ANDORRA DIGITAL

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

Ciberestafes en casos d'emergència: el cas DANA

TLP: WHITE

GENER 2025

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	22/01/2025	27/01/2025

Registre de canvis			
Versió	Pàgines	Data Modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

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

En contexts d'emergència, com ara els desastres naturals, les pandèmies, les crisis socials o els conflictes, les ciberestafes tendeixen a augmentar significativament. Els ciberdelinqüents aprofiten la vulnerabilitat emocional, la necessitat d'informació urgent i la disposició de les persones per ajudar o protegir-se. Els correus electrònics i els missatges de les xarxes socials fraudulents, que sovint contenen enllaços o arxius adjunts maliciosos, són comuns després d'aquests esdeveniments.

Després de l'impacte de la dana que va afectar València, i va causar estralls seriosos als habitatges, els vehicles i a les infraestructures, les autoritats van advertir sobre un increment en les ciberestafes. Els ciberdelinqüents es van aprofitar de la vulnerabilitat de les persones afectades mitjançant estafes en línia, adreçades especialment als qui intenten accedir a ajudes econòmiques o fer donacions solidàries per als damnificats.

Aquests fraus cibernètics es dirigeixen tant a les persones directament afectades pel desastre com als que busquen col·laborar mitjançant donacions. Mitjançant missatges enganyosos, els estafadors es fan passar per organismes oficials, companyies d'assegurances i empreses de reparació, amb l'objectiu de recopilar dades personals i financeres de les seves víctimes.

Aquest informe analitza el perill de les ciberestafes en situacions d'emergència, i aborda el cas concret de la dana de València. Es destaquen les estratègies principals emprades pels delinqüents, els riscos involucrats i les accions necessàries per prevenir aquestes ciberestafes. A més, s'aborda la importància de protegir tant les persones vulnerables com les que busquen ajudar de manera solidària.

3. CARACTERÍSTIQUES DE LES CIBERESTAFES EN EMERGÈNCIES

Les estafes en contextos d'emergència acostumen a compartir característiques específiques que les fan particularment efectives.

- **Oportunisme:** les ciberestafes es despleguen ràpidament després de l'inici d'una situació de crisi o emergència.
- **Emocionalitat:** apel·len a la por, la urgència o la solidaritat per persuadir les víctimes.
- **Diversitat de mètodes:** inclouen correus electrònics fraudulents, missatges a les xarxes socials, trucades telefòniques i aplicacions mòbils malicioses.
- **Dificultat per verificar informació:** en mig de la confusió, moltes persones no verifiquen l'autenticitat de les sol·licituds d'ajuda o de les alertes.

3.1. Psicologia darrera dels ciberdelictes

Les ciberestafes estan dissenyades per manipular les emocions i els processos de presa de decisions de les persones. Els ciberdelinqüents exploten biaixos psicològics, vulnerabilitats emocionals i patrons de comportament humà.

Aquesta forma d'estafa digital, que aprofita les emocions humanes i fa servir l'ajuda solidària com a esquer, no és un fenomen nou. Tanmateix, el fet que es repeteixi demostra que aquesta mena de manipulació psicològica continua essent efectiva.

4. MÈTODES MÉS COMUNS D'ESTAFA

Entre els mètodes més comuns d'estafa, hi ha els següents:

- **Pesca**: enviament de correus o missatges fraudulents que aparenten ser d'organitzacions legítimes (per exemple, ONG, institucions del govern) per recopilar dades personals, bancàries o instal·lar programari maliciós.

- **Campanyes de donació falses**: creació de llocs web o perfils de xarxes socials que simulen recaptar fons per a víctimes de desastres. Aquestes plataformes solen ser impossibles de rastrejar una vegada s'ha fet el pagament.

- **Ofertes falses d'ajuda, serveis o productes escassos**: anuncis de subministraments essencials, com ara aliments, medicaments o refugi, que requereixen un pagament per avançat i no es lliuren mai. Per exemple, els estafadors poden oferir productes que són escassos, com ara els equips de protecció personal durant una pandèmia, a preus inflats o les víctimes paguen per aquests productes i no els reben mai.

- **Notícies o alertes falses**: propagació de rumors o alertes manipulades per redirigir els usuaris a llocs maliciosos. Aquesta és una tàctica comuna per provocar el caos i facilitar altres tipus d'estafes. Els delinqüents difonen informació errònia per manipular les persones i adreçar-les a llocs web maliciosos.

- **Suplantació d'identitat**: perfils a les xarxes socials o correus electrònics que imiten figures públiques, governs o organitzacions humanitàries. Els delinqüents es fan passar per autoritats o representants d'organitzacions reconegudes, com ara entitats governamentals, ONG o empreses reconegudes, per sol·licitar informació confidencial o pagaments.

