

CONSELLS PER DETECTAR CORREUS MALICIOSOS

Suport Informàtic

[1]

**Ciberseguretat:
consells per
detectar correus
maliciosos**

Imatge:

© Col·legi d'Arquitectes de Catalunya (COAC)

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.

1 Remitent

Desconegut? → Molta precaució!

Conegut? → El nom del remitent (Nom Cognom) és molt fàcil de falsificar. Assegura't que l'adreça de correu és correcta. Tingues en compte que alguns clients de correu oculten l'adreça i, per veure-la, s'ha de passar per sobre del nom o clicar-lo.

3 Adjunts

No ho he demanat? → Que m'ho envii algú que conec no és cap garantia. Contacta amb el remitent per alguna altra via per assegurar que t'ho ha enviat a propòsit.

Antivirus? → Analitza els fitxers sospitosos amb un programa antivirus abans d'obrir-los.

Format del fitxer? → No només els fitxers de format desconegut són perillosos. Fulls de càlcul o fitxers de text també poden estar infectats.



2 Assumpte i cos

Ves amb compte quan l'assumpte o el text del correu:

- Siguin impersonals o genèrics
- Parlin d'algun problema **urgent** o **important**
- Estiguin **mal redactats**, amb errors gramaticals o ortogràfics
- Sol·licitin contrasenyes o informació personal

4 Enllaços

On em portaran? → Abans d'obrir qualsevol enllaç, passa el ratolí per sobre per comprovar que la pàgina web que obrirà és l'esperada.

En cas de dubte, contacta amb el remitent per alguna altra via per assegurar que l'enllaç és segur.

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

- Canviar les contrasenyes periòdicament [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 (dígit, 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).

8/11/2019

Tornar [6]

Copyright@ Col·legi d'Arquitectes de Catalunya : <https://www.arquitectes.cat/ca/suport/ciberseguretat-correus-maliciosos>

Links:

- [1] <https://www.arquitectes.cat/ca/suport/ciberseguretat-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>
- [6] <https://www.arquitectes.cat/ca/javascript%3Ahistory.back%281%29>