ANDORRA DIGITAL

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

# Informe de Ciberintel·ligència

# Suplantació i estafes a les xarxes socials


TLP: WHITE

NOVEMBRE 2025

## FITXA DEL DOCUMENT

| Versió | Redactat/Revisat per | Aprovat per | Data aprovació | Data publicació |
|---|---|---|---|---|
| 1.0 | ANC-AD | ANC-AD | 27/11/2025 | 28/11/2025 |

| Registre de canvis | | | |
|---|---|---|---|
| Versió | Pàgines | Data Modificació | Motiu del canvi |
| | | | |

| | |
|---|---|
| Propietari del document | ANC-AD |

# ÍNDEX

**1. METODOLOGIA** **4**
**2. INTRODUCCIÓ** **5**
**3. TIPUS DE SUPLANTACIÓ I TÈCNIQUES UTILITZADES A LES XARXES SOCIALS** **6**
3.1. Tipus de suplantació utilitzats a les xarxes socials 6
3.1.1 Perfils falsos i robatori d'identitat 6
3.1.2 Suplantació d'empreses i executius d'empreses 7
3.1.3 Suplantació de figures públiques 9
3.2. Tècniques d'estafa més utilitzades a les xarxes socials 9
3.2.1 Estafes romàntiques 9
3.2.2 Ofertes de treball falses 10
3.2.3 Sortejos i premis falsos 11
3.2.4 Estafes d'inversió / criptomonedes 12
3.2.5 Sextorsió 13
3.2.6 Manipulació emocional o urgència 13
**4. IDENTIFICACIÓ DE SUPLANTACIONS A LES XARXES SOCIALS** **15**
4.1. Antiguitat del compte i la seva activitat 15
4.2. Anàlisi del contingut publicat 15
4.3. Anàlisi de la xarxa i el comportament del compte 15
4.4. Verificació de comptes a xarxes socials 16
4.4.1 X (antic Twitter) 16
4.4.2 LinkedIn 17
4.4.3 Instagram 17
4.4.4 Facebook 18
**5. BONES PRÀCTIQUES I MESURES DE MITIGACIÓ** **19**
5.1. Bones pràctiques 19
5.2. Mesures de mitigació / solucions davant de problemes 19
**6. CLÀUSULA DE CONFIDENCIALITAT** **21**

# 1. METODOLOGIA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). És un esquema creat per fomentar un intercanvi més bo d'informació delicada (però no classificada) en l'àmbit de la seguretat de la informació.

A través d'aquest esquema, d'una manera àgil i senzilla, s'indica fins on pot circular la informació més enllà del receptor immediat, i aquest ha de consultar l'Agència Nacional de Ciberseguretat d'Andorra quan cal distribuir la informació a tercers.

| Codi | Com es fa servir | Com es comparteix |
|---|---|---|
| TLP: RED | S'ha de fer servir **TLP:RED** quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, la reputació o les operacions si es fa servir malament. | Els receptors no han de compartir informació designada com a **TLP:RED** amb cap tercer fora de l'àmbit on va ser exposada originalment. |
| TLP: AMBER | S'ha de fer servir **TLP:AMBER** quan la informació ha de ser distribuïda de manera limitada, però suposa un risc per a la privacitat, la reputació o les operacions si és compartida fora de l'organització. | Els receptors poden compartir informació indicada com a **TLP:AMBER** només amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per compartir aquesta informació. |
| TLP: GREEN | S'ha de fer servir **TLP:GREEN** quan la informació és útil per a totes les organitzacions que hi participen, com també amb tercers de la comunitat o el sector. | Els receptors poden compartir la informació indicada com a **TLP:GREEN** amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics. |
| TLP: WHITE | S'ha de fer servir **TLP:WHITE** quan la informació no suposa cap risc de mal ús, conforme a les regles i procediments establerts per a la seva difusió pública. | La informació **TLP:WHITE** pot ser distribuïda sense restriccions, únicament subjecta a controls de copyright. |

## 2. INTRODUCCIÓ

Les estafes i els delictes per suplantació d'identitat a les xarxes socials estan en plena expansió. Els cibercriminals fan servir plataformes com ara X (antic Twitter), Instagram, WhatsApp o Facebook com a mitjà per llançar campanyes mitjançant les quals robar informació personal delicada o diners a les víctimes.

