Agència Nacional de Ciberseguretat d'Andorra

CONSCIENCIACIÓ EN CIBERSEGURETAT

Ús professional del correu corporatiu en les organitzacions públiques i privades

Ús professional del correu corporatiu: Introducció

El correu electrònic corporatiu és una eina de missatgeria electrònica a disposició dels empleats i col·laboradors de les organitzacions. Aquests l'utilitzen per **enviar i rebre** correus electrònics mitjançant l'ús d'adreces de correu corporatiu. Es tracta d'un **recurs compartit** per tots els empleats de les entitats, ja siguin aquestes públiques o bé privades. Per tant, un **ús inadequat** del mateix tindria repercussions directes i negatives en el servei que ofereixen les organitzacions.

Les peculiars característiques d'aquest mitjà de comunicació han propiciat l'aparició d'**amenaces**, les quals s'aprofiten del propi servei de correu electrònic per propagar-se o aprofitar les possibles **vulnerabilitats** que pugui tenir el sistema per tal d'atacar-lo.

Recomanacions generals per l'ús del correu electrònic corporatiu

01 Amb seny

El correu electrònic corporatiu ha de ser utilitzat amb **sentit comú**, tenint en compte les funcions exercides pel propi usuari i **evitant posar en un compromís els Sistemes** d'Informació, la bona imatge i la reputació de l'organització.

02 Seguretat i integritat

Les organitzacions podran **filtrar** el contingut del correu electrònic corporatiu de l'usuari amb l'objectiu de prevenir la propagació de **virus** o la detecció d'activitats **delictives** o **enganyoses**. Això es duu a terme amb la finalitat de garantir la seguretat i la integritat de les comunicacions electròniques dins de l'entorn corporatiu.

Recomanacions generals per l'ús del correu electrònic corporatiu

03 La configuració de l'adreça

El sistema que ofereix el servei de correu electrònic pot **rebutjar**, **eliminar** o **bloquejar** una part del contingut dels missatges enviats o rebuts en els quals es detecti algun **problema de seguretat**. Aquesta mesura s'aplica amb la finalitat de protegir la integritat del sistema i garantir la seguretat de les comunicacions.

04 Elements suplementaris

Es podrà afegir **contingut addicional** als missatges enviats com per exemple, quan apareix un quadre d'avís en iniciar la sessió al correu. Això es fa amb l'objectiu d'**advertir** als destinataris que han de complir amb una sèrie de requisits legals i de seguretat. Aquesta pràctica es realitza amb la finalitat de conscienciar els receptors sobre la importància de seguir les normatives i les precaucions de seguretat pertinents.

Altres recomanacions i obligacions a tenir en compte:

- Utilitzeu el correu electrònic únicament i exclusivament amb finalitats **professionals**, ja que és fonamental per mantenir la integritat del sistema.
- És crucial revisar amb deteniment els **camps de direccions** abans d'enviar qualsevol missatge amb l'objectiu de garantir que s'envia a les persones correctes i que no es cometran errors d'enviament.
- Cal assegurar la **identitat del remitent** abans d'obrir un missatge. És una precaució necessària per evitar possibles amenaces a la seguretat de la informació. En cas de rebre un correu sospitós, es recomana no obrir-lo i informar el remitent, especialment si es considera que pot ser un **incident de seguretat**. En aquest cas, és essencial posar-ho en coneixement del Departament d'IT/TIC de l'organització per efectuar una investigació adequada.
- Cal restringir estrictament l'ús d'accés a **comptes de correus personals** com Gmail, Hotmail, etc., des de dispositius corporatius, ja que això pot representar una **amenaça** per la seguretat de la informació.
- És de vital importància informar de qualsevol correu que contingui **virus**, ***phisihing***, **programari maliciós**, etc., sense reenviar-lo en cap cas, amb l'objectiu de protegir la seguretat del sistema i prevenir possibles danys.

