

# Fitxa Didàctica del Taller 01:

## Estafes Digitals per a Gent Gran

Aquest taller té com a finalitat **sensibilitzar i capacitar les persones grans** davant l'augment d'estafes digitals. Es treballa amb exemples reals, dinàmiques participatives i consells pràctics per prevenir frauds. El contingut està dissenyat perquè el formador no necessiti coneixements avançats: només ha de seguir el guió i fomentar la participació.

- **Reconèixer** les principals modalitats d'estafes digitals (missatges fraudulents, webs falses, suplantació d'identitat, estafes d'inversió).
- **Detectar** senyals d'alerta (urgència, petició de dades, promeses de guanys).
- **Aplicar** mesures preventives senzilles (verificar remitents, no compartir dades).
- **Actuar** correctament davant una sospita (guardar proves, denunciar, avisar).

### 1. Introducció (10 min)

- Presentació del problema: xifres d'estafes a Espanya i Catalunya.
- Impacte econòmic i social.

### 2. Tipus d'estafes (15 min)

- Explicació amb exemples visuals: SMS falsos, webs fraudulent, estafes romàntiques, inversions fictícies.
- Dinàmica: *"Algú ha rebut un missatge semblant?"*

### 3. Senyals d'alerta (10 min)

- Frases típiques: "Actua ara", "Envia'ns el DNI", "Guanya 1.000 € en 72 hores".
- Exercici: identificar què és sospitos en exemples reals.

### 4. Com actuar (15 min)

- Pautes concretes: verificar remitents, no compartir dades, desconfiar de presses.
- Mostrar diferències entre webs reals i falses.
- Passos: captura de pantalla, contactar entitat, denunciar (Mossos, OSI), avisar familiars.
- Recursos útils: telèfons i correus oficials.

### 5. Final i resolució de dubtes (5 min)

## **Introducció**

En el primer apartat es presentarà la magnitud del problema de les estafes digitals. Explicarem quantes estafes es produeixen cada dia a Espanya, quins canals són els més utilitzats pels estafadors i quines són les pèrdues econòmiques que això genera. L'objectiu és que els participants prenguin consciència que aquest és un risc real i molt freqüent, i que qualsevol persona pot ser víctima si no pren precaucions.

Primer de tot es realitzaran un seguit de preguntes inicials per fer una dinàmica de grup i fomentar la participació dels assistents.

### **Preguntes inicials:**

1. A Espanya es realitzen més de 1.000 estafes digitals al dia Cada dia es produeixen més d'un miler d'estafes digitals, la qual cosa demostra que és un problema molt estès i en creixement. Aquestes accions fraudulentas afecten persones de totes les edats i perfils, i utilitzen tècniques cada vegada més sofisticades.
2. La majoria d'estafes es fan per correu electrònic, SMS i missatges Els ciberdelinqüents prefereixen canals ràpids i econòmics com el correu electrònic, SMS o WhatsApp. Aquests mitjans permeten enviar milers de missatges amb un cost mínim i amb gran facilitat per enganyar, ja que imiten comunicacions oficials.
3. Cada dia es bloquegen més de 250.000 trucades fraudulentas Les trucades fraudulentas són una de les tècniques més habituals. Tot i els plans de seguretat, es detecten centenars de milers de trucades diàries que intenten enganyar la víctima fent-se passar per bancs, operadors o familiars.
4. Els ciutadans espanyols van perdre 7.500 milions d'euros en un any segons dades oficials, les pèrdues per estafes digitals superen els 7.500 milions d'euros anuals. Aquesta xifra és superior al pressupost d'educació d'un curs acadèmic, fet que evidencia la gravetat i l'impacte econòmic del problema.

## Estafes freqüents

En aquest apartat es parlarà de les estafes més habituals. Primer es veurà les estafes tradicionals, aquelles que existien abans de l'era digital i que encara continuen vigents. Aquestes són la base sobre la qual s'han adaptat les estafes digitals actuals.

### Estafes tradicionals:

- **Trucades per telèfon:** Persones que es fan passar per entitats oficials o familiars per obtenir diners o dades.
- **Caixers automàtics:** Manipulació de dispositius per robar targetes o codis PIN.
- **Estafes comercials i financeres:** Ofertes falses, productes inexistents o inversions fraudulent.
- **Estafa piramidal:** Esquema on els guanys dels primers participants provenen dels diners dels nous inversors.

Posteriorment es veurà com aquestes pràctiques han evolucionat cap al món digital.

### Estafes digitals:

Aquestes pràctiques són una evolució de les estafes tradicionals, però adaptades al món online. Els estafadors aprofiten la tecnologia per arribar a més persones, amb missatges més convincents i, cada vegada més, utilitzant intel·ligència artificial per fer-los més realistes i personalitzats."