5. CAMPANYES DETECTADES DURANT LA DANA DE VALÈNCIA

Les inundacions provocades per la dana a València van generar un escenari propici per a la proliferació de diverses ciberestafes. Aquestes es van enfocar a explotar tant la solidaritat de les persones com el caos causat per l'emergència. Aquests casos posen en relleu els riscos associats amb l'ús de plataformes digitals no verificades en moments d'emergència, com també la importància de recórrer a canals oficials i confiables per fer donacions.

Entre les estratègies més habituals destaquen les campanyes de desinformació, les campanyes de suplantació d'identitat, anuncis falsos i estafes telefòniques.

5.1 Campanyes de desinformació

En situacions d'emergència, és comú que es propaguin notícies falses que generen confusió a l'opinió pública, especialment entre les persones en situació de vulnerabilitat, que solen tenir un accés més limitat a la informació oficial.

Aquests missatges falsos, difosos amb la intenció de desacreditar les institucions i les organitzacions que gestionen les ajudes, formen part d'una sèrie d'alertes enganyoses que solen sorgir després d'esdeveniments de rellevància, com ara desastres naturals, amb l'objectiu de generar pànic i desinformació. Alguns d'ells van afectar directament les donacions i el voluntariats dels ciutadans destinats a donar suport a les persones afectades per la dana.

Tot seguit, es presenten exemples d'aquestes campanyes de desinformació:

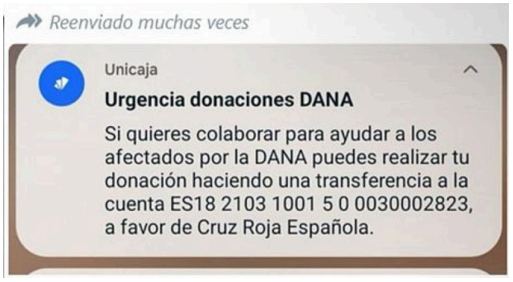
- Algunes publicacions a les xarxes socials afirmaven que els serveis d'emergència oficials, com la línia 112 de la Comunitat Valenciana, no estaven operatius, i fomentaven confusió entre les persones afectades. El missatge que va ser compartit a WhatsApp, X i Facebook assegurava que el 112 havia caigut per les conseqüències de la dana i que l'alternativa era el 963428000.

- Un altre anunci va estar relacionat amb un possible pirateig per obrir fotos del president a Paiporta. Aquest missatges, que va circular a través de WhatsApp es va viralitzar ràpidament. El text de la cadena deia:

  «Pujaran unes fotos del nostre president, a Paiporta, mentre recollia fang després de la dana, no les obris ni les vegis, et pirateja el telèfon en 10 segons i no es pot aturar de cap manera. Passa-li la dada als teus familiars i amics. NO L'OBRIS, també ho han dit a les televisions comparteix-lo» (sic).

  La cadena assegurava que veure o obrir unes suposades imatges del president a Paiporta després de les inundacions provocades per la dana, podria piratejar el telèfon mòbil en qüestió de segons. Tanmateix, no es va presentar cap evidència que recolzi aquesta afirmació.

- També es va difondre una captura d'un SMS el remitent del qual era el banc Unicaja i es va explicar que es tractava d'una estafa. Tanmateix, aquest missatge en el qual es demanava suport per a la Creu Roja Espanyola era oficial.



5.2 Campanyes de suplantació d'identitat

Uns estafadors es van fer passar per organitzacions reconegudes com ara la Creu Roja, i van demanar donacions a través de canals fraudulents. Aquestes campanyes es van fer tant en format digital, mitjançant llocs web i enllaços falsos, com amb visites físiques a llars afectades, i van demanar pagaments en efectiu o transferències bancàries.

Per altra banda, es van detectar campanyes de pesca i pesca per SMS en les quals es van enviar missatges de text fraudulents que aparentaven que procedien de l'Agència Estatal de Meteorologia (AEMET). Aquests missatges, dissenyats per enganyar els usuaris, advertien sobre una suposada tempesta greu a la regió i incloïen un enllaç que invitava a descarregar una aplicació per mantenir-se estalvi.

L'AEMET va desmentir ràpidament la veracitat d'aquests missatges, i va assenyalar que es tractava d'una estafa que tenia com a objectiu principal robar dades personals i financeres, particularment d'usuaris de dispositius Android. Els enllaços inclosos als SMS descarregaven un arxiu maliciós (*malware*) dissenyat per robar dades financeres i personals, especialment d'usuaris de dispositius Android.

Hi ha algunes evidències que poden fer sospitar de la legitimitat d'aquests missatges de text fraudulents:

- Errors ortogràfics i gramaticals: el text del missatge contenia múltiples faltes d'ortografia, com ara la manca de titllets a les paraules clau: “Se preve una tormenta severa en su region. Preparese y mantengase a salvo. Descargue la APP”. Aquestes inconsistències són indicatives que el missatge no prové d'una font oficial.

