ANDORRA DIGITAL

ANC-AD Agència Nacional de Ciberseguretat d'Andorra

AGÈNCIA NACIONAL DE CIBERSEGURETAT D'ANDORRA

CONSCIENCIACIÓ EN CIBERSEGURETAT

FRAU AL CEO I A LA DIRECCIÓ FINANCERA DE LES ORGANITZACIONS

Octubre 2024
Document d'ús públic

1. PESCA DE FRAU AL CEO I A LA DIRECCIÓ FINANCERA DE LES ORGANITZACIONS

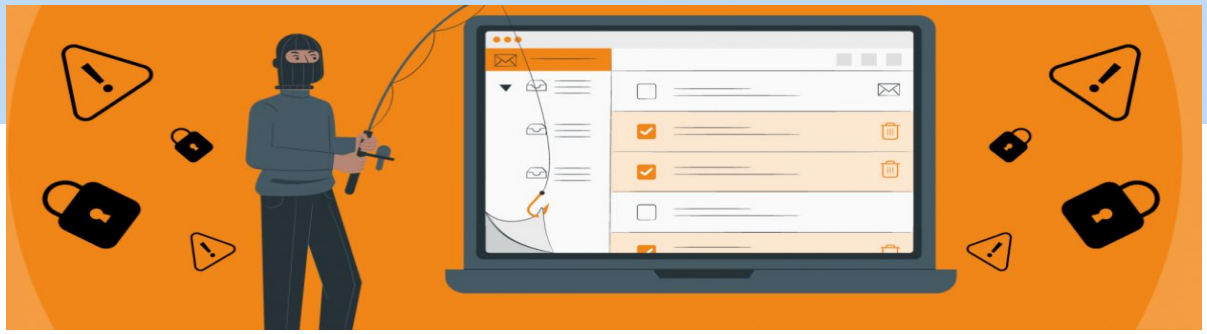
En l'àmbit dels atacs de pesca que ens podem trobar, un dels més comuns i, alhora, més important i que pot causar més perjudicis a les empreses és el del **FRAU AL CEO** i el **FRAU AL DEPARTAMENT FINANCER/COMPTABILITAT** d'una organització.

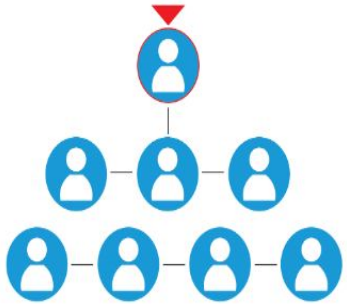
En aquest tipus d'estafa, l'atacant es fa passar pel CEO d'una organització i s'adreça a un alt càrrec d'aquesta, que, per descomptat, té accés a informació delicada i confidencial i, a més a més, té permisos per dur a terme operacions importants de caràcter econòmic i/o financer.

L'atacant, generalment, sol fer servir expressions típiques per generar **CONFIANÇA** a l'altra part, però, també, s'aprofita de la **POSICIÓ DE PODER** de la persona a qui ha suplantat, amb l'objectiu d'aconseguir que atenguin les seves demandes de manera més discreta, ràpida i diligent.

Per tant, és molt important complir en tot moment amb els **CONTROLS INTERNS** establerts a l'organització, ja sigui per a la presa de decisions clau o estratègiques o per dur a terme determinades operacions econòmiques, financeres, bancàries, etc.

Respectar, per tant, el **SISTEMA D'APROVACIÓ MÚLTIPLE** que s'hagi implementat a la companyia hauria de ser suficient per evitar aquest tipus de fraus i estafes. És important, sempre, que la **LEGITIMITAT DE LA SOL·LICITUD** quedi degudament confirmada amb el suposat remitent per un altre canal que no sigui el canal a través del qual l'hem rebuda.





Aquest tipus d'atacs contra el CEO o càrrecs importants d'una companyia es coneix amb el terme d'«estafa del directiu» o «pesca grossa» (*whaling).*

Els atacs d'estafa del directiu són sofisticats correus electrònics de suplantació d'identitat adreçats a **ALTS EXECUTIUS I PERSONES AMB CÀRRECS IMPORTANTS d'una companyia:**

- *Executius d'alt nivell, membres del Consell d'Administració, etc.*
- *Caps de departaments com RH, Vendes, Legal, Compres, etc.*
- *Càrrecs de gran visibilitat, com portaveus i personal influent dins d'un sector específic.*

A diferència de les estafes de pesca, que no tenen un **OBJECTIU ESPECÍFIC,** i de la pesca dirigida (s*pear phishing)*, que té com a objectiu **PERSONES ESPECÍFIQUES,** l'estafa del directiu porta l'atac al nivell següent, atès que no només va adreçat a persones importants de la companyia, sinó que també es fa de manera que sembli **que les comunicacions fraudulentes provenen d'una persona molt influent o que té un càrrec de nivell superior a l'organització**.

