Govern d'Andorra

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

Phishing i frau

Conscienciació en ciberseguretat

Març de 2022

ÍNDEX

1. Que és el phising?

Que és el phishing?

El **phishing és una tipologia d'atac basada en l'art de l'engany** que utilitzen els ciberdelinqüents **per robar diners, aconseguir informació confidencial o amb caràcter general perpetrar accions llegítimes.**

L'atac es **desenvolupa a través del correu electrònic i es recolza amb l'ús de tècniques per suplantar a persones de l'entorn o entitats llegítimes** com pot ser un banc, un client o proveïdor, una administració pública, una xarxa social, etc.

Igualment, busquen explotar les següents vulnerabilitats de les persones:

- La **tendència a ajudar** a altres persones.
- La **dificultat per dir que no** (sobretot quan l'engany és capaç d'induir un abús d'autoritat).
- **L'excés de confiança** d'altres persones, sobretot en l'àmbit professional.
- La **satisfacció** de ser **afalagat** i **valorat** pel nostre treball.

1. Que és el phising?

Pretextes habituals

Proporcionar/actualitzar informació per completar algun procés requerit legalment o d'interès per l'usuari o de l'Organització.

Realitzar pagaments urgents, participar a sortejos

Verificar o actualitzar credencials per labors de manteniment, millora de la seguretat, sol·licitud de serveis addicionals, etc.

Registrar-se o realitzar alguna acció telemàticament amb motiu d'actualitat (campanya de la renda, vacunació, actuacions de la direcció de tràfic, etc.)

Hi haurà situacions en les quals el delinqüent no elabori atacs molt sofisticats i/o dirigits, però en altres ocasions podria haver recollit la suficient informació i haver desenvolupat molt els mitjans per augmentar les possibilitats d'èxit en l'engany.

ÍNDEX

2. Com podem identificar un phishing?

Com podem identificar un phishing?

Hem d'estar atents a ...

OBJECTIU: L'objectiu pot ser mogut per interessos il·lícits? Surt de la tònica habitual?

És comú que els atacants ens vulguin enganyar per a fer una operació financera o per a obtenir informació confidencial. Molt important verificar amb el remitent a través d'un altre canal de comunicació qualsevol petició no usual, així com respectar sempre els controls implantats per processos.

ASSUMPTE: L'assumpte capta la teva atenció?

La majoria de correus fraudulents utilitzen assumptes cridaners com ganxo per captar l'atenció.

ENLLAÇOS EXTERNS: S'inclouen enllaços a llocs externs?

És habitual que s'incloguin enllaços a llocs que suplantin webs llegítimes o que simplement utilitzant com llançadores d'atacs. Situant el cursor a sobre de l'enllaç podem veure l'URL real. És recomanable contrastar amb la direcció/domini oficial que podrem localitzar a través d'un buscador web.

Si han acurtat els enllaços és important obtenir l'URL completa per verificar la seva legitimitat.

2. Com podem identificar un phishing?

Com podem identificar un phishing?

Hem d'estar atents a ...

REMITENT DESCONEGUT o SOSPITÓS: Esperaves un email d'aquesta persona o entitat? La direcció és coneguda o resulta sospitosa?

Encara que els atacants poden tenir informació sobre nosaltres i la nostra activitat, i poden arribar a suplantar a persones o entitats, un remitent sospitós (en conjunt amb l'assumpte i l'objectiu) deu ser el primer que ens ha de fer sospitar. Important fixar-se en la direcció/domini des de la que ens escriuen: moltes vegades utilitzant paraules lleugerament diferents (substituint alguns caràcters).

A vegades també poden aprofitar-se de vulnerabilitats tècniques per aparentment usar una direcció llegítima. L'ús d'aquesta tècnica anomenada email spoofing pot detectar-se analitzant les capçaleres (atributs de l'email). Haurem de fixar-nos també en la firma del correu. La seva absència o canvi respecte a la que podem conèixer és un indicador de possible frau.

COS DEL CORREU: Està mal redactat o sembla una mala traducció?

Si el correu no està personalitzat, utilitza de forma errònia expressions, té frases mal estructurades i faltes d'ortografia, o inclòs presenta algunes paraules o expressions en un altre idioma, són indicis d'un atac fraudulent.

ADJUNTS:
S'inclouen arxius adjunts no esperats o sospitosos?

