

AGÈNCIA NACIONAL DE CIBERSEGURETAT D'ANDORRA

CONSCIENCIACIÓ EN CIBERSEGURETAT

WHALING

Gener 2026
Document d'ús públic

1 ATAC D'ENGINYERIA SOCIAL: *WHALING*

2 EL *WHALING* A TRAVÉS DE LA MISSATGERIA INSTANTÀNIA (WHATSAPP)

3 RECOMANACIONS



1. ATAC D'ENGINYERIA SOCIAL: *WHALING*

QUÈ ÉS EL *WHALING*?

El *whaling* és un tipus d'atac de pesca adreçat a alts càrrecs d'empreses o d'organitzacions (públiques o privades) i també a altres persones que tenen determinats càrrecs o rols en les organitzacions.



PESCA

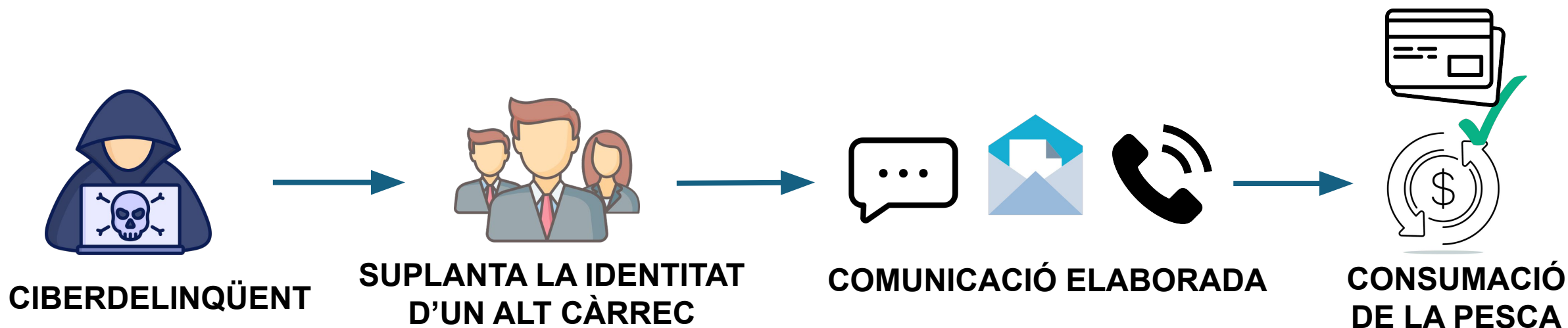
Manipulen les persones per obtenir informació delicada.

Com?

Creen un perfil fals o un enllaç enganyós □ robar contrasenyes, informació personal i/o financera.

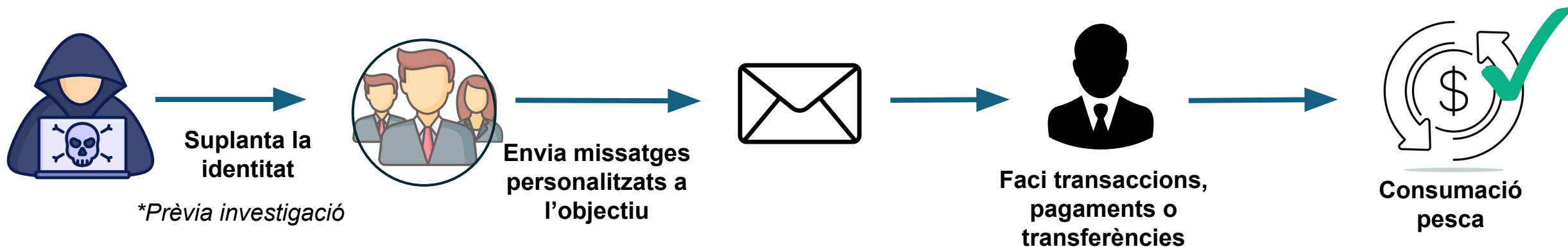


Aquest tipus de pràctiques fraudulentes es fan, generalment, via correu electrònic, tot i que també es poden dur a terme a través de missatgeria electrònica instantània (WhatsApp), missatges de text (pesca per SMS), trucades de telèfon (pesca per veu), etc. Les comunicacions estan elaborades de manera molt acurada, amb l'objectiu manipular el destinatari perquè faciliti dades delicades de la seva organització, informació personal o autoritzi pagaments i transaccions il·legítimes.