- **Missatges fraudulents:** Arriben per SMS, correu electrònic o WhatsApp. Sovint simulen ser empreses conegudes, com Correus, bancs o serveis tècnics. Exemple: un missatge que diu que tens un paquet pendent i has de clicar un enllaç, o un fals tècnic de Microsoft que et demana instal·lar un programa per controlar el teu ordinador.
- **Pàgines web falses:** Imiten webs oficials per robar dades personals o bancàries. Poden semblar molt reals, amb logotips i dissenys copiats. (es mostrarà un exemple de com es pot fer una pàgina web falsa amb ia en segons).

Altres estafes habituals:

- **Esquema piramidal/Ponzi:** Prometen guanys ràpids, però els diners dels nous inversors es fan servir per pagar els primers participants.
- **Tarifes anticipades:** Et demanen pagar una quantitat per avançat per obtenir un préstec, premi o servei que mai arriba.
- **Estafes immobiliàries:** Ofertes falses de lloguer o venda d'immobles. Cobren un dipòsit i després desapareixen.
- **Falses ONG:** Històries emotives per demanar donacions, sovint per WhatsApp o trucades.

- **Estafes romàntiques:** Algú crea un perfil fals i estableix una relació sentimental per guanyar-se la confiança i demanar diners.
- **Suplantació telefònica:** Es fan passar per familiars (com un fill o net) que diu haver tingut un accident i necessita diners urgentment.

#### **Estafes d'inversió:**

També hi ha frauds relacionats amb inversions. Prometen guanys molt alts i ràpids en productes com criptomonedes o aplicacions que no estan regulades per la CNMV. Recordeu: si no està regulat, és molt probable que sigui una estafa."

#### **Recovery Room:**

Les anomenades 'Recovery Room'. Són falsos serveis que prometen recuperar els diners perduts en una estafa, però en realitat busquen cobrar-te més diners o obtenir informació personal.

## **Senyals d'alerta**

En aquest apartat es mostrarà com detectar les estafes digitals. Els estafadors utilitzen tècniques psicològiques per fer-nos actuar ràpidament i sense pensar. Mostrant els tres punts principals.

### **1. Sensació d'urgència**

Els missatges fraudulents intenten crear pressió perquè actuïs immediatament. Volen que no tinguis temps de reflexionar. Frases típiques són: «El teu compte serà bloquejat si no actues ara» o «Oferta vàlida només fins a les 23:59 d'avui». Si reps un missatge així, desconfia."

### **2. Petició de dades personals o descarregues**

"Un altre senyal és quan et demanen informació sensible: DNI, número de targeta, contrasenya o PIN. També poden demanar-te que descarreguis un fitxer o instal·lis un programa. Això és molt perillós perquè poden robar-te diners o suplantar la teva identitat."

### **3. Promeses de guanys ràpids o recompenses**

"Moltes estafes ofereixen diners fàcils, premis o descomptes irrealistes. Frases com «Guanya 1.000 € al dia sense experiència» o «Has estat seleccionat per un premi exclusiu». Si sona massa bé per ser cert, probablement és una estafa."

Fer un recordatori al final:

***si un missatge us genera pressa, us demana dades o promet diners fàcils, és molt probable que sigui un frau.***

## **Com actuar**

Es mostrarà com fer per evitar caure en una estafa i com actuar si sospitem que volen enganyar. Aquestes són les recomanacions bàsiques:

### **Com prevenir riscos:**

#### **1. Comprova sempre el remitent i l'enllaç:**

Si reps un correu o missatge, revisa si l'adreça és oficial i si la web comença per «https». Les webs falses sovint tenen noms estranys o lleugeres variacions."

#### **2. No comparteixis dades sensibles:**

Mai donis contrasenyes, codis, números de targeta o PIN. Les entitats oficials ja tenen les teves dades i no les demanaran per correu ni per missatge."

#### **3. Desconfia de les presses**

Si el missatge et fa sentir que has d'actuar ràpid, para i pensa. Truca al número oficial de l'empresa abans de fer res."

### **Que fer si sospites d'una estafa?**

#### **1. Guarda proves:**

Fes una captura de pantalla del missatge o correu. Si algú pregunta com fer-ho, explica que és tan fàcil com prémer el botó de captura al mòbil o al teclat.

#### **2. Contacta amb l'entitat oficial:**

Busca el telèfon o correu real de l'empresa (no el que surt al missatge) i pregunta si és legítim.

#### **3. Denuncia el cas:**

Truca al 112 (Mossos d'Esquadra) o contacta amb l'Oficina de Seguretat de l'Internauta. Si és una estafa financera, avisa la CNMV ([registro@cnmv.es](mailto:registro@cnmv.es) o 900 535 015).

#### **4. Avisa altres persones:**

Explica-ho a familiars o amics perquè no caiguin en el mateix engany.

Recorda finalment que:

**actuar ràpid és important, però sempre amb calma i pels canals oficials**

## **Final i resolució de dubtes**

L'últim apartat consistirà en aclarir qualsevol dubte sobre els continguts explicats: com identificar estafes, quins passos seguir per prevenir-les i què fer si ja han estat víctimes. El formador ha de fomentar la participació, escoltar amb atenció i donar respostes basades en els consells del taller, reforçant la idea que no hi ha preguntes incorrectes i que la seguretat digital és responsabilitat de tots