Els atacants solen adjuntar documents (normalment de tipus ofimàtic) que tenen incrustat codi maliciós per a desenvolupar l'atac. A vegades podríem ser requerits a activar unes certes funcions (com les macros) que possibilitaran la seva execució. Una bona pràctica és analitzar els arxius adjunts abans d'obrir-los amb el programari antivirus.

ÍNDEX

3. Email spoofing

Una mala configuració facilita la suplantació tècnicament

ELS ATACANTS PODEN APROFITAR VULNERABILITATS TÈCNIQUES PER A SUPLANTAR L'ADREÇA DEL REMITENT
En cas que els atacants utilitzin aquesta tècnica tenim possibilitats d'identificar el frau si analitzem les capçaleres dels correus. És a dir, els registres del trànsit de la comunicació entre el servidor de correu remitent i el destinatari.

Analitzant les capçaleres podem identificar:

- La informació relativa a l'emissor (tant l'adreça de remitent com l'usuari que el va enviar) i al receptor
- Els servidors de correu intermedis pels quals passa el missatge des de l'origen fins a la seva destinació
- El client de correu que es va utilitzar per a enviar-lo
  Les dates i hores d'enviament i recepció.

L'usuari "remitent" i l'autenticat en el servidor de correu origen no són el mateix.

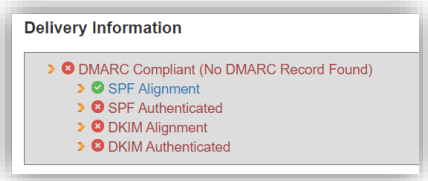
Headers Found

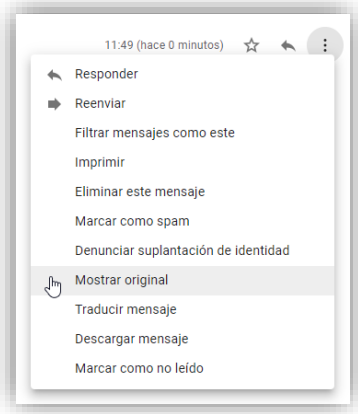
Header Name	Header Value
Return-Path	
Received-SPF	none receiver=mail.alkar.net; client-ip= envelope-from=
Message-ID	<d42874f4e305f177cd0bf1325d907371.squirrel@webmail.bayyus.net>
Date	Fri, 20 Apr 2018 11:34:08 +0100
Subject	
From	Group < @ com>
To	
CC	< @ ma.com.ua>
Reply-To	<purchase@optnusa.com>
User-Agent	SquirrelMail/1.5.2 [SVN]
Content-Type	text/plain; charset="utf-8"
Content-Transfer-Encoding	quoted-printable
X-AntiAbuse	This header was added to track abuse, please include it with any abuse report
X-Get-Message-Sender-Via	cpan8.webline-servers.com: authenticated_id: purchase@bayyus.net
X-Authenticated-Sender	cpan8.webline-servers.com: purchase@bayyus.net
MIME-Version	1.0

Com visualitzar les capçaleres en GMAIL?

En les opcions del mateix correu hem de triar 'Mostrar original'. Després, podem analitzar les capçaleres directament o donant-nos suport en serveis web com mxtoolbox.com, el qual ens avisarà d'indicadors de filtres que no compleix el correu:

Per visualitzar la capçalera en Outlook: Missatge > Accions > Altres accions > Veure codi font





També configurant una direcció de resposta diferent i menys sospitosa.

Exemple 1

En aquest cas la direcció sembla d'un domini legítim.

El primer indicatiu de sospita ha de ser el fet que no es tingui cap activitat o operació pendent amb el suposat remitent.

El missatge té una falta de personalització i redacció deficient. Un altre indicatiu que el missatge no és legítim

Desplaçant el punter sobre l'enllaç podríem veure la direcció completa i comparar-lo amb la legítima. Si no la coneixem amb una simple cerca en Google podríem obtenir-la per a realitzar la comparació.

