

CONSELLS DE CIBERSEGURETAT



- **Protegeix els teus dispositius.** Instal·la antivirus i actualitza'l periòdicament.
- **Contrasenyes d'accés segures.** Haurien de contenir de vuit a dotze caràcters (entre els quals caràcters majúscula, minúscula, números i símbols). Recordeu canviar-les cada tres mesos.
- **Realitzar còpies de seguretat.** Recordeu actualitzar les còpies de seguretat periòdicament.
- **Segmentació de perfils.** Delimitar l'accés a la informació en funció de les necessitats i tasques de cada empleat.
- **Governança en ciberseguretat.** Preveure un protocol d'actuació per donar resposta a possibles amenaces, i fer-lo extensiu a tots als treballadors.
- **Doble factor d'identificació.** A l'hora de realitzar accions compromeses cal utilitzar una doble verificació.
- **Utilitza una xarxa Wi-Fi coneguda.** La informació transmesa a través de les connexions públiques pot ser capturada.
- **Realitza connexions segures.** L'adreça web que comenci per HTTPS i mostri un cadenat de color verd a la barra d'adreces garanteix la navegació de forma segura.
- **Ofereix únicament les dades personals necessàries.** En cas que t'estranyi que per efectuar la compra et demanin alguna dada personal no la facilitis.
- **No clicar enllaços desconeguts.** No tenir pressa a l'hora de clicar enllaços. Cal agafar-nos el temps necessari per tal de fer les verificacions corresponents.
- **Alerta als Deepfakes o hipertrucatges.** Desconfieu de comunicacions fora del canal habitual que us facin realitzar accions no acordades prèviament a nivell d'empresa.

EN CAS D'HAVER ESTAT VÍCTIMA D'UN CIBERATAAC:

1. Comuniqueu-ho al gestor informàtic.
2. Recolliu tota la informació possible.
3. Denuncieu els fets a la policia.