

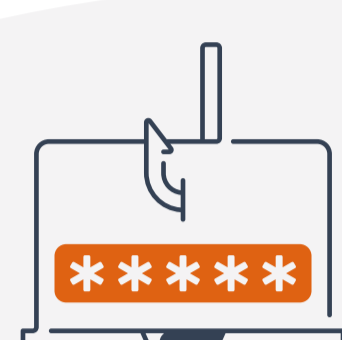
# Ciberseguretat: una missió compartida

## ENGINYERIA SOCIAL, L'ART DE L'ENGANY



L'enginyeria social consisteix en enganyar la víctima perquè revele, voluntàriament, informació sensible o faça accions que vulneren la seguretat de les dades i dispositius que maneja.

### Tipus de fraus en línia més habituals



Phishing



Smishing



Vishing



Sextortion



Baiting



Brushing



Dumpster diving



Shoulder surfing

### Sis consells per a identificar estos fraus:



- (1. Verificar sempre el remitent dels correus electrònics (Phishing).** Els atacants solen utilitzar direccions que s'assemblen molt a les reals, però amb xicotetes variacions.



- (2. Presta màxima atenció a les trucades de telèfon fraudulentes (Vishing) i els SMS enganyosos (Smishing)** que se servixen de la sensació d'urgència, curiositat o por per a manipular al destinatari i que este realitze una acció no desitjada.



- (3. Compartir contrasenyes mitjançant mètodes no xifrats suposa posar en risc els comptes, així com la informació que contenen.** Cap sector (banca, telefonia, sanitat...) demanarà les teues contrasenyes per telèfon, xat o similar.



- (4. Protegir les dades personals dels nostres ciutadans.** Manegem informació sensible, així que evita revelar informació personal de tercers davant peticions estranyes per telèfon o correu electrònic sense abans verificar la identitat del remitent.



- (5. La formació i conscienciació en ciberseguretat és fonamental perquè els usuaris estiguen prevenuts i sàpien com actuar davant possibles riscos cibernètics en l'àmbit laboral i personal, per això en les entitats públiques és necessari promoure estes accions per a garantir la seguretat de la informació de l'organització.**



- (6. Reportar qualsevol comportament anòmal al teu suport de Ciberseguretat o de Tecnologies de la Informació.**

