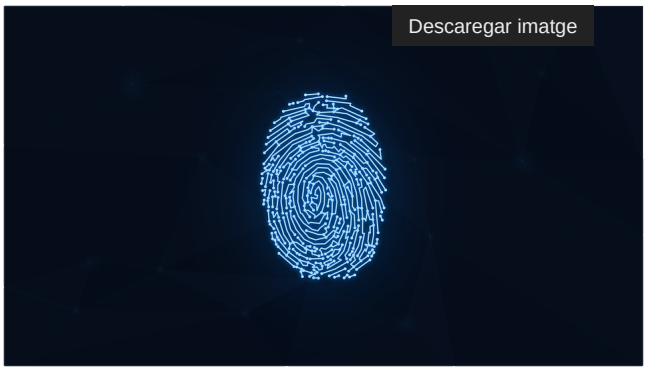
dilluns, 28 de març de 2022

Identitat digital i ciberseguretat. Algunes recomanacions



Cada dia depenem més de la nostra identitat digital, per la qual cosa hem d'anar amb molt de compte amb la gestió de les nostres credencials i amb l'ús dels dispositius amb els quals accedim a internet. De fet, segons l'Agència de Ciberseguretat de Catalunya (https://ciberseguretat.gencat.cat/ [https://ciberseguretat.gencat.cat/]), en el segon trimestre de 2021 les dades personals equivalents a més del 50% dels ciutadans catalans van quedar exposades.

En el context de la Universitat de Lleida, hem de tenir cura de les nostres credencials que ens permeten accedir als serveis de la universitat. Per evitar
problemes de ciberseguretat podem seguir les següents recomanacions:

Correu electrònic:

- Si el remitent és desconegut, o l'adreça és estranya, desconfieu d'aquest.
- No feu clic a cap enllaç ni descarregueu cap fitxer que no arribi d'una font fiable.
- Limiteu l'ús del correu electrònic corporatiu a entorns professionals.

Contrasenyes:

- Utilitzeu contrasenyes robustes (mescla de majúscules, minúscules, dígits (0-9) i signes de puntuació).
- Renoveu-les de forma periòdica.
- No les compartiu amb ningú.
- No reutilitzeu les mateixes contrasenyes per serveis diferents. Així, si algú aconsegueix la contrasenya, no tindrà accés a la resta de serveis.
- En cas que sospiteu que algú ha tingut accés a la vostra contrasenya, aviseu als serveis tècnics a través de l'eina CAU-TIC perquè revisin si hi ha hagut alguna activitat maliciosa amb el vostre compte, i feu un canvi de contrasenya mitjançant el campus virtual:
  PAS/PDI: Intranet - Directori - Canvia la clau d'accés.
  ESTUDIANTS: Utilitats - Obre l'eina directori - Canvia la clau d'accés.
  EXTERNS: Reinicia la clau, pàgina principal cv.udl.cat (sense haver iniciat sessió)

Programari:

- Treballeu amb entorns on les dades se sincronitzin al núvol, i mireu d'activar-hi mecanismes de doble factor d'autenticació.
- Tingueu sempre actualitzat tant els navegadors com el sistema operatiu dels vostres dispositius.
- Feu anar un antivirus i manteniu-lo actualitzat.
- No instal·leu programari que no en pugueu verificar la procedència.
- No connecteu dispositius USB que no siguin propis o no conegueu la procedència.
- Activeu el bloqueig de pantalla amb clau en cas d'inactivitat del dispositiu.
- Apagueu el vostre equip de treball quan acabeu la jornada de treball.

Si teniu qualsevol dubte sobre temes de ciberseguretat, podeu adreçar-vos a l'eina de suport CAU-TIC (http://cautic.udl.cat/ [http://cautic.udl.cat/])

Jordi Juárez i Òscar Flores - Unitat SAAD (amb la col·laboració de Sistemes d'Informació i Comunicació de la UdL)