La raó és molt simple, el gran gruix de la població té comptes en una o diverses xarxes socials. S'han integrat al dia a dia de milions de persones i, per això, més enllà de ser un canal de comunicació, han esdevingut un risc potencial. Un vector d'atac amb una capacitat de llançar campanyes malicioses amb una alta taxa d'èxit. Cal destacar que, segons xifres oficials, la població mundial dedica entre 4 i 6 hores diàries a les xarxes socials o aplicacions de missatgeria, cosa que augmenta les oportunitats que els delictes dels cibercriminals tinguin èxit.

A més, a través de les xarxes socials es facilita tanta informació, sigui personal o professional, que permet que els atacants disposin amb tantes dades de les víctimes que el disseny d'una estratègia per cometre qualsevol mena d'acció maliciosa pot arribar a fregar la perfecció.

Per això, mitjançant aquest informe s'abordaran els diferents tipus de suplantació més freqüents a les xarxes socials: des de perfils falsos fins a la suplantació d'empreses i persones influents. També s'analitzaran les diferents tècniques d'estafes executades pels cibercriminals, que van des de la pesca i estafes romàntiques fins a fraus financers, criptoestafes i manipulació emocional.

Per acabar, s'explicaran les diferents estratègies per poder identificar aquest tipus d'estafes i s'analitzaran els riscos que s'hi associen, tot exposant una sèrie de bones pràctiques i mesures de prevenció que poden ajudar usuaris i empreses a detectar i evitar ser víctimes d'aquest tipus d'amenaces.

# 3. TIPUS DE SUPLANTACIÓ I TÈCNIQUES UTILITZADES A LES XARXES SOCIALS

Com ja s'ha esmentat, les xarxes socials han esdevingut una de les eines perfectes per als cibercriminals per, mitjançant diferents tipus d'estafes, obtenir beneficis econòmics o dades confidencials.

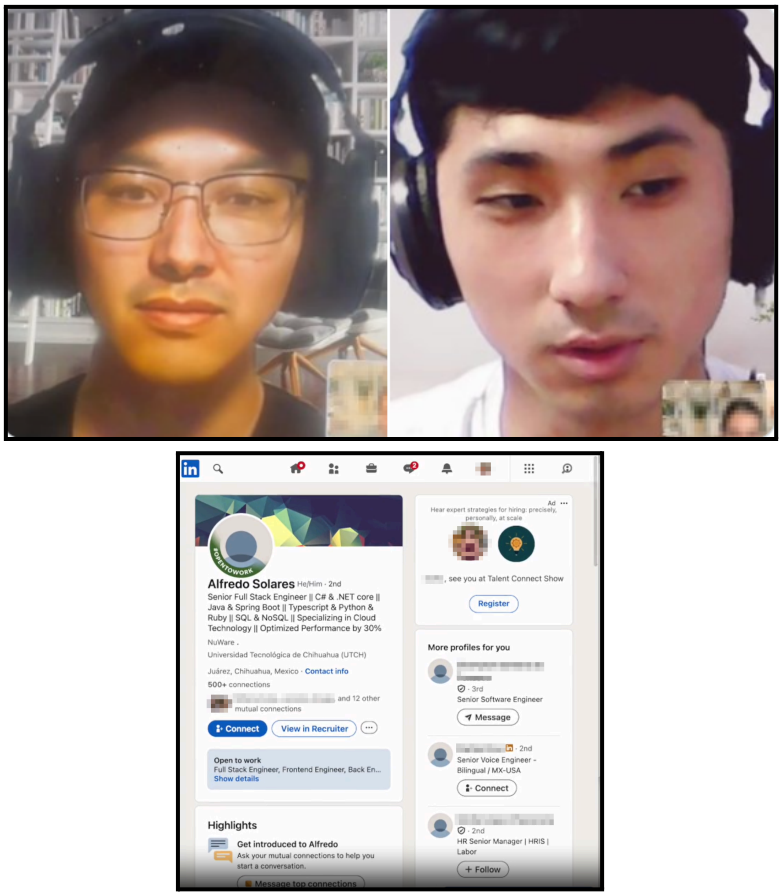
## 3.1. Tipus de suplantació utilitzats a les xarxes socials

A continuació, s'exposen els tipus de suplantació més utilitzats en xarxes socials, inclosos casos reals que permetran una comprensió més bona de com els ciberdelinqüents duen a terme les seves accions.

### 3.1.1 Perfils falsos i robatori d'identitat

La creació de perfils falsos és una de les pràctiques més comunes per part dels ciberdelinqüents. El modus operandi és senzill: fan servir fotos de perfil, nom, biografia i altres dades personals d'una persona real sense el seu consentiment. O, per altra banda, creen una persona totalment fictícia amb l'ús de la IA i hipertrucatge.

