CIBERSEGURETAT PER A PROFESSIONALS MÈDICS

Col·legi de Metges de Barcelona

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

10 recomanacions per adquirir hàbits digitals segurs

ACTUALITZACIÓ DE SISTEMES I PROGRAMES

Cal **mantenir al dia** les actualitzacions de tots els **dispositius i programes**. Deixa actualitzar sempre el **sistema operatiu** dels teus equipsintenta mantenir sempre els navegadors actualitzats en l'última versió. No instal·lis programes i aplicacions d'origen dubtós o desconegut. Fes servir únicament proveïdors de confiança, botigues d'aplicacions i/o webs oficials.

ANTIVIRUS

Deixa actualitzar **l'antivirus** i ***l'antimalware*** (protecció contra el codi maliciós). Assegura't que l'antivirus dels teus equips està **sempre activat**. És recomanable que l'antivirus instal·lat sigui de **qualitat** i evitar-ne els gratuïts.

GESTIÓ DE CONTRASENYES I COMPTES DE CORREU

Utilitza sempre contrasenyes per accedir als teus equips i dispositius i evita guardar-les als navegadors. Procura tenir un compte de **correu principal** reservat per a les gestions i connexions més rellevants, amb una **contrasenya exclusiva** i usa un **doble factor d'autenticació**.
És important utilitzar **contrasenyes robustes** que combinin lletres, números, signes de puntuació, majúscules i minúscules.
Cal mantenir totes les **credencials d'accés personal en secret**, especialment les que utilitzes per accedir a llocs com la teva entitat bancària, el teu lloc de treball, La Meva Salut, etc. És recomanable utilitzar-ne de diferents en l'**àmbit professional i personal**. Si en tens moltes i per no reutilitzar-les es recomana l'ús d'un gestor de contrasenyes.

CORREUS ELECTRÒNICS I SMS SOSPITOSOS

Desconfia de correus electrònics o SMS de remitents sospitosos, desconeguts o que no t'esperis i **no descarreguis ni executis elements o enllaços adjunts**.
Podria tractar-se d'una campanya de ***phishing*** (que captura credencials, dades personals o bancàries) o que descarregui un virus o un ***ransomware*** (xifrat i segrest de les dades) al dispositiu. No tinguis pressa i no facis res del que et demanin sense haver-te assegurat abans que l'operació és legítima. Recorda que les entitats bancàries no solen demanar, i menys encara de manera urgent, dades d'accés o credencials personals a través de correu electrònic o SMS.

CONNEXIONS SEGURES

És preferible utilitzar la connexió 4G/5G del teu dispositiu que connectar-se a **xarxes WIFI obertes o gratuïtes**. Si malgrat tot has de connectar-t'hi, evita accedir a informació sensible o intercanviar aquest tipus de contingut per correu electrònic. Tampoc és segur realitzar operacions bancàries en aquestes connexions.

CÒPIES DE SEGURETAT

Assegura't de tenir còpies de seguretat de la informació que t'interessa guardar. Cal que sempre disposis d'una còpia de seguretat protegida que no pogués ser compromesa en cas d'atac, per exemple mantenir-la desconnectada de la xarxa.

CIBERSEGURETAT PER A PROFESSIONALS MÈDICS

Col·legi de Metges de Barcelona

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Generalitat de Catalunya

SUPORTS EXTERNS

És aconsellable utilitzar **discos encriptats i protegits amb una contrasenya**. Hi ha programes que ofereix aquesta opció. No és aconsellable la utilització de llapis de memòria per la facilitat amb què es poden perdre. En el cas que hagis de fer-ne servir, utilitza aquelles que permeten xifrar les dades. Guarda els dispositius extraïbles en un lloc segur. Sigues prudent a l'hora de connectar dispositius extraïbles subministrats per tercers als teus equips.

CONFIDENCIALITAT DE LES DADES

Has de tenir especial cura i reserva amb les dades confidencials de documents, informes i altres informacions que generes o que tractes. Busca assessorament expert en matèria de protecció de dades.

CONFIGURACIÓ DE PRIVACITAT A LES XARXES SOCIALS

Si ets usuari de xarxes socials, configura el teu compte de manera que puguis **protegir la teva privacitat**. Utilitza contrasenyes fortes i el doble factor d'autenticació. **Minimitza la informació personal** que comparteixes a les xarxes socials per tal d'evitar atacs i enganys.

GESTIONS ONLINE

La majoria d'entitats disposen d'**APPS per fer tràmits o gestions**. És recomanable que utilitzis aquest mètode per interactuar amb la teva entitat en lloc de fer les gestions a través de pàgines web amb el teu navegador. Amb l'ús d'APPs oficials evitaràs accedir a falses webs i caure en campanyes de phishing (suplantació d'identitat).

RECORDA:
Davant de qualsevol dubte, sospita o incident de seguretat, posa't en contacte amb el departament tècnic de la teva organització o amb el teu expert de referència. És aconsellable disposar d'assessorament expert en matèria de seguretat i sobre serveis asseguradors de ciberprotecció.