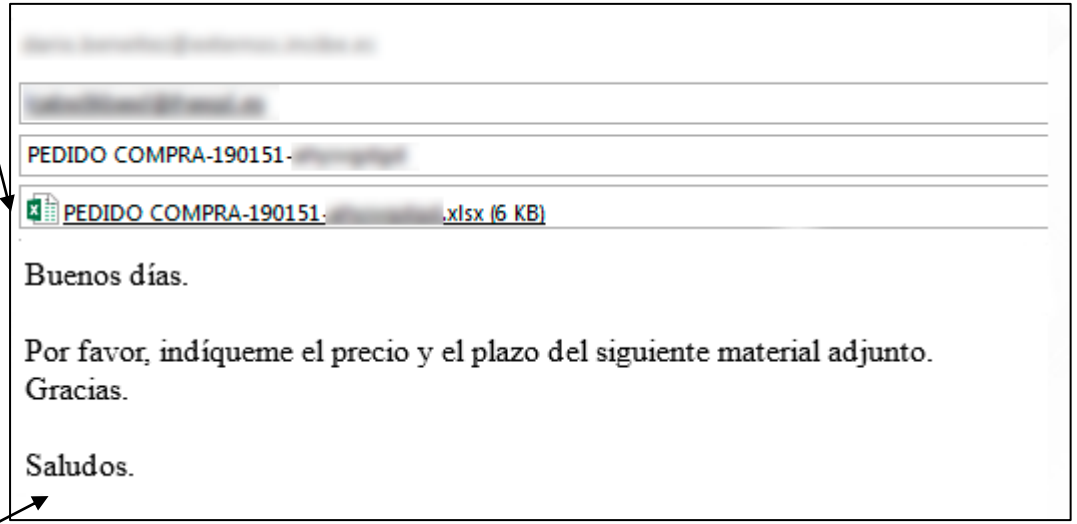
Mai hem de punxar sobre l'enllaç, ja que podríem infectar l'equip i obrir una bretxa per a una intrusió.

imagen: OSI

Exemple 2

Si el missatge és sospitós mai s'han d'obrir fitxers adjunts.

Els atacants solen adjuntar fitxers
amb codi maliciós per infectar els nostres equips



La falta d'una signatura corporativa en un primer correu d'una organització als seus clients és molt sospitós.

També la falta de detalls de tancament, entre ells com contactar si es requereix més informació.

imagen: incibe

Exemple 3

Direcció sospitosa i assumpte que busca captar ràpidament l'atenció.

Aquest tipus de campanya de phishing es llança a qualsevol usuari i es caracteritzen per la falta de personalització.

És cert que alguns phishing són molt elaborats i poden arribar a calcar l'estructura original.

