ANDORRA DIGITAL

ANDORRA DIGITAL CIBERSEGURETAT

Transformació Digital d'ANDORRA

LA INTEL·LIGÈNCIA ARTIFICIAL FA QUE L'ENGINYERIA SOCIAL SIGUI ENCARA MÉS PERFECTA

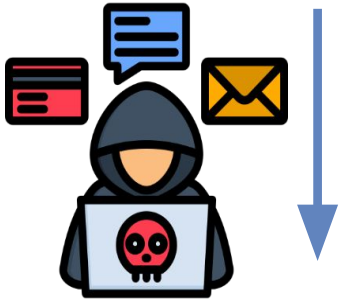
Setembre 2026
Document d'ús públic

Índex

Índex

1. INTRODUCCIÓ

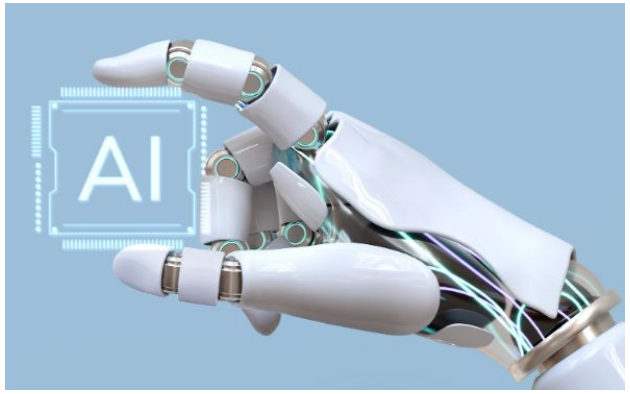
ENGINYERIA SOCIAL tècniques que fan servir els ciberdelinqüents per dur a terme els ciberatacs.



En què consisteix?

En lloc d'atacar directament els sistemes informàtics, ataquen les **PERSONES**.

La baula més vulnerable de la cadena



La **intel·ligència artificial** ha revolucionat els atacs d'enginyeria social.

Els ciberdelinqüents creen missatges, correus electrònics, àudios i vídeos molt més **creïbles**, **personalitzats** i **difícils de detectar.**

Intel·ligència artificial

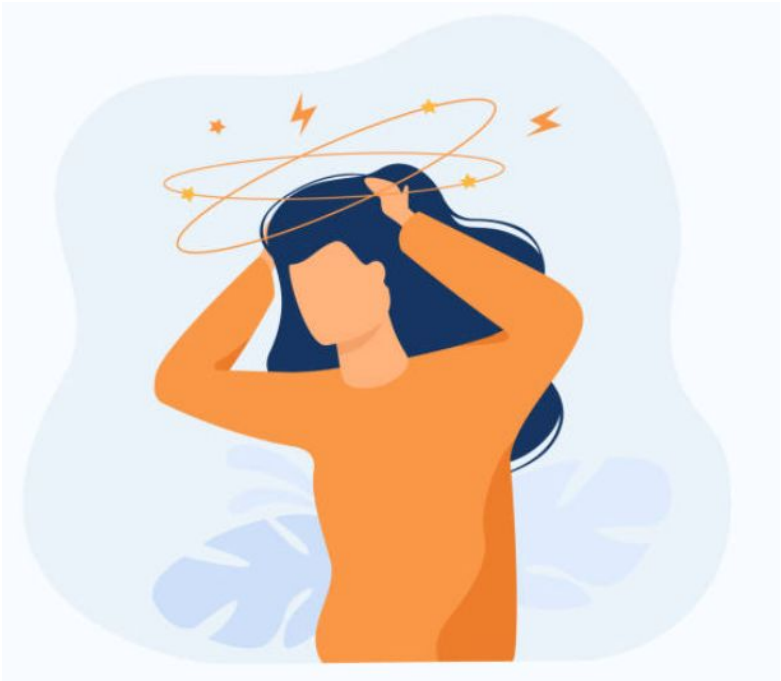
- Permet automatitzar gran part del procés i augmentar significativament la probabilitat d'èxit.
- Detectar faltes d'ortografia, errors gramaticals o missatges poc creïbles és més complicat amb la IA, atès que aquests senyals desapareixen cada vegada més.

