els ciberdelinqüents creen **reds wifi falses amb un nom igual o molt semblant al de l'original.** Normalment trien xarxes wifi públiques amb gran afluència. **Si accedim a aquesta wifi ens poden robar dades (si accedim al nostre compte bancari, reds socials o correu electrònic).**
- És important **no accedir mai als nostres comptes des de xarxes wifi públiques** i prestar especial atenció si veiem dues wifi amb el mateix nom o molt similar.