Ciberseguretat: consells per detectar correus maliciosos [1]

Publicat:
08 novembre 2019

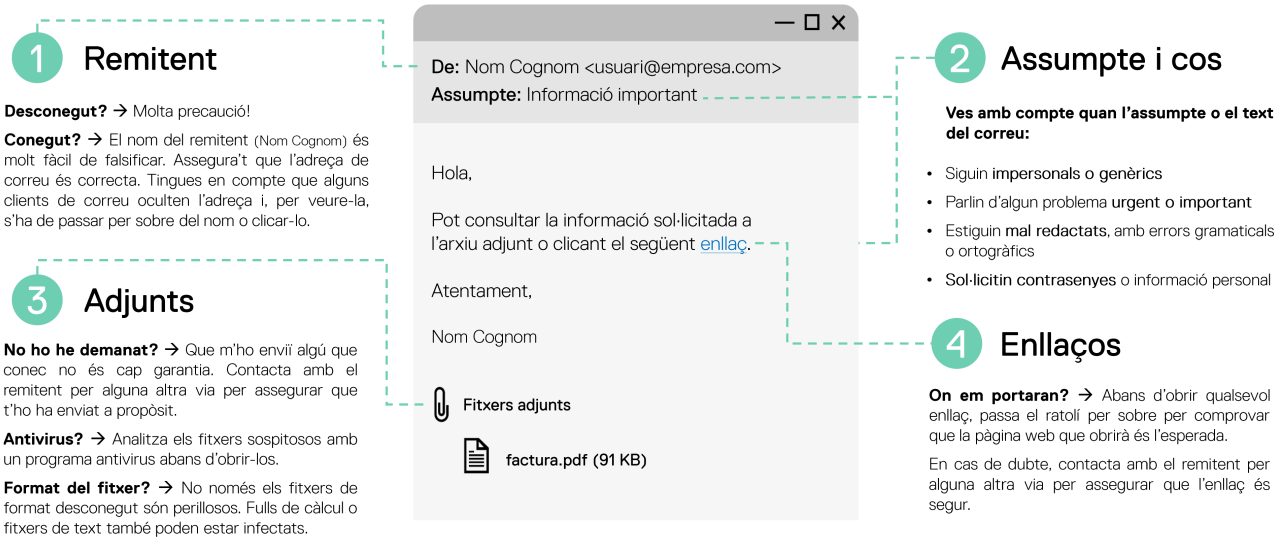
Malauradament, la delinqüència digital és cada cop més habitual, i un dels mitjans preferits pels ciberdelinqüents és el correu electrònic.

I precisament aquests dies en què tots veiem incrementada la nostra activitat en línia, recordem que és necessari extremar la seguretat.

Tot i que els filtres *antispam* del correu electrònic del COAC eviten que ens arribin molts d?aquests correus, és necessari que com a usuaris prenguem mesures per detectar els correus maliciosos que han superat els filtres de seguretat. D?aquesta manera podrem evitar pràctiques com el *ransomware* (xifrat del nostre disc dur per demanar-nos el

pagament d?un rescat) o el *phishing* (suplantació d?identitat per robar-nos dades bancàries o contrasenyes).

Tot seguit us fem un resum del que cal tenir en compte en l?ús que fem del correu electrònic.



Bones pràctiques per prevenir el "credential stuffing" i el "phising"

· Canviar les contrasenyes periòdicament (consulta el manual per canviar la contrasenya del teu compte de correu col·legial) [2]

· No fer servir la mateixa contrasenya en més d'un lloc.

· Utilitzar contrasenyes d'una certa longitud (més de 8 caràcters) i que continguin informació alfanumèrica (dígits, lletres i caràcters especials).

· Utilitzar un gestor de contrasenyes o bé, si cal, escriure-les en un paper.

Evitar obrir correus electrònics que:

· Sol·licitin informació personal o dades d'accés (el COAC mai demanarà un usuari o contrasenya via correu electrònic).

· Continguin arxius adjunts que no esperem o amb noms o formats no familiars.

· Provinguin d'adreces de correu desconegudes, però alhora "familiars" (p. ex. administrador.coac@hotmail.com [3], coac@gmail.com [4], coac.alert@gmail.com [5]).

· Que el text exigeixi urgència, contingui amenaces o busqui generar alarma.

· Que el text contingui idiomes desconeguts, un estil poc familiar o tingui paraules, expressions o concordances de gènere mal escrites.

· Semblin missatges massa bons per ser veritat (premis, viatges gratis, etc).

Links
[1] https://arquitectes.cat/ca/content/ciberseguretat-consells-detectar-correus-maliciosos
[2] https://www.arquitectes.cat/ca/modificaci%C3%B3-de-la-contrasenya-des-del-correu-web
[3] mailto:administrador.coac@hotmail.com
[4] mailto:coac@gmail.com
[5] mailto:coac.alert@gmail.com