L'**enginyeria social** consisteix a manipular psicològicament una persona per tal que:

- Reveli informació confidencial.
- Faci una acció determinada.
- Autoritzi una transacció.
- Faciliti accessos o credencials.

Principis psicològics més emprats

- Urgència
- Autoritat
- Por
- Curiositat
- Confiança
- Recompensa



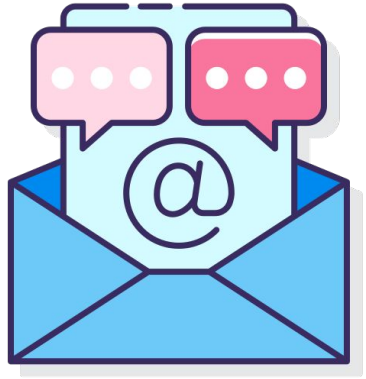
ANDORRA DIGITAL

ANDORRA DIGITAL
CIBERSEGURETAT

2. COM AJUDA LA IA ELS ATACANTS

Correus electrònics perfectes

- Abans:
  - Errors ortogràfics
  - Traduccions deficients
  - Missatges genèrics



«Soc del departament de TI. Hem detectat una activitat sospitosa en el teu compte. Necessitem que validis la teva contrasenya immediatament.»

- Ara:
  - Correus personalitzats
  - Sense errors
  - Adaptats a l'idioma i al càrrec de la víctima

Pesca hiperpersonalitzada

La IA pot analitzar:

- LinkedIn
- Xarxes socials
- Web corporatiu
- Notícies de l'empresa

Per construir missatges com:

«Hola, X, he vist que vas participar en el projecte X. Necessito que revisis urgentment aquest document abans de la reunió amb el teu cap (nom).»

El missatge sembla real perquè fa servir informació pública.

Hipertrucatge (*deepfake*)

Imatges, vídeos o àudios **editats o generats utilitzant** la **IA**.

- **Hipertrucatge de veu**

La IA pot clonar una veu utilitzant pocs segons d'una gravació.

Exemple:

Un treballador rep una trucada que sembla del director:
«Necessito que autoritzis aquesta transferència urgentment.»

La veu és pràcticament idèntica.

- **Hipertrucatge de vídeo**

Els atacants poden generar videotrucades falses en què sembla que hi ha:

- Un director
- Un company
- Un proveïdor

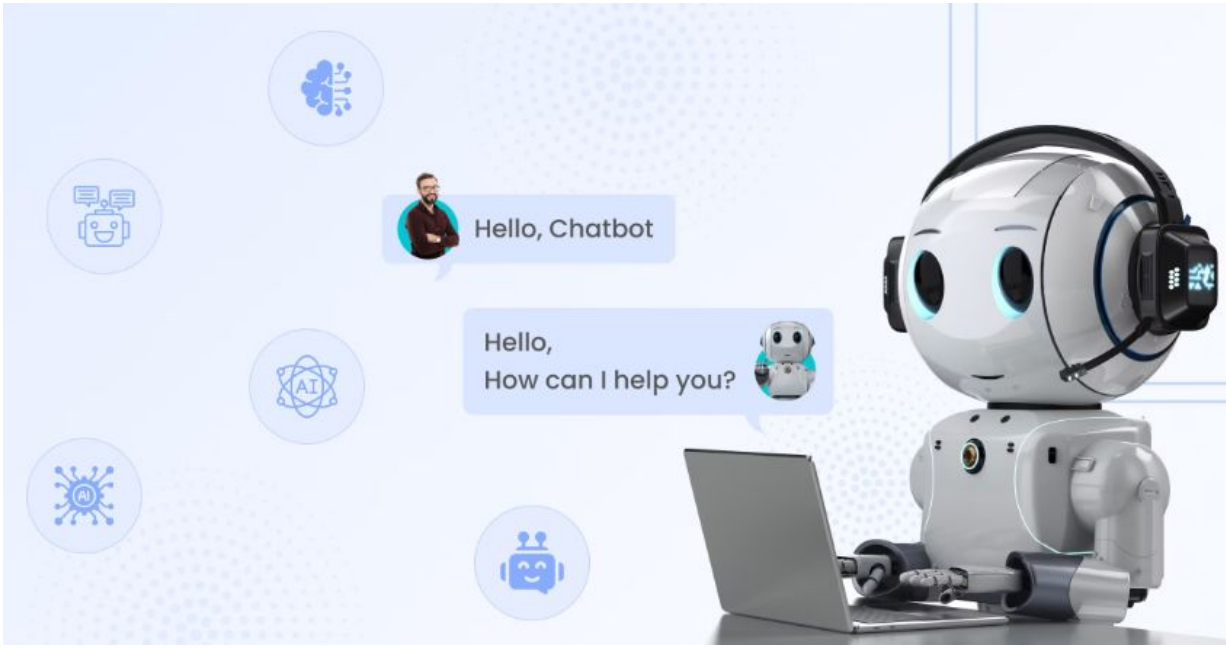
Fins i tot poden simular reunions corporatives.

