APRENENT TECNOLOGIES A L'AULA
AMB L'ÀNGEL COLOMER

NOCIONS MOLT BÀSIQUES SOBRE SEGURETAT

Diferents preocupacions que m'han arribat darrerament sobre la seguretat en Internet (*tan relacionades amb les notícies sobre l'ús del programa Zoom com sobre la recepció de cartes d'intents d'extorsionar o de robar dades, etc*.) més les brillants xerrades de Jaume Pujol, expert en Seguretat Informàtica, m'han portat a fer aquesta fitxa dedicada a comentar unes nocions mínimes bàsiques sobre la Seguretat per Internet, més dedicades al tema dels ordinadors, sobre les que ja he tractat en altres ocasions i en diverses xerrades.
Ja sabem que la seguretat al 100% no existeix, però almenys, prenent mesures, podrem reduir-ne les males conseqüències de no tenir-les en compte.

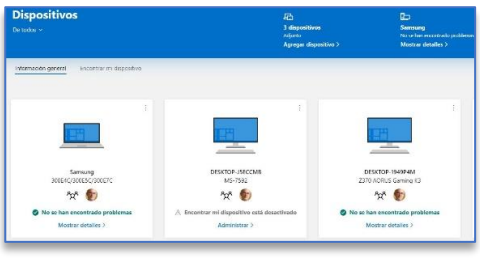
Que passa quan engeguem l'ordinador?

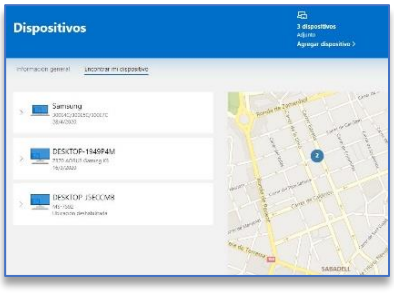
Doncs que ja en la primera pantalla que podem veure en obrir l'ordinador ens demana, un cop mostrat el nostre nom d'usuari, que ens hi identifiquem per poder treballar.
Com a norma general, en els ordinadors amb Windows, en configurar-lo, Microsoft ens diu que millor crear un compte amb ells, amb:

- Un nom d'usuari (*generalment una adreça de correu electrònic*)
- Una contrasenya.

Aquest compte ens valdrà per:

- Tots els equips que tinguem amb Windows (*portàtils, sobretaules, etc*.)
- Poder identificar-nos i entrar-hi
- Poder-los localitzar si mai el perdéssim o ens el prenguessin.





Parlem de contrasenyes.

És la clau que ens dóna accés a tot el que tenim dins l'ordinador (*fotos, vídeos, documents, comptes del banc, correus, etc*.) i també a programes i a xarxes socials; en resum a la història de la nostra vida, pensaments, records, etc.

Ja se sap que seguretat i comoditat són, a voltes, difícils de compaginar, però pel que ens hi juguem, cal que les contrasenyes complexin un mínim de condicions:

- No han de ser fàcilment endevinables o fàcils de memoritzar si algú veu quan les escrivim.
  - No el típic "12345", ni la paraula "contrasenya".
  - No el número de telèfon.
  - No el número del DNI.
  - No l'adreça del domicili (*carrer i número*) o nom de la parella.
  - No la data de naixement o qualsevol altre fàcilment deduïble.
  - Com més llarga, millor.
  - Millor barrejar números, signes i lletres minúscules i Majúscules. Si busqueu a https://pasword.kasperky.com podeu comprovar, tot i que ja ho intuíeu, la "fortalesa" de la vostra contrasenya:
  -

*Contrasenya **1234***
Massa fàcil, oi?

*Contrasenya **Fort¿09?Kolo***
Tampoc cal passar-se!

- No fem servir la mateixa en tots o molts llocs. És còmode, però si en troben una, les tenen totes.
- No han de ser fàcilment accessibles. Se'n necessiten tantes que és impossible memoritzar-les totes; en algun lloc les hem de tenir.
  D'acord, però que aquest lloc sigui segur, fàcil de trobar per nosaltres, però complicat pels altres i si pot ser que requereixi un codi, millor.
- Si mai l'oblidéssim, podem recuperar-la o restablir-ne una altra de nova.

Parlem de com poden obtenir dades nostres?

Són molts els serveis, programes, informació, etc., que podem fer servir gratuïtament; però, quan ens parem a pensar, és molt estrany que algú inverteix un munt de capacitat, recursos, tecnologia i diners sense cobrar-nos, oi?
S'ho cobren; d'una manera o altra s'ho cobren. La forma més corrent consisteix a obtenir dades nostres, edat, sexe, estat civil, aficions, pàgines que consultem, temes d'interès, nivell de consultes i de compres, relacions, estudis, viatges, nombre de seguidors, horaris, equips que tenim i que utilitzem, rutes que fem, amics que tenim, música que escoltem, pelis que ens agraden, companyies amb les quals treballem o ens subministrem, etc.

Com les obtenen les dades?

- Doncs, normalment som nosaltres mateixos qui les donem, quan acceptem "galetes", quan ens donem d'alta o registrem i donem més dades que les obligatòries, etc.