2 ■ EL *WHALING* A TRAVÉS DE LA MISSATGERIA INSTANTÀNIA (WHATSAPP)

COM ES DUU A TERME EL WHALING?



OBJECTIU DE L'ATAC

El *whaling* és un **atac de pesca** adreçat exclusivament a **executius o alts càrrecs de l'organització**.

Persones amb capacitat per poder autoritzar pagaments o transferències bancàries, transmetre informació delicada de l'organització o amb capacitat de decisió en aquesta.

El ciberatacant es fa passar per un company de l'organització, o per un amic o associat de nivell igual o inferior.

Envia missatges personalitzats.

De fet, és tan acurat el nivell de **personalització i investigació** prèvia que es fa **sobre l'objectiu** que els estafadors fins i tot espion les converses entre el remitent i l'objectiu.

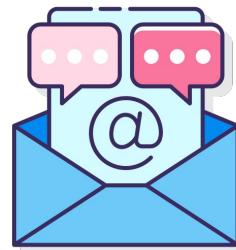
Molts atacants inclús intenten segrestar el compte de correu electrònic real del remitent per enviar el missatge d'atac directament des d'allà, i així aconseguir que sembli més autèntic.

METODOLOGIA DEL WHALING



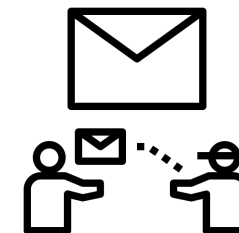
Establir l'OBJECTIU del ciberatac

- Robar informació confidencial
- Instal·lar programari maliciós
- Robar grans sumes de diners
- Robar dades delicades



Crear un MISSATGE REAL

**TRIAR +
INVESTIGAR**
l'objectiu per tal
que l'atac tingui èxit.

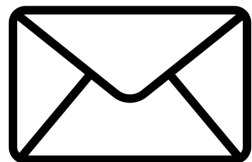


MOMENT de llançar el missatge

Els missatges més eficaços s'**interposen** en el context d'**una conversa** en curs, incloent-hi **referències detallades** d'un projecte o una oportunitat específica i presentant una situació creïble.

TÀCTIQUES D'ENGINYERIA

SOCIAL



DOMINIS DE CORREU ELECTRÒNIC FALSIFICATS

Creen dominis de correu electrònic similars.

El correu pot contenir firmes de correu electrònic copiades, declaracions de privacitat, etc.



INSISTÈNCIA EN LA CONFIDENCIALITAT

«Si us plau, no comparteixi això amb ningú de moment», amb la finalitat d'evitar que l'objectiu es comuniqui amb altres persones que puguin qüestionar la petició.



SENSACIÓ D'EMERGÈNCIA

Referències a terminis crucials o quotes endarrerides, etc. Això pot portar l'objectiu a actuar amb més rapidesa, sense considerar detingudament la petició.



PESCA PER VEU

Inclouen números de telèfon als quals l'objectiu pot trucar per obtenir una confirmació, fins i tot acompanyen els correus electrònics de pesca amb missatges de veu i es fan passar pel remitent.

3. RECOMANACIONS



Sentit comú

Si et sol·liciten **informació sensible** o que **facis una acció urgent**, utilitza **un altre mètode de comunicació per verificar-ho**: una trucada telefònica o una conversa en persona.



Revisa abans de fer clic

Compte amb **els enllaços i els arxius adjunts**. No facis clic ni obris arxius de correus electrònics que no esperis o de fonts desconegudes o no fiables.



Compte amb les urgències

Ves amb compte si es tracta d'**alguna cosa urgent** i et demanen que **no contactis amb ningú més** o que no demanis una **segona validació**, encara que sigui un alt càrrec de l'organització.



Revisa el remitent

Comprova les **adreces dels correus electrònics, els dominis i pensa per quin motiu s'han posat en contacte amb tu**.

Avís Legal

Aquest document conté informació pública.

El seu objectiu és la conscienciació en ciberseguretat pels ciutadans, empreses i entitats d'Andorra.

© Agència Nacional de Ciberseguretat d'Andorra.