Un cas molt conegut descobert per l'equip Bitso Quetzal Team, va revelar com dos agents nord-coreans del grup Lazarus van intentar infiltrar-se al seu equip, fent-se passar per enginyers *full stack* mexicans. Els agents van crear perfils de LinkedIn molt creïbles i van utilitzar hipertrucatges per a les entrevistes amb videotrucada.




*Il·lustració 1 - Agents nord-coreans en una entrevista de feina + Perfil de LinkedIn fals*

Prèviament, havien creat perfils a LinkedIn amb què reforçaven i donaven credibilitat als personatges que havien creat, amb l'objectiu de cridar l'atenció de l'entitat objectiu i poder formar part de la seva plantilla.

En aquest cas concret, la finalitat era infiltrar-se a l'empresa per, posteriorment, actuar com a *insiders*, i tenir accés a informació delicada, exfiltrar-la i, fins i tot, la capacitat d'orquestrar alguna acció disruptiva que pogués afectar l'operativa normal de l'entitat.

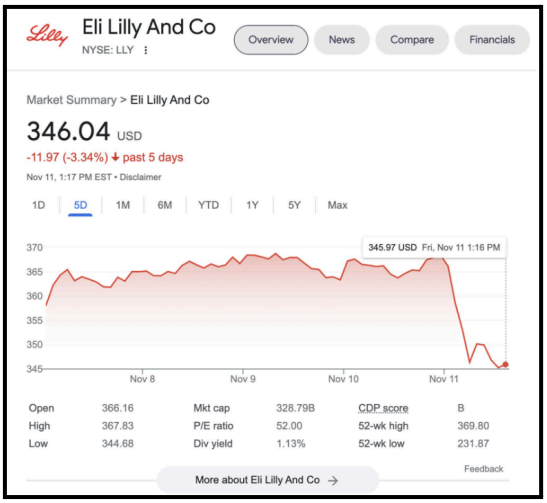
### 3.1.2 Suplantació d'empreses i executius d'empreses

Els cibercriminals també intenten imitar comptes d'empreses o comptes d'alts càrrecs i responsables.

Aquest tipus de suplantació pot arribar a comportar danys a la reputació de l'empresa i pèrdues milionàries tal com va passar a la companyia Eli Lilly and Company l'any 2022, quan un compte fals que estava verificat a la xarxa social X (antic Twitter), va publicar el post següent:


*Il·lustració 2 - Post fals a X suplantant Eli Lilly and Company*

Eli Lilly and Company és una farmacèutica i l'impacte del post que es mostra a la imatge, el qual va generar una enorme confusió i donava falses esperances a molts pacients, es va traduir en una caiguda de més del 4 % en les accions de l'empresa, és a dir, va perdre més de 15.000 milions de dòlars de valor. De fet, l'empresa es va veure obligada a disculpar-se després de les crítiques rebudes.





*Il·lustració 3 - Caiguda del 4 % de les accions d'Eli Lilly and Co + Post de disculpes als clients d'Eli Lilly and Co*

### 3.1.3 Suplantació de figures públiques

La suplantació de figures públiques per part dels cibercriminals és un altre dels esdeveniments més recurrents. Els principals objectius d'aquest tipus de suplantació, en què els atacants es fan passar per referents per a la població, és promoure desinformació, inversions enganyoses, estafes amb criptomonedes o dur a terme qualsevol mena de campanya fraudulenta secundària, com ara redirigir usuaris a URL malicioses.

Un cas molt conegut que va passar l'any 2022 va ser el pirateig a la xarxa social X, on uns ciberdelinqüents van aconseguir accedir a les eines internes de la xarxa social i van publicar posts des de comptes verificats de les figures públiques més influents del món, com Joe Biden, Elon Musk o Barack Obama.

Els posts publicats estaven relacionats amb una estafa de criptomonedes, en què es demanava diners per avançat i després es prometia tornar el doble del que es va lliurar.

En diverses hores els ciberdelinqüents van aconseguir recaptar més de 100.000 dòlars.


*Il·lustració 4 - Posts fraudulents a X de Joe Biden i Barack Obama*

## 3.2. Tècniques d'estafa més utilitzades a les xarxes socials

A continuació, exposarem les tècniques d'estafa més utilitzades a les xarxes socials, igual que l'apartat anterior, juntament amb casos reals que ens ajudaran a comprendre com els cibercriminals comenten aquestes estafes.