Queda prohibit l'ús del correu electrònic corporatiu per les següents accions:

- Enviar **missatges en cadena**. Les alarmes de virus i les cadenes de missatges sovint són correus electrònics simulats amb l'objectiu de saturar els servidors i la xarxa.
- Respondre a missatges de **correu brossa**. La majoria d'aquests missatges es generen i s'envien a adreces de correu electrònic aleatòriament generades, amb l'esperança que les respostes obtingudes confirmin l'existència d'adreces de comptes reals.
- Enviar informació confidencial a un **remitent desconegut** o a un contacte habitual si dubtes de la seva procedència.
- Executar **arxius adjunts sospitosos**. Mai s'han d'executar els arxius adjunts rebuts sense analitzar-los prèviament amb l'eina corporativa establerta per a aquest propòsit.
- **Falsificar, ocultar, suprimir o substituir** la identitat de l'emissor en qualsevol correu electrònic. Aquestes pràctiques són inacceptables i contràries a les polítiques de seguretat de la informació.

Queda prohibit l'ús del correu electrònic corporatiu per les següents accions:

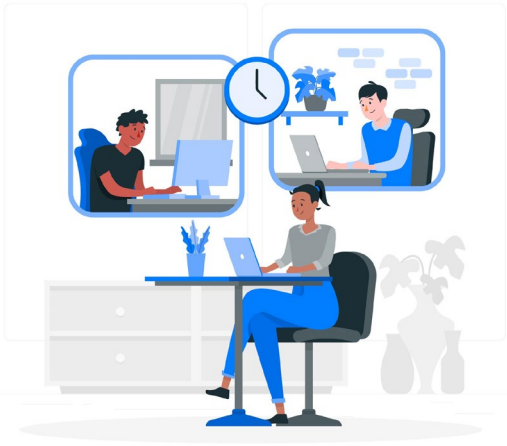
- Enviar correus electrònics que continguin en el cos o als adjunts informació amb dades considerades **confidencials** no està permès, llevat que s'adoptin mesures de **xifratge** o similars per protegir-ne la confidencialitat.
- **Cedir** l'ús del compte de correu a terceres persones pot provocar una **suplantació d'identitat i** l'accés a informació confidencial de l'organització, i per tant no està permès.
- L'acció d'**enviar o reenviar** correus de manera **massiva** ha de fer-se amb precaució. En cas d'autorització prèvia per a l'enviament a un grup de destinataris, és recomanable utilitzar una **llista de distribució** o, en defecte d'això, col·locar la llista d'adreces en el camp de còpia oculta.
- Fer ús del correu electrònic com si fos un **espai d'emmagatzematge** no és una funció principal i pot provocar problemes de rendiment i capacitat del sistema. És important mantenir el correu electrònic com una eina de comunicació i no com un dipòsit de documents o arxius.

Precaucions a adoptar amb l'accés remot de l'adreça corporativa:

Desactiveu les característiques de «Recordar Contrasenya» del vostre navegador

Si un dispositiu cau en mans equivocades, el fet que el navegador recordi les contrasenyes **facilita l'accés no autoritzat** a comptes i sistemes corporatius.

D'altre banda, alguns tipus de malware estan dissenyats per extreure contrasenyes emmagatzemades als navegadors. Si es guarden credencials, augmenta considerablement el risc.



Activeu l'opció d'eliminació automàtica d'informació sensible del vostre navegador

En activar aquesta opció, s'eliminen automàticament dades com l'historial de navegació, descàrregues, formularis completats, cau, *cookies*, contrasenyes i sessions autenticades.

A més, es **protegeix la privadesa de l'usuari** i en cas que el dispositiu es perdi o sigui robat, l'eliminació automàtica garanteix que les dades personals i confidencials no quedin exposades.

També, en eliminar les *cookies* i dades de navegació es dificulta el seguiment per part d'anunciants o altres tercers.

Per últim, garantim que el navegador comenci de zero cada vegada que s'inicia, la qual cosa pot millorar el rendiment i reduir l'acumulació de dades innecessàries.