Bots de conversa (*chatbots*) maliciosos

La IA permet mantenir converses convincents durant hores:

- Correu
- WhatsApp
- Teams
- Telegram

L'atacant sembla una persona real.



ANDORRA DIGITAL

ANDORRA DIGITAL
CIBERSEGURETAT

3. ATACS MÉS COMUNS POTENCIATS PER LA IA

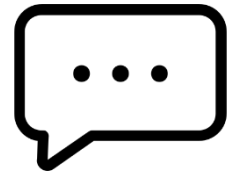
Pesca □ Correus fraudulents

- **Objectiu**
  - Robar credencials
  - Instal·lar programari maliciós
  - Obtenir informació

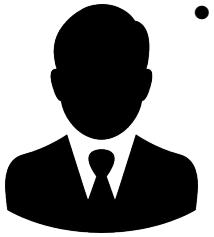
Pesca per SMS (*smishing*) □ Missatges SMS fraudulents

Exemples:

- «El seu paquet està retingut.»
- «Cal que validi el seu compte.»



Pesca dirigida (*spear phishing*) □ Atacs dirigits a una persona concreta.



- **Característiques:**
  - Molt personalitzats
  - Difícils de detectar
  - Basats en informació real

Pesca per veu (*vishing*) □ Frau mitjançant trucades telefòniques.

- La IA permet:
  - Clonar veus
  - Simular converses
  - Automatitzar respostes

Estafa del directiu (*whaling*) □Atacs dirigits a:

- Directius
- Gerents
- Personal financer

L'impacte econòmic sol ser elevat.

ANDORRA DIGITAL

ANDORRA DIGITAL
CIBERSEGURETAT

4. COM ES POT DETECTAR UN POSSIBLE ATAC

- **Sol·licituds urgents** □ La urgència cerca evitar que pensem.

«Fes-ho ara.»
«És confidencial.»
«No ho diguis a ningú.»

- **Enllaços sospitosos** □ Cal verificar sempre: domini, URL real i certificat.

SENYALS D'ALERTA

- **Peticions inusuals** □ Pregunta't:
  - És habitual aquesta sol·licitud?
  - La persona sol demanar això?
  - Està seguint el procediment normal?

- **Canvis de comportament** □ Si un company fa servir expressions estranyes, escriu de manera diferent o sol·licita accions fora del que és habitual, es pot tractar d'una suplantació.

- **Sol·licitud d'informació delicada**□ Mai no s'ha compartir:
  - Contrasenyes
  - *Tokens* AMF
  - Informació financera
  - Dades personals

ANDORRA DIGITAL

ANDORRA DIGITAL
CIBERSEGURETAT

5. COM ES PODEN PREVENIR ELS ATACS?

- **Aplicació del principi de «confiança zero»**
  - No confiïs automàticament en
    - Correus
    - Trucades
    - Missatges
    - Videoconferències

  VERIFICA-HO SEMPRE

- **Limitació de l'exposició pública**
  - Evita compartir informació. Com més informació pública existeix, més fàcil és personalitzar un atac.

- **Verificació a través d'un altre canal** - Si reps una petició sensible:
  - Truca directament.
  - Envia un Teams al contacte conegut.
  - Verifica amb una altra persona.

- **Ús de l'AMF** - L'autenticació de múltiples factors redueix significativament l'impacte del robatori de credencials.

- **Formació continuada** - La millor eina continua sent: **La conscienciació dels usuaris**

6. BONES PRÀCTIQUES PER ALS TREBALLADORS

Abans de fer clic

Pregunta't:

Espero aquest missatge?
Conec el remitent?
La sol·licitud té sentit?
Hi ha pressió o urgència?
Podria verificar-ho per un altre canal?