### 3.2.1 Estafes romàntiques

Les estafes romàntiques s'han tornat cada cop més reals, i aprofiten la confiança i, sobretot, la vulnerabilitat emocional de les víctimes. Un cas molt mediàtic va ser una dona francesa que va creure estar en contacte amb el famós actor Brad Pitt.

En el cas de Brad Pitt, la víctima va ser contactada per Instagram per algú que feia passar per la mare de l'actor. El cibercriminal va fer ús de fotos generades per IA. Així, mitjançant deepfakes i missatges, va anar creant una relació propera. Finalment, va sol·licitar a la víctima una transferència d'1 milió de dòlars per a un suposat trasplantament de ronyó. Víctima que va acabar caient a l'estafa i va transferir 850.000 dòlars.


*Il·lustració 5 – Hipertrucatge i missatges falsos que suplantaven l'actor Brad Pitt*

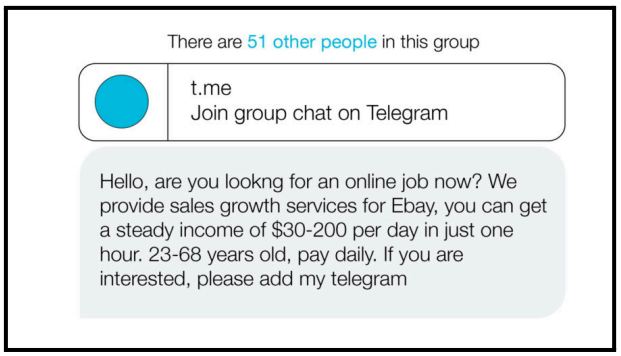
Encara que sembli increïble, aquest no és l'únic cas reportat, ja que 2 dones espanyoles també van ser enganyades, creient que tenien una relació amb Brad Pitt, i el que els va suposar una pèrdua de 325.000 euros.

### 3.2.2 Ofertes de treball falses

Les ofertes de feina falses són una tècnica d'estafa en les quals els ciberdelinqüents es fan passar per reclutadors per enganyar persones que busquen feina. En aquest tipus d'estafes es publiquen llocs de treball que solen prometre salaris alts, per atraure més gent.

L'objectiu final està relacionat amb obtenir dades confidencials de les víctimes, com també cobrar pagaments per tràmits que no existeixen o instal·lar qualsevol mena de codi maliciós que pugui robar dades.

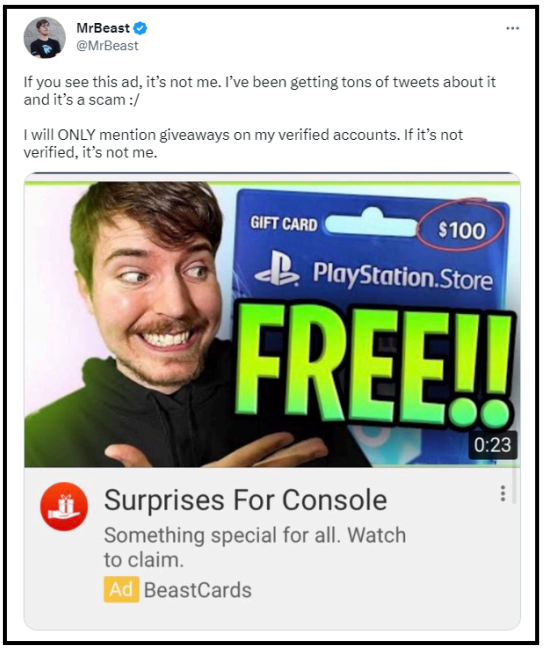
Les estafes més comunes relacionades amb ofertes de feina estan relacionades amb tasques pagades. Un cas molt comú d'estafa és la següent: a l'«oferta de treball» publicada prometen entre 30 i 200 dòlars al dia per donar serveis per «intentar augmentar vendes a través d'eBay». Al principi els ciberdelinqüents paguen petites quantitats per augmentar la confiança amb la víctima. Quan la confiança és més gran, els cibercriminals van demanant que paguin per certs productes i serveis amb la promesa de tornar-ho tot amb una comissió. Però els diners no arriben i molt menys la comissió.




*Il·lustració 6 – Oferta de treball falsa a l'app de missatgeria Telegram*

### 3.2.3 Sortejos i premis falsos

Hi ha una cosa que s'està popularitzant molt els darrers anys: els sorteigs o premis fraudulents. Els ciberdelinqüents fan servir la imatge de personatges públics, per generar més confiança i proximitat amb la víctima.