- Ús de llenguatge alarmista: s'intentava generar urgència al receptor, una tàctica comuna a les estafes, per induir l'usuari a actuar ràpidament sense verificar l'autenticitat del missatge.

- L'AEMET no envia SMS ni demana descàrregues externes: la mateixa AEMET, a través del seu compte oficial a X, va aclarir que no fan servir SMS per comunicar-se i que la seva aplicació només està disponible a les botigues oficials d'aplicacions, com ara Google Play i l'App Store.

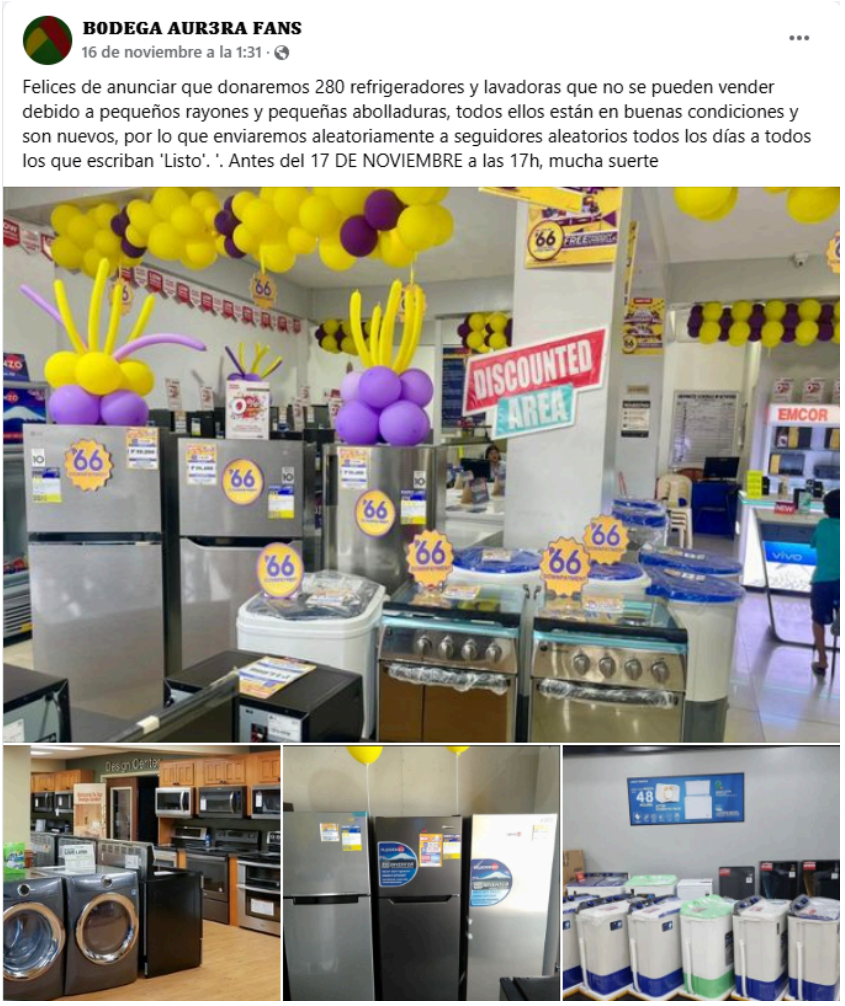
5.3 Anuncis falsos

En relació amb els anuncis falsos, s'esmenten dos casos:

- Un anunci fraudulent a Facebook pretenia captar l'atenció dels usuaris amb la promesa de regalar refrigeradors i rentadores noves amb defectes menors als qui interactuessin amb la publicació comentant la paraula «Listo». El missatge està dissenyat per semblar legítim i apel·lar a les emocions, i ofereix productes de valor sense cap cost. El text de l'anunci diu:

  «Felices de anunciar que donaremos 280 refrigeradores y lavadoras que no se pueden vender debido a pequeños rayones y pequeñas abolladuras. Todos ellos están en buenas condiciones y son nuevos, por lo que enviaremos aleatoriamente a seguidores aleatorios todos los días a todos los que escriban 'Listo'. Antes del 17 DE NOVIEMBRE a las 17h, mucha suerte.»

  L'objectiu principal és recol·lectar informació personal o fomentar la interacció per incrementar la visibilitat d'una pàgina enganyosa. En certs casos, les persones que comenten o comparteixen la publicació són contractades posteriorment i se'ls demana que completin «tràmits», on se'ls exigeix proporcionar dades delicades o, fins i tot, fer pagaments.



- Anuncis falsos de serveis: promocionen serveis de reparació urgent que mai es concreten després de rebre el pagament inicial.