El nom d'«estafa del directiu» o «pesca grossa» (*whaling*, en anglès) fa referència, per tant, a l'**atac específic adreçat als «peixos grossos» de les companyies**, com, per exemple, al director executiu (CEO) o al gerent de Finances. Això incorpora un element d'enginyeria social a l'atac, ja que els treballadors se senten en l'obligació de respondre a les sol·licituds d'una persona que consideren important.

Com funcionen els atacs d'estafa del directiu i com et pots protegir

Els atacs d'estafa del directiu són:

- ***Missatges ben dissenyats i redactats**, capaços d'enganyar els més previnguts.*
- ***Llenguatge** que s'ajusta al de l'objectiu.*
- ***Situacions creïbles i urgents**, com qüestions normatives o legals.*

Una de les estratègies podria ser un correu electrònic que sembli que prové d'algun cap de la direcció de l'empresa i en el qual l'atacant faci al·lusió a determinada informació que ha obtingut en línia. Per exemple, que l'adreça de correu electrònic del remitent sembli legítima i, fins i tot, que en el correu s'inclogui el logotip de la companyia o vincles a llocs web fraudulents i dissenyats per semblar que són reals.

Atès que aquests «**peixos grossos**» solen tenir **molta credibilitat** i un **gran nivell d'accés** a l'organització, l'atacant té una molt bona justificació per esforçar-se a dissenyar els atacs de manera que semblin més creïbles.

La primera **estratègia** per resguardar-se dels atacs d'estafa al directiu o pesca grossa és **educar les persones importants de l'organització** perquè vigilin davant la possibilitat de ser víctimes d'aquests atacs.

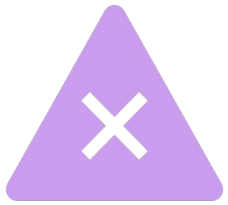
Cal que sempre s'autoformulin algunes preguntes com ara si ***esperaven rebre un correu electrònic, un fitxer adjunt o un enllaç relacionat amb aquell remitent i amb aquell contingut; si la sol·licitud té alguna cosa estranya...***

De fet, només posant el **cursor sobre el nom del remitent en un correu electrònic**, es pot veure quina és l'adreça de correu electrònic completa.

D'altra banda, els executius i la direcció de l'organització han de tenir **especial cura a l'hora de publicar i compartir informació a través de les xarxes socials** (Facebook, Twitter i LinkedIn), ja que els atacants poden fer servir qualsevol mena d'informació personal seva, com, per exemple, la data del seu aniversari, aficions, vacances, càrrecs laborals, ascensos i relacions, per dissenyar atacs molt més sofisticats i personalitzats.

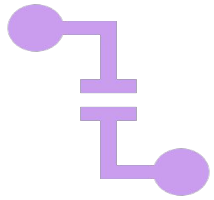
RECOMANACIONS

Com pots actuar davant d'aquests fraus?



No responguis missatges sospitosos i, per descomptat, no facis cas de peticions si dubtes de la identitat del remitent.

En cas de dubte, posa't en contacte amb el suposat remitent per un canal diferent o contacta el teu superior directe.



No entris a enllaços sospitosos, ni obris documents adjunts sense haver-los revisat prèviament amb una eina de programari antimaliciós.

Respecta en tot moment els controls interns establerts a la companyia, especialment els adreçats a prevenir els atacs de frau.