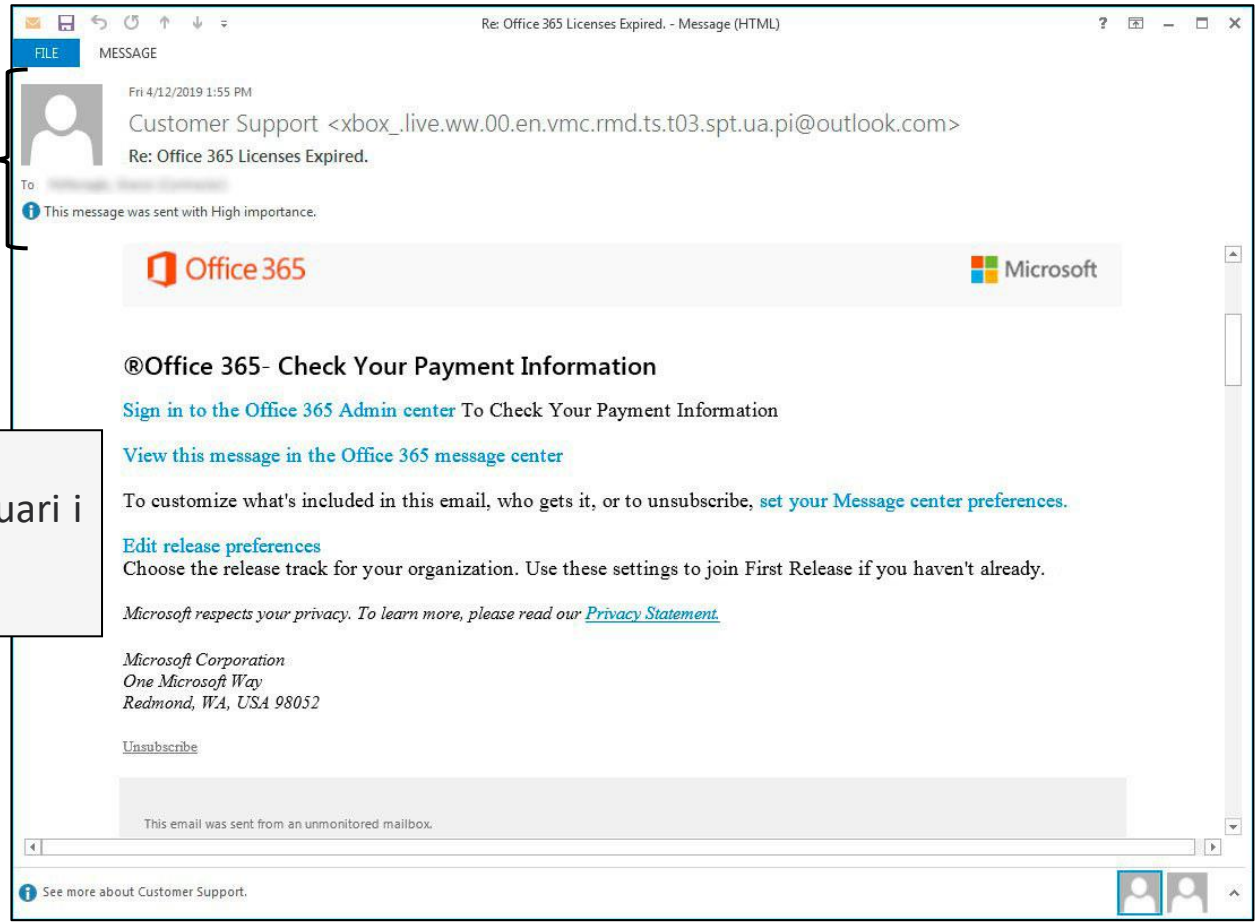


imagen: BleepingComputer

ÍNDEX

4. Frau del CEO

No et fiïs de ningú... ni del teu cap!

És habitual que l'atacant doni a entendre que les comunicacions es donen des d'un dispositiu mòbil. També es solen utilitzar serveis de missatgeria com WhatsApp.

EXPRESIONS TÍPIQUES

"T'informo que el tractament d'una operació financera confidencial serà tractada per tu..."

"Pots atendrem aquesta tarda amb prioritat?"

"Necessito que facis una transferència, vaig a agafar un avió ara i no podré atendre't..."

"Envia'm el saldo dels nostres comptes corrents a dia d'avui, es urgent..."

Dins dels atacs phishing, un dels més comuns és el FRAU DEL CEO

En aquesta estafa l'atacant es fa passar pel CEO d'una empresa, i es dirigeix a un alt càrrec amb accés a informació sensible i amb permisos per a fer operacions financeres.

L'atacant usarà expressions per a generar confiança, però també s'aprofitarà de la posició de poder del suplantat per a aconseguir que li atenguin de manera discreta i diligent.

És molt important COMPLIR EN TOT MOMENT AMB ELS CONTROLS INTERNS, especialment els dirigits per a mitigar el frau. Respectar el sistema d'aprovació múltiple que estigui implantat, i davant qualsevol situació anòmala hauria de confirmar-se la legitimitat de la sol·licitud amb el supòsit remitent per UN ALTRE CANAL DE COMUNICACIÓ o amb el nostre superior directe.

Exemples Frau del CEO

Confidencial

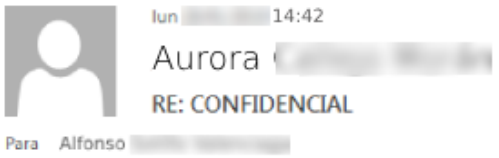
Para

Hola ,

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

(Tenemos que hablar solamente por mail)

Cordialmente



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.