*Il·lustració 7 – Post a X del youtuber MrBeast publicitant sortejos falsos amb la seva imatge*

En el cas exposat, els ciberdelinqüents utilitzen la imatge del famós youtuber James Stephen Donaldson (MrBeast) que és molt conegut per premiar amb diners els seus subscriptors en diferents reptes i desafiaments.

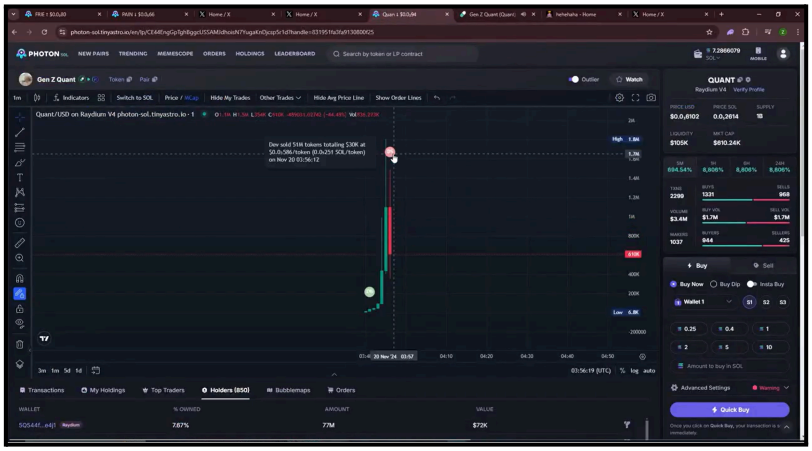
Aquest tipus d'estafa incita a fer clic a l'anunci de YouTube on el més probable és que l'anunci us porti a una pàgina de pesca on es roben credencials o s'usa per instal·lar qualsevol mena de codi maliciós (*malware*). En aquest cas concret, el premi eren targetes de regal de la PlayStation store.

### 3.2.4 Estafes d'inversió / criptomonedes

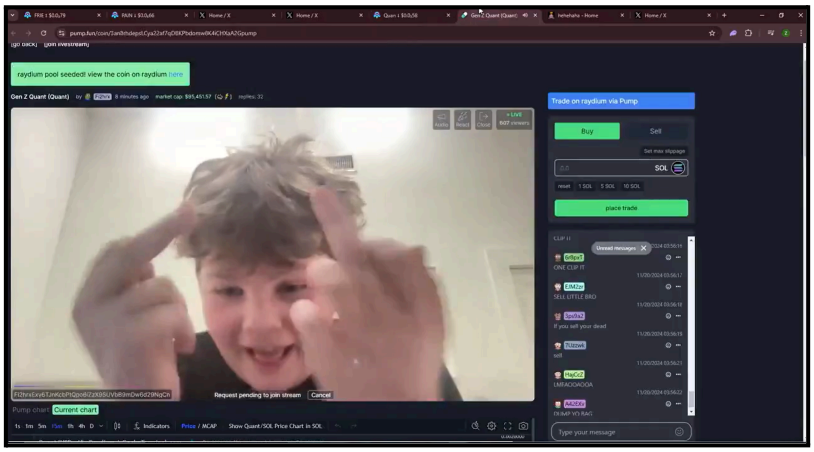
Les estafes relacionades amb inversions, incloses les que contemplen criptomonedes, són cada cop més comunes, perquè els estafadors prometen rendibilitats superiors a la mitjana amb poc o gens de risc.

Un dels casos més il·lustratius es va produir el novembre de l'any 2024, quan un nen de 13 anys va crear una *memecoin* anomenada «Gen Z Quant». En ser el seu creador, ben aviat va adquirir uns 18,98 M de tokens per 460 dòlars. Després, el nen va promocionar la *memecoin* a diferents xarxes socials i en streaming, i va indicar que el token generaria un retorn del 100 % de rendibilitat.

Va atraure milers de seguidors que van comprar tokens, i van inflar el preu de la *coin*. En ple *stream*, quan la *memecoin* estava al punt més alt, el nen va vendre de cop tots els seus tokens valorats en aquell moment en 30.000 dòlars. La venda va provocar que el seu preu col·lapsés immediatament, i va deixar tots els altres titulars de la *memecoin* arruïnats.




