NAVEGACIÓ SEGURA EINES I CONSELLS

1. INTRODUCCIÓ

QUE HEM DE TENIR EN COMPTE

La seguretat sempre és un aspecte important alhora d'utilitzar les TIC, tot i que no cal ser alarmista ni paranoic, si que hem de tenir alguns hàbits que evitaran sobretot tenir un ensurt.
Per tant és important que quan pensem en la nostre seguretat incorporem hàbits a la nostra vida digital...per exemple configurar correctament les xarxes socials, no compartir les contrasenyes...

Però no podem oblidar que aquest hàbits també hi haurien d'anar incorporats, el fet de tenir el nostre sistema operatiu actualitzat, disposar d'un antivirus i un tallafocs i preocupar-nos de l'estat del nostre ordinador.

2. LA NAVEGACIÓ

LA INFLUÈNCIA DELS NAVEGADORS

Navegar per internet és una de les tasques que més farem, per tant, quines són les qüestions més importants que hem de tenir en compte:

- **La privacitat** - No podem ignorar aquesta qüestió, les nostres dades són confidencials de manera implicita, i hem d'impedir que les webs no recopilin informació que no sigui estrictament necessaria per poder navegar

- **Seguretat personal** - La seguretat comença per nosaltres per tant hem de ser conscients que un dels pilars de la seguretat rau en la seguretat de les nostres contrasenyes i en no compartir-les amb ningú.

- **Seguretat amb les comunicacions** - Sempre que es produeixin transaccions o hi pugui haver-hi dades sensibles, com gestions amb bancs i caixes, hem de ser exigents amb que els canals per on transmetem la informació siguin segurs a través de tecnologies lliures, estandars com és el SSL.

El navegador web té iun paper important en totes aquestes qüestions, ara mateix tots els navegadors web són gratuits però no tots són lliures. Com a punt de partida és important que el navegador sigui lliure, ja que ens pot proporcionar més transparència però com que el mercat de navegadors és molt gran i la seguretat d'aquests és canviant nosaltres us proposarem un:

El Mozilla Firefox , perquè és lliure i segur, això no vol dir que sigui el més segur de tots però si un dels més segurs.

3. LES COMUNICACIONS

EL PROTOCOL HTTPS

Per a poder assegurar-nos de que les comunicacions són segures, els navegadors utilitzen el protocol SSL (Secure Sockets Layer) que ofereixen comunicacions segures a través d'encriptar les dades.
Quan naveguem per una pàgina que encripta les dades veurem que l'adreça del nostre navegador canvia de *http* a *https,* per exemple:

Adreça amb http:

Adreça amb https:

Una altre qüestió important és que us assegureu que esteu navegant al lloc web corresponent per evitar *falsificacions* de web, la manera més efectiva és escrivint vosaltres l'adreça.

Si sospiteu d'una adreça podeu utilitzar el recurs de URL Void (http://www.urlvoid.com/) on simplement indiqueu l'adreça web i si en el resultat us surt *CLEAN* vol dir que és una adreça fiable

Aquest xifratge que proporciona el SSL és el que us donarà la seguretat de poder fer pagaments per internet.

4. LES CONTRASENYES

Actualment el mètode més estès per obtenir accés a informació personal que hem emmagatzemat al nostre equip i/o serveis en línia és mitjançant contrasenyes, com per exemple, el correu electrònioc

La major part de les vegades una contrasenya **és l' única barrera entre les nostres dades confidencials** i els ciberdelinqüents.Per la qual cosa val la pena invertir una mica de temps i esforç per gestionar-les eficaçment.

COM GENERAR UNA CONTRASENYA SEGURA

Una bona contrasenya ha de complir tres d'aquestes quatre característiques:

- Tenir nombres
- Tenir lletres
- Tenir majúscules i minúscules
- Tenir símbols ($, @, &, #, etc.)

BONS HÀBITS

- La longitud no ha de ser inferior a set caràcters.Com més llarga sigui més difícil de reproduir.
- Canvia les teves contrasenyes regularment. Com més crítica sigui la contrasenya –per exemple, no és el mateix la contrasenya del banc que la d'un fòrum- amb més freqüència és aconsellable canviar-la.
- Utilitzaregles mnemotècniques:: per exemple, amb una frase fàcil de memoritzar i creant una regla per escurçar-la.

  Exemple:La primera lletra de cada paraula.>

  Frase:El 4 de novembre és el meu aniversari

  Contrasenya:E4dNeemA

HÀBITS QUE CAL EVITAR

- La contrasenya no ha de contenir informació que sigui fàcil d'esbrinar. Per exemple, nom d'usuari del compte, informació personal (aniversaris, nombre de fills, etc.) o lletres que estiguin unes al costat de les altres al teclat (123456, qwerty, etc.).
- No utilitzis la mateixa contrasenya per a comptes diferents. Sobretot si són d'alt risc, com les dels serveis bancaris o comercials.
- Evitacontrasenyes que continguin paraules existents en algun idioma. Els atacs de diccionari proven cadascuna de les paraules que figuren al diccionari o paraules d'ús comú.

- No guardis les contrasenyes en un lloc públic i a l'abast de tothom.
- Canvia les contrasenyes que vénen per defecte amb els dispositius i serveis en línia.Un exemple és el dels routers WiFi, que porten per defecte contrasenyes públicament conegudes que un atacant podria utilitzar.
- Limita l'ús dels gestors de contrasenyes del navegador per a serveis crítics.Si és possible, el millor lloc és la memòria d'un mateix.

5. EXTENSIONS

Alguns navegadors com Mozilla Firefox o Google Chrome es poden afegir complements per a complementar o millorar la seguretat de la nostra navegació. Per a poder instal·lar-nos qualsevol extensió o complement de Firefox hem d'anar a Eines > Complements i cercar l'extensió que volguem.
Us deixem amb un llistat d'extensions que trobem útils:

- **BlockSite**: Ens permet afegir manualment llocs que volguem bloquejar

- **Ghostery**: Aquesta extensió t'alerta quan un lloc web ens està vigilant mitjançant l'anàlisi del lloc per detectar si està corrent algun script amagat de rastreig de comportament.

- **Password Hasher** - Generador de contrasenyes fortes

- **Web of Trust -** Adverteix sobre els llocs webs que poden infectar amb malware o que envien spam.