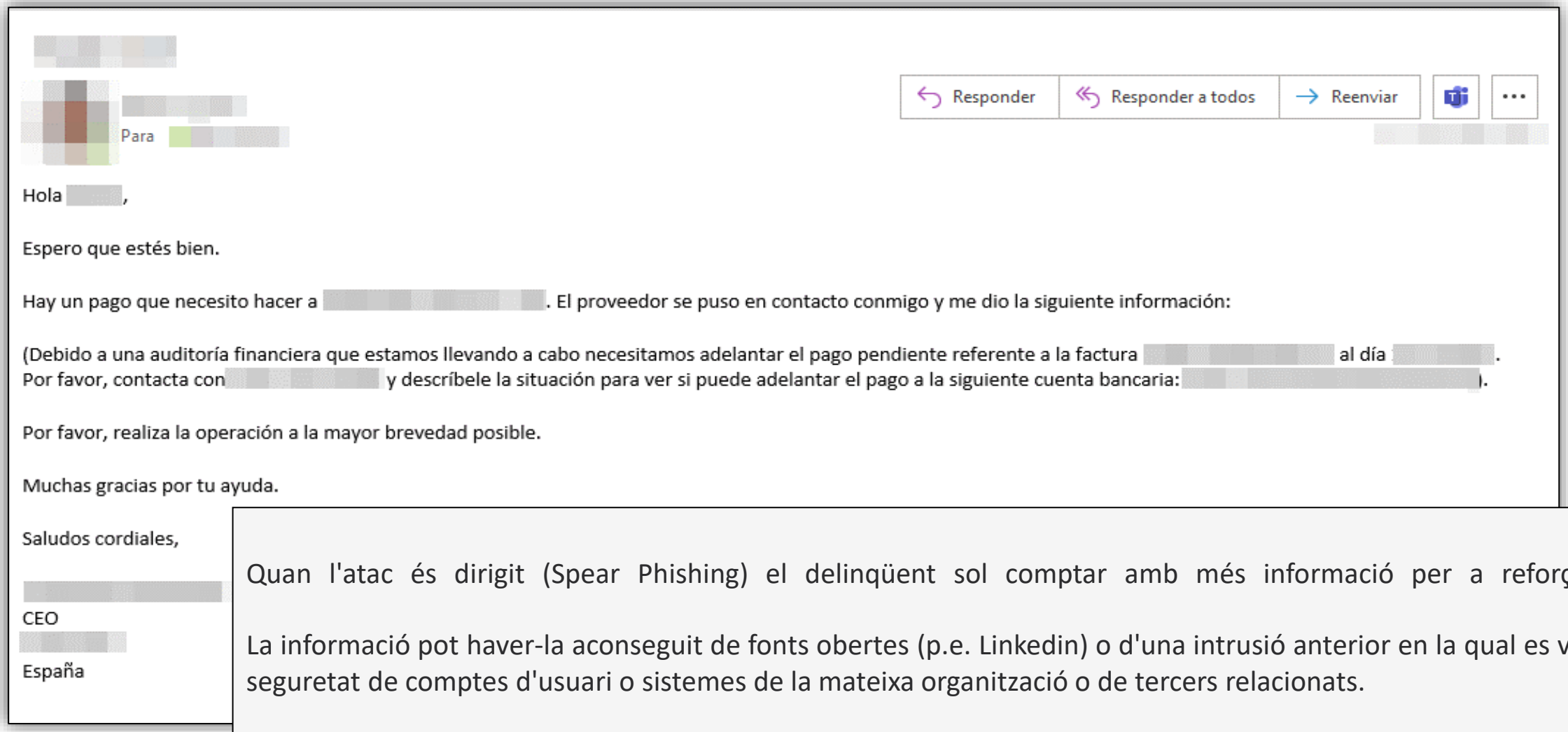
Atentamente.

Enviado desde mi iPhone

Els atacants busquen també informació confidencial per donar-li continuïtat al frau.

Busquen complicitat, discreció i urgència.

Exemples Frau del CEO



Responder | Responder a todos | Reenviar | ...

Para

Hola ,

Espero que estés bien.

Hay un pago que necesito hacer a . El proveedor se puso en contacto conmigo y me dio la siguiente información:

(Debido a una auditoría financiera que estamos llevando a cabo necesitamos adelantar el pago pendiente referente a la factura al día .
Por favor, contacta con y descríbele la situación para ver si puede adelantar el pago a la siguiente cuenta bancaria:).

Por favor, realiza la operación a la mayor brevedad posible.

Muchas gracias por tu ayuda.

Saludos cordiales,

CEO

España

Quan l'atac és dirigit (Spear Phishing) el delinqüent sol comptar amb més informació per a reforçar l'engany.

La informació pot haver-la aconseguit de fonts obertes (p.e. Linkedin) o d'una intrusió anterior en la qual es va vulnerar la seguretat de comptes d'usuari o sistemes de la mateixa organització o de tercers relacionats.

ÍNDEX

5. Com actuar en aquests casos? Recomanacions

No responguis missatges sospitosos ni molt menys atenguis peticions si dubtes del remitent En cas de dubte contacta el supòsit remitent per un altre canal o amb el teu superior directe.

No accedeixis a enllaços sospitosos ni obris documents adjunts sense haver-los revisat amb eines antimalware.

Respecta en tot moment els controls interns de l'Organització, especialment els dirigits a prevenir el frau.

imagen: Freepik.com

Govern d'Andorra

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

ANDORRA
DIGITAL

Entitats col·laboradores

andorra
telecom

DAND
DIGITALAND by Ibermática | TIN