- En altres casos, perquè saben com entrar en els nostres equips o enredar-nos perquè els hi donem, per exemple fent-se passar per empreses que coneixem (*demanant dades, contrasenyes*) o introduint virus (*enviats per email o dins de programes*) en el nostre equip, etc.

I què en fan de les dades?

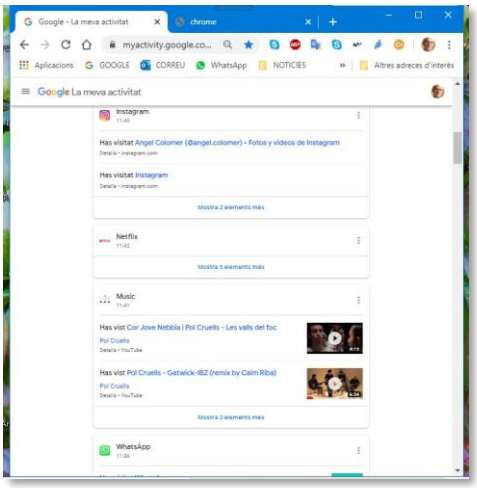
- En el millor dels casos aquestes "dades nostres" les venen a empreses i grups que es dediquen a la publicitat, estudis de mercat, agències de viatges, gabinets de propaganda política, immobiliàries, farmacèutiques, sector automobilístic, estudis de la conducta, vendes, lloguers, etc. (*Mireu tots els anuncis que us arriben per email i quin tipus d'anuncis tan personalitzats als vostres gustos que se us apareixen quan us moveu per Internet, o fins i tot el curiós que resulta quan feu una cerca per Google, que els primers resultats que proporciona siguin els més adequats a com sou vosaltres*).
- En el pitjor dels casos, les intenten utilitzar amb finalitat de delinquir, estafant, extorsionant, demanant pagaments per recuperar dades que ens han sostret o codificat, accedint a comptes bancaris, fent compres suplantant la nostra identitat, etc.

Activitat; qui sap la meva activitat?

Per exemple, si a Google mirem https://myactivity.google.com/myactivity, podem veure tot el que he anat fent avui:

- He publicat a "Instagram".
- He mirat el "Netflix".
- He vist uns videoclips de "YouTube"
- Abans he repassat el "Whatsapp"

I així puc veure tota "l'activitat" del que he anat fent cada dia.



Hi ha altres programes que fan també seguiment (*Spotify, Facebook*) a banda dels que jo, voluntàriament, deixo que em segueixin, o que publiquin les rutes que faig.

Perfil? Qui sap el meu perfil?

Són molts els programes que, en inscriure'ns ens demanen dades personals, suposadament per ajustar més les nostres preferències, localitzar amics, companys de feina, d'estudi, de club o de la mateixa ciutat.
El número 1, és Facebook i, molta gent els hi facilita despreocupadament.

Això ens pot passar mai a nosaltres?

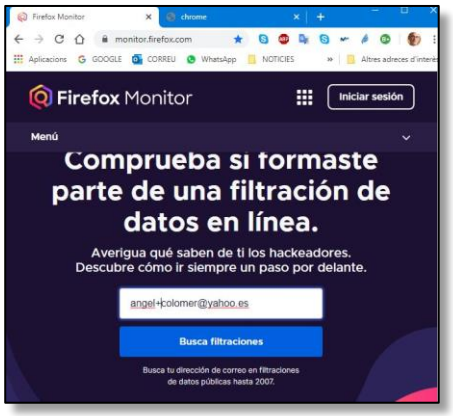
Que algú faci servir el nostre perfil, les nostres dades? Això sols els hi passa als altres. Però, fem una prova?:

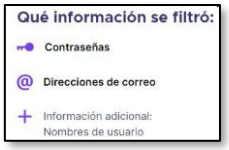
- Entreu a Google https://monitor.firefox.com/
- On ho demana, escriviu el vostre email.

El programa us indicarà:

- Si ha estat agafat/filtrar fraudulentament alguna vegada.
- I, si ho ha estat, que podeu fer per protegir-vos.

Com deia en Lluís Llach, que tingueu sort!





Hi ha altres webs, com https://haveibeenpwned.com/ que també permeten verificar si us han “agafat” mai els vostres comptes.

Localitzar des d’on esteu treballant

Clicant a https://es.infobyip.com/ en el vostre navegador, s’accedeix a una web que informa de dades sobre l’adreça electrònica (IP) del vostre ordinador, amb quina companyia es connecta a Internet, des d’on treballa, mida del monitor, sistema operatiu, etc. fins i tot quin poble està situat a la vostra antípoda (*que ja em direu que m’importa, però mira!*)
Com veieu, eines que poden tenir la seva utilitat, però que utilitzades per mans del “costat fosc”, poden servir per fer malifetes.

De temes que tractin sobre la Seguretat Informàtica, n’hi ha molts, i de molt útils i interessants.
En aquesta “Primera Part” n’hem pogut veure alguns d’ells; però queda per tractar temes com Antivirus, neteja periòdica, etc. que podem tractar en altres “Segones Parts”.

De moment, recordem el que ens deien a l'escola: "*Compte! No abaixeu la guàrdia, que el dimoni no fa mai vacances*!".

No descuidem la Seguretat, però, alhora, que no ens obsessioni.