*Il·lustració 8 – Moment en què la* memecoin *«Gen Z Quant» va perdre tot el valor*




*Il·lustració 9 – Moment en què el nen es va burlar en* streaming *de tots els titulars de la* memecoin *«Gen Z Quant»*

### 3.2.5 Sextorsió

Aquest tipus de pràctica consisteix en un xantatge pròpiament dit, mitjançant el qual els ciberdelinqüents, després d'obtenir imatges o vídeos sexuals explícits de les víctimes, posteriorment les coaccionen amb diferents objectius: poden abastar des del rèdit econòmic fins a l'obtenció de més material.

Aquest tipus d'estafes comencen de manera molt semblant a les estafes romàntiques, ja que generalment se solen iniciar amb un contacte consentit a través de xarxes socials o aplicacions de cites. Després d'això, el ciberdelinqüent es guanya la confiança de la víctima mitjançant afalacs, regals o simulant un vincle sentimental, fins a aconseguir aquest material íntim de la víctima amb què després l'amenaçarà de publicar-lo.

També hi ha casos on el cibercriminal aconsegueix piratejar el mòbil o dispositius de la víctima. Acció que li permet robar imatges ja existents.

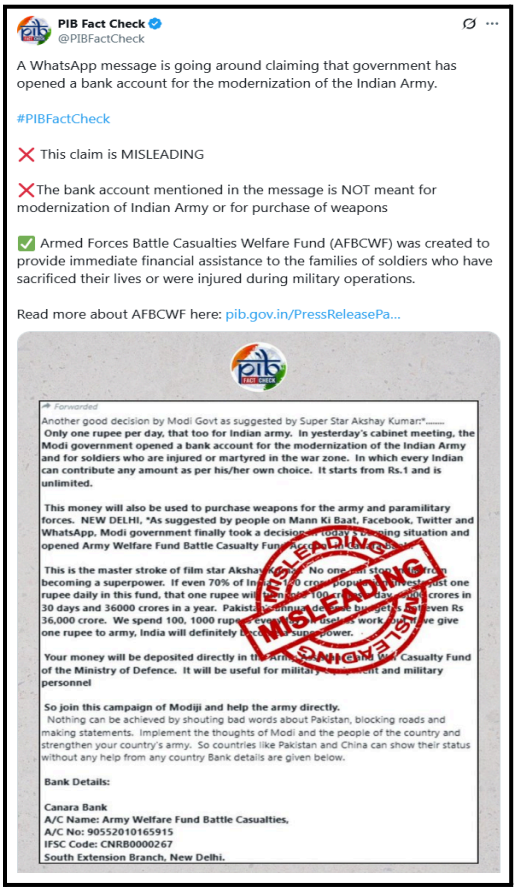
### 3.2.6 Manipulació emocional o urgència

Els casos de manipulació o urgència comencen amb un missatge, un correu, un anunci que sol tenir contingut que genera por, pressió o urgència per tal que les víctimes actuïn de manera ràpida i impulsiva. La finalitat?, aconseguir algun tipus de transferència econòmica o dades delicades.

Entre aquest tipus de pràctiques són recurrents les estafes relacionades amb donacions o aportacions a organitzacions humanitàries.

Un cas molt conegut va passar a l'Índia recentment, en què el Ministeri de Defensa de l'Índia va emetre un comunicat on van advertir sobre un missatge enganyós que estava circulant a l'aplicació de missatgeria WhatsApp on s'animava a fer donacions a l'exèrcit del país.

L'objectiu era obtenir diners per al suposat suport a soldats ferits i a la modernització de l'aparell militar indi.




*Il·lustració 10 – Post a X del compte de PIB Fact Check de l'Índia advertint de l'estafa*

# 4. IDENTIFICACIÓ DE SUPLANTACIONS A LES XARXES SOCIALS

Com ja hem vist a l'apartat anterior, la suplantació d'identitat a les xarxes socials és una de les tècniques més repetides en fraus digitals.

La gran varietat d'aquestes tècniques, com també la quantitat de recursos i eines que possibiliten que els cibercriminals puguin llançar campanyes d'una sofisticació considerable, fa que cada vegada siguin més difícils de detectar.

Per això, s'exposen una sèrie d'indicadors que poden permetre que qualsevol usuari destriï sobre la legitimitat d'un perfil o, per contra, detecti si es tracta d'una suplantació.

## 4.1. Antiguitat del compte i la seva activitat

La data de creació d'un compte o la seva antiguitat és un dels primers elements que cal corroborar.