SI TENS DUBTES

ATURA'T, VERIFICA i CONSULTA

Abans de compartir informació

Pregunta't:

Qui la sol·licita?
Està autoritzat?
És realment necessària?

És millor cinc minuts verificant que provocar un incident de seguretat.

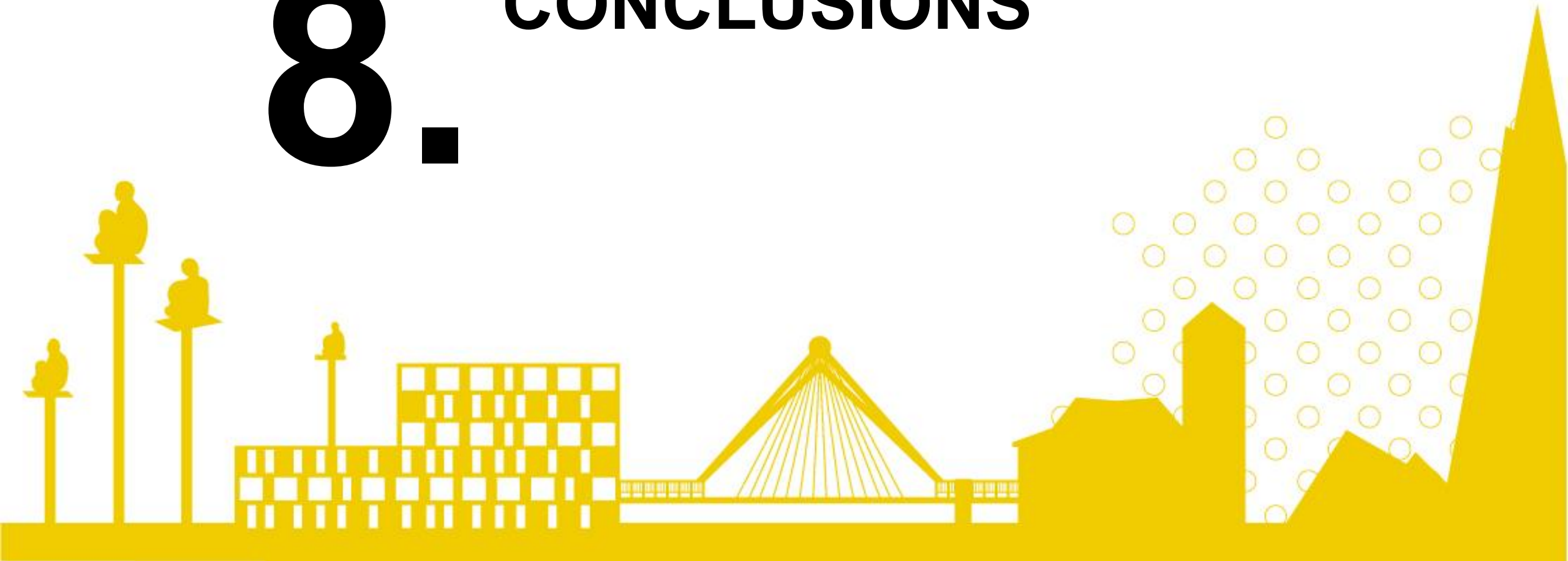
ANDORRA DIGITAL

ANDORRA DIGITAL
CIBERSEGURETAT

7. QUÈ CAL FER SI SOSPITES QUE ÉS UN ATAC?

- **No responguis.**
- **No facis clic.**
- **No descarreguis fitxers.**
- **No facilitis informació.**
- **Comunica-ho immediatament a l'equip de seguretat o TI.**
- **Conserva evidències (correu, captura de pantalla, missatge, etc.).**

8. CONCLUSIONS



- La IA no només ajuda les empreses, també ajuda els ciberdelinqüents.
- Els atacs d'enginyeria social són cada vegada més realistes i personalitzats.
- La tecnologia per si mateixa no és suficient per aturar-los.
- El pensament crític i la verificació continuen sent la millor defensa.
- Quan una sol·licitud impliqui diners, credencials o informació delicada: **«Confia menys, verifica més.»**

ANDORRA
DIGITAL