

Estafes amb Intel·ligència Artificial

Com la IA generativa està canviant la cara del fraudel



Conselleria de Salut
Direcció General de Prestacions,
Farmàcia i Consum

Per què parlem avui d'IA i estafes

El frau no és nou, però la IA generativa ha canviat tres coses alhora: l'escala, la credibilitat i el cost d'executar un engany.

EL CANVI DE FONTS

Abans feien falta temps, idiomes i coneixements tècnics. Avui n'hi ha prou amb una eina accessible i uns minuts per a produir un engany convincent.

Per això qualsevol perfil —jove o major, tècnic o no tècnic— està avui en el radar dels estafadors.

Com ha canviat el frau amb la IA

De mensajes mal escritos y obvios → a comunicaciones impecables, personalizadas y multilingües.

L'APARENÇA JA NO ÉS PROVA D'AUTENTICITAT

De fotos de perfil robades → a vídeos i veus sintètiques que reproduïxen rostres, gestos i accents reals.

Idea força: cal canviar la forma en què verifiquem el que veiem i sentim en una pantalla.

Tipologies principals

Quatre grups, una idea:
la IA aporta cara, veu,
text i plataforma.

Deepfakes en vídeo
Clonació de veu
Falsos assessors
Phishing amb IA

No són categories estanques;
un cas sol combinar vàries.



Tipologia 1 · Deepfakes de vídeo

Què és: vídeo manipulats o generats des de zero en el qual una persona apareix dient o fent alguna cosa que mai va dir o va fer.

USOS FRAUDULENTS HABITUALS

Falsos directius en videotelefonades demanant transferències urgents, famosos suplantats recomanant inversions, familiars en dificultats demanant diners.

Pista pràctica: demanar un gest inesperat en directe (girar el cap, tapar-se mitjana cara) continua dificultant la suplantació en vídeo.

Tipologia 2 · Clonació de veu

Què és: reproducció de la veu d'una persona real a partir d'uns pocs segons d'àudio públic —una entrevista, un vídeo en xarxes, un missatge breu

ESTAFES TÍPIQUES

«Estafa del fill» o del familiar per crida o nota de veu, i autoritzacions falses de transferències en entorns professionals.

Pista pràctica: acordar en família una paraula de seguretat i, davant qualsevol urgència econòmica per àudio, retornar l'anomenada al nombre real.

Tipologia 3 · Falsos assessors i influencers

Què és: perfils inventats —o reals suplantats— que ofereixen «formacions», senyals d'inversió o tutories privades.

CARACTERÍSTICA COMUNA

Prometen rendibilitat ràpida, garantida i sense risc, recolzats en testimoniatges i vídeos generats amb IA que donen aparença de comunitat.

Pista pràctica: si ningú de l'entorn de l'usuari coneix a aquest «expert» fora de la xarxa social on va aparèixer, és un senyal d'alarma.

Tipologia 4 · Phishing hiperpersonalitzat

Què és: missatges (SMS, email, xarxes) que esmenten dades reals —el banc, l'operador, l'assegurança— perquè la IA permet redactar a mesura i a gran escala.

EL QUE HO FA NOU

Webs i aplicacions clonades amb un nivell de detall visual i funcional que abans era impensable: logos, tipografies i comportaments idèntics a l'original.

Pista pràctica: mai prémer l'enllaç rebut. Entrar sempre teclejant la direcció o des de l'aplicació oficial.

Cas real anonimitzat · El fals professor

- **Context:** una persona contacta en xarxes amb un suposat professor que ofereix formació gratuïta en cripto.
- **El ganxo:** durant setmanes rep vídeos del «professor» explicant i mostrant guanys, tots generats amb IA.
- **El pas al frau:** després de guanyar-se la confiança, se'l convida a operar en una plataforma aparentment legítima.
- **El parany:** realitza diversos dipòsits i veu xifres creixents en pantalla durant un temps.
- **El tancament:** en intentar retirar, la plataforma exigeix comissions, impostos o verificacions que no acaben. El «professor» desapareix.
- **Lliçó clau:** la cara que «explica», la gratuïtat i la sensació de comunitat són palanques que la IA escala massivament.
- Cap element aïllat —ni el rostre, ni els vídeos, ni els testimoniatges— és prova de legitimitat.
- Cas anonimitzat, sense dades identificatives ni referències a procediments en curs.

Senyals d'alerta · Checklist pràctic

- Promesa de rendibilitat **alta, ràpida i sense risc**.
- Pressió per a prendre **decisiones immediates** o accedir a oportunitats «exclusives».
- Impossibilitat de verificar a la persona fora del canal on va aparèixer.
- La comunicació es trasllada ràpidament a missatgeria privada (WhatsApp, Telegram).
- La plataforma mostra beneficis, però posa traves creixents per a retirar.
- Sol·licitud **d'instal·lar apps fora de les botigues oficials** o de compartir pantalla.
- Identitat l'única prova de la qual són els propis vídeos i testimoniatges que apareixen en el canal.
- Petició de pagar **noves comissions, impostos o «verificacions»** per a alliberar fons.

Què fer si has estat víctima

- **No esborrar res:** conservar missatges, captures, correus, àudios, vídeos i justificants de pagaments.
- **Denunciar:** Policia Nacional o Guàrdia Civil. Existeixen unitats especialitzades en delictes tecnològics.
- **Comunicar a entitats implicades:** banc, operador o plataforma des de la qual es van fer els pagaments.
- **Buscar suport:** associacions com ASUFIN ofereixen orientació a persones afectades per frauds financers.
- **Assessorament professional:** advocats especialitzats i perits poden valorar l'abast del cas.
- **Revisar accessos:** canviar contrasenyes i activar verificació en dos passos en comptes que poguessin estar compromeses.
- **Dades de pagament:** si es van compartir, demanar targetes noves i vigilar moviments durant les setmanes següents.
- **No tornar a pagar:** pagar per a «recuperar» el perdut és una segona estafa habitual. Detenir qualsevol nou desemborsament.

Per a tancar

La IA no inventa el frau, però el fa més creïble i més accessible per a qui l'organitza.

La millor defensa no està en una eina nova, sinó en un canvi d'hàbit: verificar abans de confiar.



Verifica
siempre por
un canal
distinto.



¿Te ha gustado la formación?

Déjanos una **reseña en Google**.

Ayúdanos a que más personas conozcan nuestras actividades gratuitas.

Puedes escribir tu reseña **escaneando este QR:** ➔

Tan solo te llevará 1 minuto.

¡Gracias!



GRÀCIES