EXPRESSIONS TÍPIQUES QUE ENS PODEM TROBAR EN AQUEST TIPUS DE FRAUS

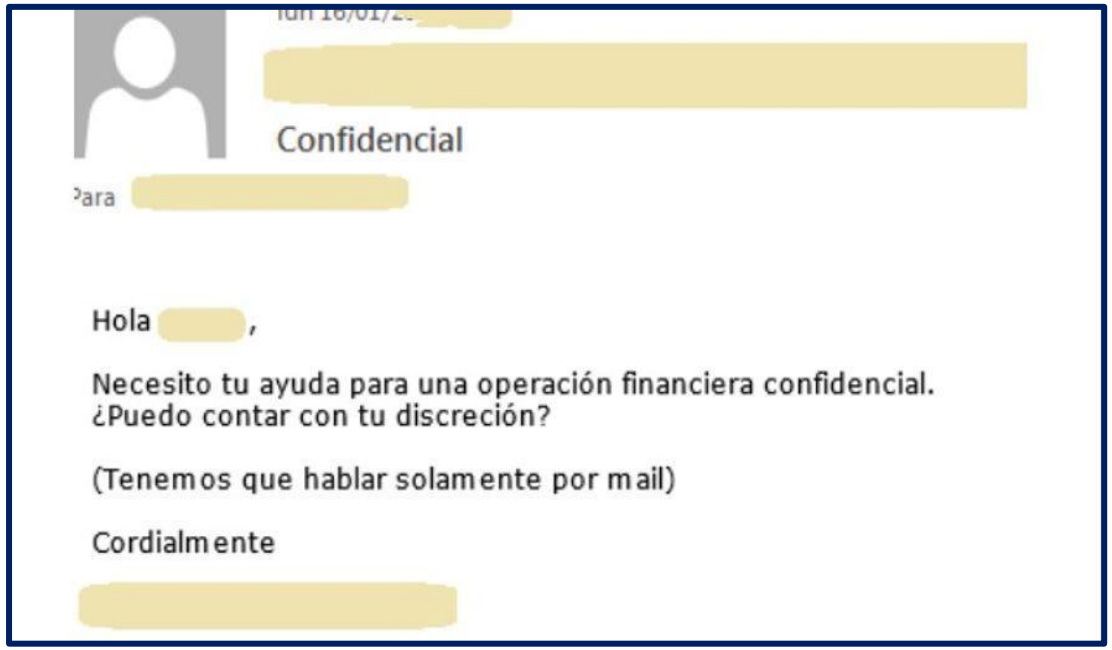
«T'informo que t'encarregaràs del tractament d'una operació financera confidencial…»

«Envia'm, si us plau, el saldo actual dels nostres comptes corrents. És urgent…»

«Necessito, si us plau, que facis una transferència bancària, perquè haig d'agafar un avió ara mateix i no podré fer-la…»

«Si us plau, em pots atendre aquesta tarda amb prioritat?»