Els comptes de creació recent amb una alta taxa d'activitat han de fer sospitar, a més dels perfils que no han tingut activitat en molt de temps i, de sobte, comencen a publicar enllaços de manera recurrent.

Un altre dels indicadors que poden ajudar a identificar un cas de compte sospitós són els seguidors que té. En la majoria dels casos, el nombre de seguidors és molt alt, però realment són bots i no perfils reals.

## 4.2. Anàlisi del contingut publicat

Els ciberdelinqüents solen deixar pistes que els delaten i aquests serien els punts clau que permeten diferenciar un compte legítim d'un que no ho és:

- Estil i to de comunicació.
- Posts aliens al perfil real.
- Enllaços sospitosos i trucades urgents.
- Freqüència irregular de posts.

## 4.3. Anàlisi de la xarxa i el comportament del compte

La manera com interactua un compte dona senyals clars sobre la seva legitimitat, és per això que cal prestar atenció especial a aquests punts:

- Seguidors i seguits.
- Interaccions automatitzades o bots.
- Antiguitat i activitat recent.

- Interaccions amb altres comptes sospitosos.

## 4.4. Verificació de comptes a xarxes socials

La verificació oficial de les xarxes socials és un indicador molt útil per poder diferenciar entre comptes legítims i comptes falsos.

A continuació, es veuran les diferències entre les diferents xarxes socials.

### 4.4.1 X (antic Twitter)

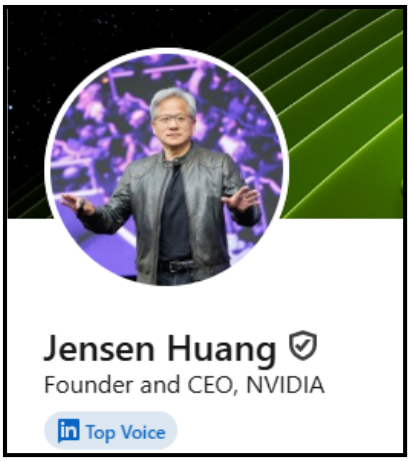
La xarxa social X (antic Twitter), fa servir diferents colors i insígnies per poder diferenciar els comptes. Aquests serien els diferents sistemes de verificació:

- Insígnia blava: és la més comuna i, per tant, amb la qual cal tenir més cura, perquè aquesta insígnia només indica que el compte té una subscripció de X Premium, és a dir, que és de pagament.
- Insígnia daurada: està reservada per a organitzacions o empreses, requereix la subscripció de X Premium, amb la diferència que cal fer una verificació de l'entitat.
- Insígnia grisa: únicament els governs o entitats governamentals la poden obtenir.
- Insígnia d'afiliació: apareix als comptes individuals que estan vinculats a una organització amb insígnia daurada.


*Il·lustració 11 – Diferents tipus de verificacions a la xarxa social X*

### 4.4.2 LinkedIn

La xarxa social de LinkedIn podríem dir que és la xarxa amb el sistema de verificació més segur. La raó és que exigeix una verificació d'identitat prèvia mitjançant documents oficials com un DNI o un passaport.

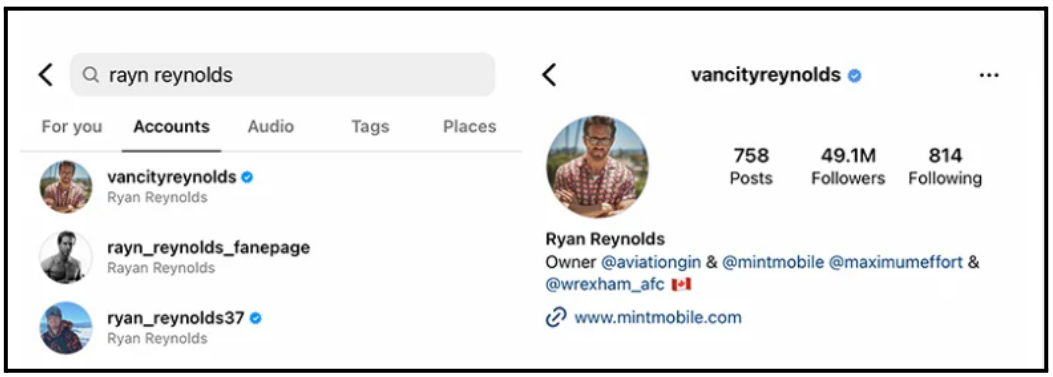



*Il·lustració 12 – Verificació a la xarxa social de LinkedIn*

### 4.4.3 Instagram

A la xarxa social d'Instagram hi ha dos tipus de verificacions, la marca blava gratuïta per a empreses i persones públiques i la verificació de pagament més coneguda com a «Meta Verified».

