ANDORRA DIGITAL

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

L'impacte dels correus maliciosos en les micropimes i els autònoms

TLP: WHITE

AGOST 2025

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	28/08/2025	01/09/2025

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

Els petits negocis s'han erigit en l'objectiu principal dels ciberdelinqüents i un dels mitjans principals per atacar-los és el correu electrònic, especialment mitjançant campanyes de pesca o tècniques de suplantació (spoofing).

Aquest frau consisteix a suplantar la identitat d'una persona o organització i, generalment, l'objectiu és que els receptors dels correus descarreguin algun arxiu, facin clic a un enllaç o, simplement, segueixin les indicacions dels atacants, sigui per modificar el número del compte al qual s'ha d'enviar una transferència o fer el pagament d'una factura falsa.

La raó per la qual les micropimes i els autònoms estan en el punt de mira és deguda al fet que disposen d'un grau més petit de maduresa en ciberseguretat, sigui per manca de recursos o per manca de conscienciació. Això, alhora, es tradueix en una probabilitat més gran que un atac acabi tenint èxit.

Tot seguit, s'exposaran els tipus principals de suplantació (spoofing), com es duen a terme i com es poden identificar.

3. EL PERILL DELS CORREUS MALICIOSOS: DE LA PESCA A LA SUPLANTACIÓ

L'ús de correu electrònic està integrat dins de l'operativa de qualsevol organització, per petita que sigui, sigui per comunicar-se amb els proveïdors o amb els clients.

Per això s'ha convertit en un dels riscos principals per a les pimes, micropimes i autònoms, perquè és el vector predilecte dels ciberdelinqüents.

A més, els atacants han anat evolucionant la manera d'enganyar els receptors dels correus electrònics per aconseguir els seus objectius. I dues de les tècniques més prevalents i amb un impacte més gran són la pesca i la suplantació.

3.1. Sobre la pesca

No cal aprofundir molt sobre en què consisteix la pesca perquè probablement és una de les tècniques de ciberatac més populars. De fet, ja sigui a nivell personal o professional, qualsevol usuari ha patit un intent d'atac d'aquesta mena.

Mitjançant un correu electrònic s'intenta enganyar el receptor amb l'objectiu que faciliti dades personals, contrasenyes, informació delicada, o alguna cosa similar, fent-se passar per un remitent legítim com ara un banc, un client o un membre de la mateixa organització.

Algunes de les variants de la pesca més utilitzades són la pesca dirigida (*spear phishing*), la pesca grossa (*whaling*), l'estafa del correu professional (BEC), la pesca per SMS (*smishing*) o la pesca per veu (*vishing*).

3.2. La suplantació o l'*spoofing*: què és i quines variants té

La coneguda com a *email spoofing* és una tècnica basada en enginyeria social que s'orienta a la suplantació d'identitat d'un correu electrònic. És a dir, a diferència de la pesca aquesta tècnica se sosté en la falsificació del correu electrònic remitent.

L'objectiu és que el receptor, atesa la confiança que li genera el remitent, acabi fent allò que vol l'atacant.

3.2.1. Tipus de suplantació basats en correu electrònic

Aquesta tècnica de suplantació es pot dur a terme de diverses maneres, i se n'identifiquen 5 modalitats amb característiques pròpies.

- **Suplantació mitjançant domini similar**: aquesta variant es coneix com a «looalike domain spoofing» i es basa a fer servir un correu fals en el qual apareix un domini que se sembla molt a aquell que es pretén suplantar. Per a això, l'atacant fa servir un domini de gran

similitud ortogràfica/tipogràfica, que ha registrat prèviament. Per exemple, fer servir un compte de correu amb domini «@microsft.com» en lloc de «@microsoft.com».

- **Spoofing mitjançant suplantació de nom**: en aquest cas allò que se suplanta és ell nom del destinatari i també es coneix com a «Display Name spoofing». I consisteix a enganyar la vista amb el nom del remitent, com a l'exemple següent:

  De: "Suport Apple" <suport.apple@gmail.com>

- **Spoofing mitjançant domini legítim sense compromís real**: en aquest cas el ciberdelinqüent falsifica l'adreça "From" a l'encapçalament del correu i fa servir el domini real. Tanmateix, ho fa sense tenir accés real al servidor de correu. Per a això sol ser necessària una mala configuració dels protocols SPF, DKIM i DMARC.

- **Spoofing mitjançant domini legítim amb compromís real:** es tracta del conegut com a Business Email Compromise (BEC). I en aquesta variant els ciberdelinqüents fan servir un compte veritable per llançar l'atac que prèviament ha compromès i que tenen sota control. Per a això, prèviament se li han robat a l'usuari legítim al qual pertany, sigui mitjançant l'obtenció de les seves credencials, amb la infecció amb algun programari maliciós o algun altre mètode similar. Estaríem davant del tipus de suplantació més perillós atès que en fer-se servir un compte veritable, les validacions tècniques SPF, DKIM i DMARC es passen sense problemes.

- **Suplantació interna:** en aquesta darrera variant els ciberdelinqüents aconsegueixen enviar correus falsos entre comptes dins de la mateixa organització sense haver compromès cap compte. I, una altra vegada, això és possible quan no s'ha configurat correctament el servidor de correu.

4. CARACTERÍSTIQUES DE L'*EMAIL SPOOFING*

4.1. Víctimes múltiples

En primer lloc, cal tenir en compte que és un tipus d'atac en el qual, com a mínim, sempre hi ha dues víctimes: la persona suplantada i la persona a la qual s'adreça el correu electrònic.