2. EXEMPLES DE POSSIBLES INTENTS DE PESCA QUE POT REBRE EL CEO I EL DEPARTAMENT FINANCER D'UNA COMPANYIA



Confidencial

Para

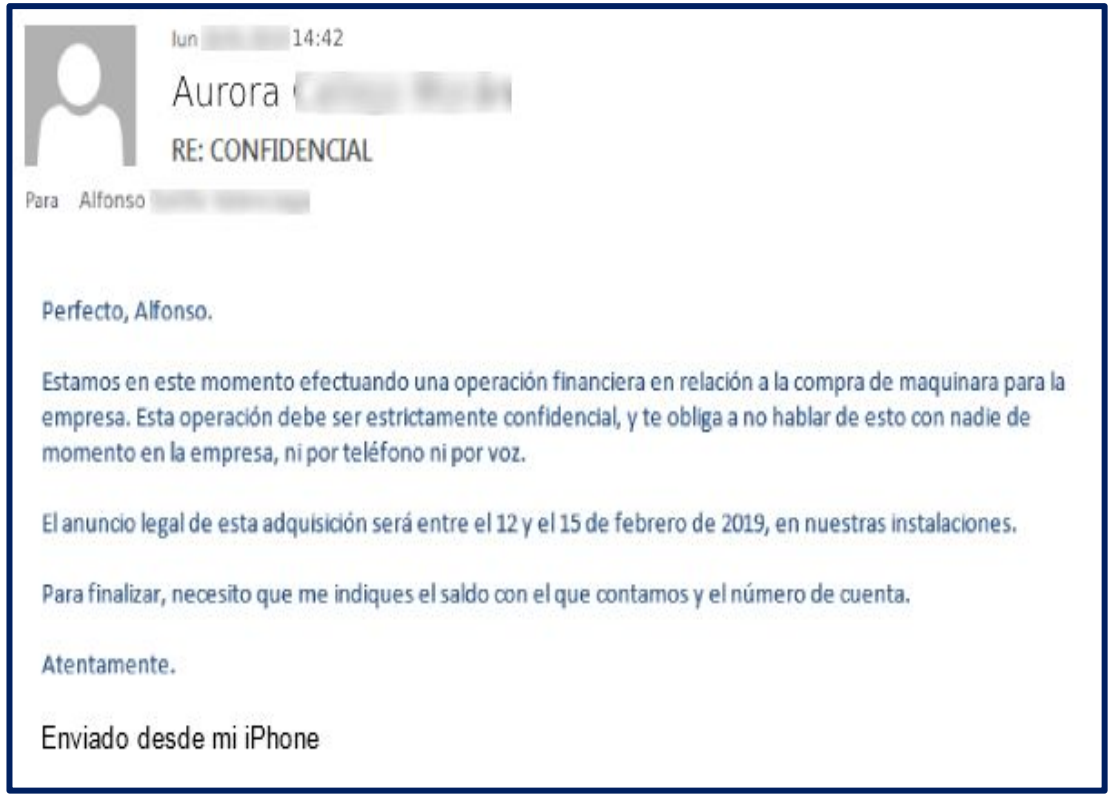
Hola ,

Necesito tu ayuda para una operación financiera confidencial.
¿Puedo contar con tu discreción?

(Tenemos que hablar solamente por mail)

Cordialmente

Cerquen COMPLICITAT, DISCRECIÓ i URGÈNCIA.



lun 14:42

Aurora

RE: CONFIDENCIAL

Para Alfonso

Perfecto, Alfonso.

Estamos en este momento efectuando una operación financiera en relación a la compra de maquinara para la empresa. Esta operación debe ser estrictamente confidencial, y te obliga a no hablar de esto con nadie de momento en la empresa, ni por teléfono ni por voz.

El anuncio legal de esta adquisición será entre el 12 y el 15 de febrero de 2019, en nuestras instalaciones.

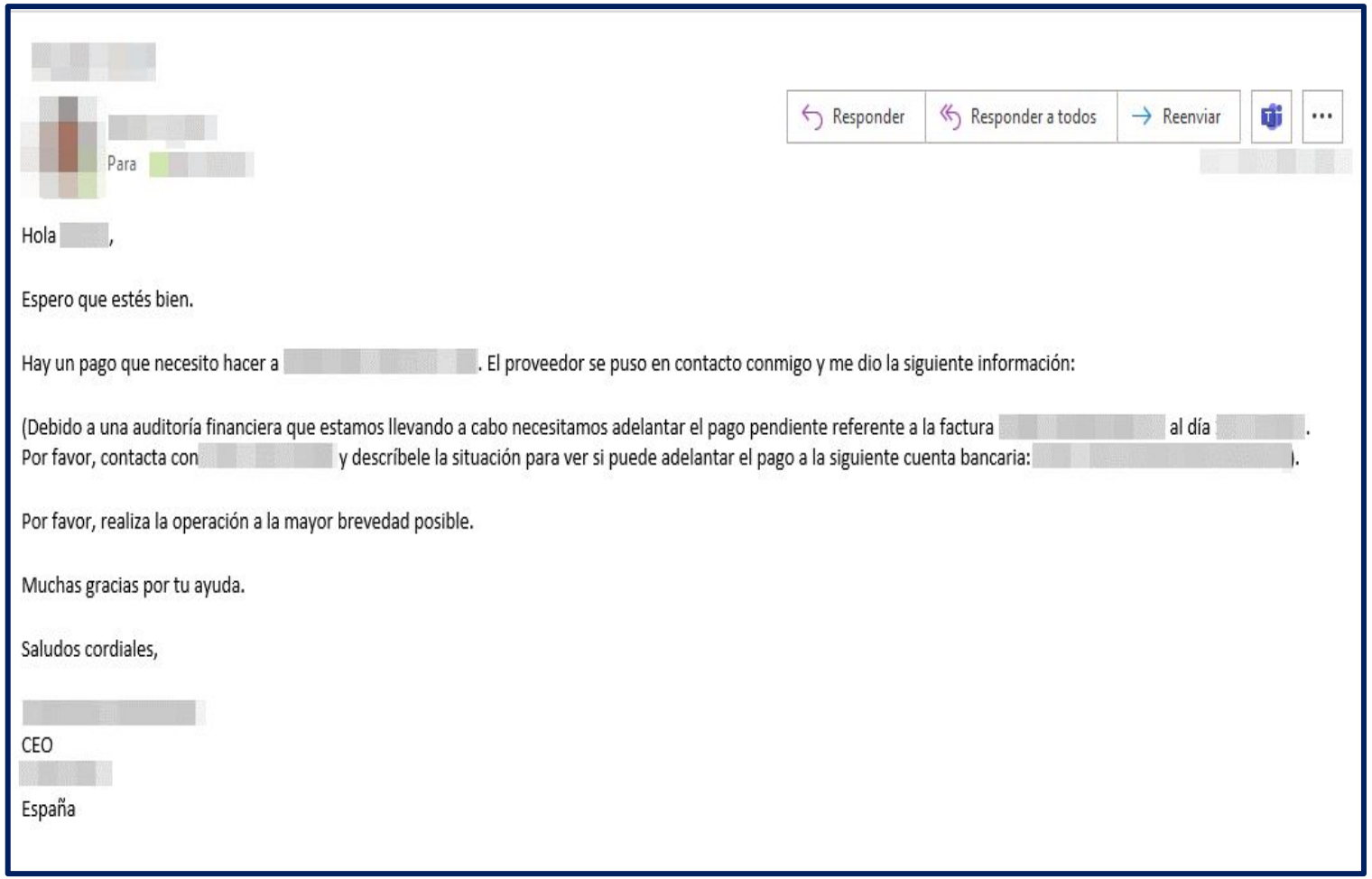
Para finalizar, necesito que me indiques el saldo con el que contamos y el número de cuenta.