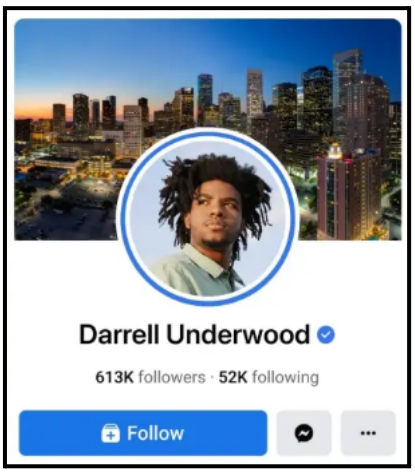
Totes dues verificacions requereixen un DNI i un *selfie*. Entre aquestes dues verificacions no hi ha cap mena de diferència visual a la marca blava, són completament idèntiques, però el fet que hagis de verificar el compte amb un DNI i un *selfie* fa que Instagram protegeixi contra la suplantació d'identitat.




*Il·lustració 13 – Verificació a la xarxa social d'Instagram*

### 4.4.4 Facebook

El sistema de verificacions a la xarxa social Facebook és idèntica a Instagram, perquè comparteixen el mateix ecosistema (Meta Platforms).




*Il·lustració 14 – Verificació a la xarxa social de Facebook*

# 5. BONES PRÀCTIQUES I MESURES DE MITIGACIÓ

Tot seguit, analitzarem les millors pràctiques i mesures de mitigació per poder protegir-se i identificar i evitar les diferents estafes que s'han abordat al llarg del document.

## 5.1. Bones pràctiques

- El més important i bàsic és tenir contrasenyes fortes i úniques, això se sol repetir molt, però és una realitat. Combinar lletres majúscules i minúscules amb números i caràcters especials farà que la nostra contrasenya sigui forta i robusta, també evitar repetir contrasenyes a diverses plataformes és molt important.

- Habilitar l'autenticació 2FA, això afegeix una capa extra de seguretat a tots els nostres comptes.

- Verificar perfils i enllaços sospitosos: abans d'interactuar amb un perfil estrany o accedir a un enllaç sospitós és de vital importància confirmar si el perfil amb el qual estem parlant és legítim o no, tal com hem analitzat a l'apartat d'identificació de suplantacions.

- Configurar la privadesa del nostre compte: limitar la visibilitat del nostre compte, publicacions i dades personals a contactes propers.

- Revisar les sol·licituds d'amistat que rebem als nostres comptes per no acceptar perfils desconeguts sospitosos.

- Monitorar l'activitat dels nostres comptes, és molt important, revisar les notificacions d'inicis de sessió, canvis de nom, missatges sospitosos ens ajudarà a tenir més control dels nostres comptes.

- Formar-se sobre noves estafes ens donarà més coneixement, així reconeixerem immediatament la pesca (*phishing*), els sortejos falsos, els missatges d'urgència, els URL sospitosos, etc.

## 5.2. Mesures de mitigació / solucions davant de problemes

- El primer pas després d'haver estat víctima d'una suplantació d'identitat o estafa és recopilar totes les evidències, sigui captures de pantalla, missatges, nom d'usuaris, enllaços o URL implicades, tota aquesta recol·lecció de dades ens ajudarà en un futur davant d'una possible denúncia.

- Contactar amb la xarxa social on s'ha produït la suplantació, i demanar la revisió del compte fals per eliminar-lo. Totes les xarxes socials tenen un apartat d'ajuda on gestionen aquests casos:
    - X (Twitter):https://help.x.com/es/safety-and-security/report-x-impersonation
    - Instagram:https://es-es.facebook.com/help/instagram/370054663112398
    - Facebook:https://es-es.facebook.com/help/306643639690823
    - LinkedIn:https://www.linkedin.com/help/linkedin/answer/a1338436

## 6. CLÀUSULA DE CONFIDENCIALITAT

Aquest document és propietat de l'Agència Nacional de Ciberseguretat d'Andorra. Tota la informació que conté és confidencial, aquesta informació s'actualitzarà regularment per reflectir els possibles canvis dels productes i no podrà ser copiada o revelada a terceres persones sigui totalment o en part, sense consentiment previ exprés de l'Agència Nacional de Ciberseguretat d'Andorra.