4.2. Es basa en la manipulació psicològica

Aquest punt és transversal a gairebé tots els mètodes d'estafa basats en enginyeria social. L'èxit d'un atac de suplantació rau a fer creure que el correu és legítim. Per a això, els ciberdelinqüents poden jugar amb diferents elements com ara:

- La urgència: molts d'aquests correus apressen els receptors a executar una acció de manera ràpida mitjançant alguna excusa creïble que obliga el receptor a haver de prendre una decisió, generalment delicada, sense gairebé temps de pensar-hi.
- L'autoritat: també es veu amb freqüència i generalment es basa en les jerarquies que hi ha a les organitzacions. Aquí el que cerca l'atacant és que el receptor faci allò que li indica un superior suplantat.
- Disseny i format: a més, l'ús de plantilles que simulen la identitat visual de l'organització que es tracta de suplantar ajuda a fer molt més creïble el correu que envia l'atacant.

4.3. No cal un gran coneixement tècnic

Aquest factor fa possible que pugui ser una tècnica utilitzada per persones que no disposen de coneixements tècnics profunds de ciberseguretat.

A diferència de quan s'al·ludeix a tècniques de «hacking», on per norma general es requereix tenir nocions importants a nivell de telecomunicacions, xarxes, programació o àrees similars, la suplantació es basa a falsificar encapçalaments i l'engany visual, no a comprometre sistemes.

4.4. És un mitjà i no una finalitat

L'spoofing o suplantació d'identitat es podria considerar la fase inicial d'una altra mena d'atacs com ara la pesca (orientada al robatori de credencials o dades delicades), el Business Email Compromise (orientat al robatori de diners) o la distribució de programari maliciós (per segrestar equips i aconseguir que formin part d'una xarxa zombi o, fins i tot, infectar amb un programari de segrest).

5. L'AUGE DE CORREUS MALICIOSOS CONTRA ELS PETITS NEGOCIS

Per ser precisos cal aclarir que s'ha vist un augment important de qualsevol mena de ciberatac contra els petits negocis.

Les raons es podrien resumir en la manca de conscienciació. La ciberseguretat no s'ha percebut com un element estructural de micropimes o autònoms. A l'imaginari col·lectiu és quelcom que s'ha percebut fins fa relativament poc com a una cosa més associada a grans corporacions.

Però no és així. Qualsevol organització està en risc de ser objectiu d'un ciberatac. De fet, els ciberdelinqüents tenen molt en compte que la probabilitat que l'atac tingui èxit és més gran si s'adreça contra un negoci petit, tot i que el rèdit sigui menor. Això ha provocat que cada vegada més s'hagi vist un creixement important de campanyes dirigides a aquests.

I aquesta manca de conscienciació que s'esmentava és la que ha provocat que, a més, les micropimes i els autònoms no disposin dels recursos mínims a nivell de ciberseguretat per manca d'inversió, ni es doti els membres de l'organització d'una formació mínima que els permetria identificar, almenys, atacs bàsics.

Del començament d'any ençà, a Andorra s'ha vist un augment important de campanyes de correu malicioses dirigides contra petits negocis que, fins a la data, han provocat un total de 27 incidents les conseqüències dels quals abasten des de pèrdues econòmiques importants fins a l'exfiltració d'informació delicada i confidencial.

6. RECOMANACIONS PER PREVENIR L'*EMAIL SPOOFING*

6.1. Formació

L'èxit d'un atac mitjançant un correu maliciós, sigui una campanya de pesca o un cas de suplantació, resideix en el factor humà. Per això, i tot i que soni molt bàsic, per identificar i prevenir aquesta mena d'atacs, la formació dels membres de l'organització es converteix en un element crític. Com a mínim, qualsevol empleat hauria de saber:

- Com identificar un correu sospitós
- En quines circumstàncies no s'ha de fer clic a enllaços o arxius adjunts
- Com verificar la identitat del remitent al complet

6.2. Filtres antispam

Aquest és un altre requisit bàsic. La majoria dels correus maliciosos es poden identificar i filtrar automàticament pels mateixos serveis de correu.

6.3. Configuració de SPF, DKIM i DMARC

Com s'ha explicat prèviament la configuració correcta d'aquests protocols dificulta enormement tot aquell atac que pretengui suplantar el domini d'una organització. Per això, qualsevol organització, per petita que sigui, s'ha d'assegurar que aquesta acció s'ha aplicat.

6.4. Protocols d'actuació definits per als pagaments

Una altra acció clau és definir com és el procés de comunicació i pagament amb clients i proveïdors. És a dir, establir una metodologia concreta per executar qualsevol transferència.

Així, en cas que les passes que s'han definit no es respectin, per molt urgent que sigui qualsevol correu electrònic que arribi i apressi a fer qualsevol acció, si se surt del marc operatiu establert no es durà a terme.

6.5. Implantació del MFA per accedir al correu

D'aquesta manera, encara que es robin les credencials d'accés a qualsevol membre de l'organització, l'atacant no podrà comprometre el compte. Els factors d'autenticació múltiples s'han convertit en un element bàsic de protecció. Actualment, qui únicament depèn d'una contrasenya per fer un inici de sessió s'exposa a patir incidents amb un nivell d'impacte fàcilment prevenible.

6.7. Registre de dominis similars

Aquesta mesura pot ajudar tot i que de manera limitada. En primer lloc, perquè té un cost que potser no és assumible per qualsevol mena d'organització, sobretot quan es tracta de les més petites, a més perquè les possibles combinacions siguin tantes que calgui registrar una gran quantitat de dominis.

Tanmateix, sí que es podrien adquirir aquells dominis que es poguessin considerar més perillosos per dur a terme un intent d'engany. Per exemple, si el nostre domini dos «lamevaferreteria.ad», potser també s'hauria de considerar registrar «lamevaferreteria.com», «lamevaferreteria.net» o «lamevaferreteria.org».

7. 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.