5.4 Estafes telefòniques

Es van detectar estafes telefòniques relacionades amb la dana a València, en les quals els estafadors es fan passar per representants d'empreses d'assegurances o serveis públics. Durant les trucades, aquests estafadors afirmaven falsament que calia proporcionar dades personals i bancàries per gestionar reclamacions d'ajudes. Tanmateix, el veritable objectiu d'aquestes trucades era obtenir informació delicada i fer càrrecs fraudulents als comptes de les víctimes.

6. CAS D'ESTUDI

6.1 Campanya frau ayudavalencia.es

El govern espanyol va suspendre la pàgina web «ayudavalencia.es» per causa d'indicis de frau vinculats a donacions fraudulentes fetes mitjançant criptomonedes. La decisió es va prendre després que es detectessin possibles activitats il·lícites relacionades amb les peticions d'ajuda per als afectats per la dana a València.

La mesura, adoptada amb caràcter d'urgència, va sorgir arran d'una denúncia presentada per la Policia Nacional espanyola, que va advertir sobre irregularitats a les transaccions econòmiques demanades a través de Bitcoin, un canal que va generar sospites atesa la seva opacitat i el potencial per al blanqueig de diners.

L'operació la va coordinar Red.es, entitat adscrita al Ministeri d'Assumptes Econòmics i Transformació Digital, en col·laboració amb les forces de seguretat de l'Estat. Per garantir la suspensió de l'accés a la pàgina, Red.es va treballar juntament amb els operadors principals de telecomunicacions del país, i va aconseguir el bloqueig de la navegació cap al lloc web.

7. RECOMANACIONS

La prevenció és la millor eina contra les ciberestafes. En adoptar un enfocament crític, verificar les fonts i ser previngut davant dels missatges, correus o publicacions sospitoses, es pot marcar la diferència per protegir la informació personal i evitar ser una víctima d'aquesta mena de delicte.

Tot seguit, es presenten mesures clau per prevenir les ciberestafes que sorgeixen a partir de situacions d'emergència:

7.1 Recomanacions generals

Com a recomanació general, és important ser caut amb correus electrònics i missatges sospitosos:

- Evitar interactuar amb correus electrònics que tinguin assumptes alarmistes, arxius adjunts o enllaços relacionats amb emergències.
- Verificar que la informació sobre el desastre procedeixi de fonts confiables, com ara organismes oficials locals o nacionals, o entitats reconegudes de resposta a emergències.
- Desconfiar de sol·licituds que apel·lin a l'emoció. Per exemple, s'ha d'anar amb molt de compte amb súpliques difoses a les xarxes socials, missatges de text o, fins i tot, sol·licituds porta a porta que busquin donacions immediates. Igualment, abans de fer qualsevol contribució, cal investigar si l'organització és legítima.

7.2 Com actuar davant de missatges fraudulents (pesca/pesca per SMS)

Si es reben missatges sospitosos, com és el cas de l'SMS que simulava ser de l'AEMET:

- Eliminar el missatge immediatament i bloquejar el remitent per evitar intents de contacte en un futur.
- Informar sobre l'incident els organismes corresponents, com ara a l'Agència Nacional de Ciberseguretat d'Andorra, en aquells casos que les campanyes es detectin la país, o bé a l'INCIBE (Instituto Nacional de Ciberseguridad espanyol) quan es detectin a Espanya, per tal que puguin advertir altres usuaris

Si es fa clic a l'enllaç, però no es descarrega res:

- Esborrar qualsevol enllaç o arxiu descarregat associat.
- Escanejar el dispositiu amb un antivirus per assegurar que no hagi estat compromès.

Si es descarrega i executa un arxiu sospitós:

- Desconnectar el dispositiu d'Internet o del wifi per evitar que la infecció es propagui.

- Executar una anàlisi completa amb un antivirus per eliminar qualsevol amenaça.
- Si el problema persisteix, cal considerar restablir el dispositiu als seus valors de fàbrica.

Igualment, cal reunir evidències (captures de pantalla, missatges, arxius) i denunciar-ho a les autoritats pertinents.

7.3 Com gestionar anuncis falsos a les xarxes socials

Pel que fa als anuncis sospitosos, es recomana el següent:

- No interactuar amb publicacions sospitoses: evitar comentar, compartir o fer clic als enllaços inclosos a les publicacions sospitoses.
- Verificar sempre la font: confirmar que les promocions, anuncis o sol·licituds provenen de comptes verificats o pàgines oficials.
- Denunciar contingut enganyós: fer servir les eines de denúncia disponibles a les plataformes com ara Facebook o Instagram per informar de publicacions fraudulentes.
- Educar i comunicar a altres persones: informar a familiars i amics sobre aquest tipus d'estafes i explicar-los com reconèixer-les per evitar que es converteixin en víctimes.

8. 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.