Atentamente.

Enviado desde mi iPhone

Quan l'atac és dirigit (***spear phishing***), el delinqüent sol disposar de més informació per reforçar l'**ENGANY.**

Pot haver aconseguit la informació de fonts obertes, com, per exemple, **LinkedIn, Facebook, Instagram**, d'una **intrusió anterior** en la qual es va vulnerar la seguretat dels comptes personals de la persona a qui es dirigeix l'atac, o si es van vulnerar els **sistemes d'informació** de l'organització o de **tercers relacionats**.



3. NOVA MODALITAT DE PESCA: ESTAFA DE LES TARGETES BANCÀRIES (*CARDING*)

Compte amb l'estafa de les targetes bancàries, poden robar-te les dades de la teva targeta de crèdit!!

L'estafa de les targetes bancàries és un **tipus de frau** que agafa informació de **targetes de crèdit robades** i la fa servir de manera **fraudulenta**.

1. Tècniques emprades pels atacants per obtenir les dades de les targetes de crèdit

- *Usuaris víctimes de fraus com pesca, pesca per SMS, pesca per veu, etc.*
- ***Distribució de programari maliciós** capaç de capturar les pulsacions del teclat.*
- ***Bases de dades de clients i usuaris de webs** la seguretat de les quals s'hagi vulnerat.*
- ***Webs fraudulents** en els quals els usuaris han introduït les seves dades bancàries.*
- *Ús de **lectors amb comunicació sense fil RFID o NFC** capaços d'obtenir les dades de la targeta de crèdit.*

2. Procediment d'actuació

Un cop aconseguides les dades de la targeta, els atacants fan compres per verificar que la informació que han replicat a la seva targeta virtual és **vàlida**. Per regla general, comencen fent petites compres de productes amb un import baix i, a poc a poc, en van augmentant l'import.

Cal tenir en compte que, generalment, l'estafa de les targetes bancàries augmenta en els períodes de les principals campanyes comercials (Nadal, rebaixes, Black Friday…), aprofitant la **sobrecàrrega de transaccions bancàries**. Per la qual cosa, et recomanem que vigilis especialment durant aquestes dates, per evitar que et facin **càrrecs econòmics indeguts i il·legítims** al compte.

Consells per protegir-te d'aquest frau:

1. No facis cas dels missatges ***spam*** o correus electrònics amb **remitents desconeguts**.
2. **Controla** regularment les **teves operacions i transaccions bancàries**.
3. **Desactiva el sistema NFC del teu mòbil** mentre no el facis servir.
4. Quan facis compres en línia, assegura't bé que la botiga en qüestió és de confiança i que utilitza una **passarel·la de pagament o accepta mètodes de pagament segur**.
5. Fes servir les **targetes virtuals** que t'ofereix el banc a l'hora de fer pagaments en línia.
6. **Deshabilita a l'aplicació del teu banc l'opció d'NFC i RFID** si no utilitzes aquest mètode de pagament.
7. No donis en cap cas les **dades bancàries per telèfon**.
8. No utilitzis **ordinadors públics** per fer compres.
9. Actualitza els **programes i** les **aplicacions** que utilitzes amb freqüència.
10. Activa l'**autenticació de doble factor** per als pagaments amb targeta de crèdit.

Avís Legal

Aquest document conté informació pública.

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