1. Introducció

L'ús dels comptes personals per acreditar-nos a les diferents plataformes d'ús diari creix exponencialment, per això és molt recomanable la utilització de credencials segures, ja que els portals de validació són el primer punt de seguretat que tenen els sistemes, per tant la utilització de contrasenyes no segures pot comprometre la seguretat dels sistemes als que accedim diàriament.

La major part de les vegades les credencials d'un usuari són vulnerades ja que s'utilitzen dates de naixement, la ciutat on estem vivint o el nostre número de telèfon, on un atacant pot aconseguir aquestes dades amb la utilització d'enginyeria social. Un altre dels motius en que les nostres credencials són vulnerades és per utilitzar paraules comuns amb el que un 'atac per diccionari' podria esbrinar la paraula de pas en qüestió de segons.

1.1. Resum de recomanacions

Per una bona gestió de les credencials personals, és recomanable que se segueixin les següents pautes per la creació i manteniment de paraules de pas:

- La periodicitat amb la qual les contrasenyes han de ser canviades en cap cas serà superior d'un any.
- Cada cop que s'hagi de renovar la paraula de pas s'ha de generar una totalment diferent, que no sigui una seqüència derivada de l'anterior, com per exemple afegir un número i anar-lo incrementant.
- No s'ha d'utilitzar la mateixa paraula de pas pels diferents comptes personals ja que si s'aconsegueix esbrinar tots estarien vulnerats.
- Quan es generi una paraula de pas mai s'ha d'anotar en un full, ni emmagatzemar en fitxers del propi ordinador sense encriptar.
- Mai enviï les seves credencials per correu electrònic o les comuniqui via telèfon.
- Si té sospites de que la seva paraula de pas ha pogut ser vulnerada, faci el canvi tan aviat com sigui possible.

1.2. Creació d'una paraula de pas

Per crear una paraula de pas segura es poden fer servir els següents tips:

1. Les paraules de pas han de tenir un mínim de 8 caràcters. No han de contenir més de 2 caràcters repetits. No han de contenir més de 2 caràcters consecutius (abc, 123, qwe...)

2. Es recomana com a mínim la utilització d'una lletra minúscula, una lletra majúscula, un dígit i un caràcter especial per la formació de la paraula de pas.

3. No s'han d'utilitzar dades personals (noms, DNI, número de telèfon, noms d'usuari) ni paraules que apareguin als diccionaris.

Una recomanació habitual a l'hora de crear contrasenyes és fer servir frases familiars per a que sigui fàcil de recordar la paraula de pas. En el següent exemple farem el canvi de minúscules a majúscules en la primera lletra de cada paraula i substituirem les lletres 'o', 'e' i 'l' per '0', '3' i '!' respectivament.

- Els bunyols es mengen sols

- 3!sBuny0!s3sM3ng3nS0!s

1.3. Utilitats i Eines

A la xarxa disposem de multitud de gestors de paraules de pas y webs per certificar si algun dels nostres comptes ha sigut vulnerat.

1.3.1. Filtració de credencials

Si volem comprovar si algun dels nostres comptes personals s'ha vist afectat per alguna filtració, podem adreçar-nos al següent enllaç on introduint el nostre correu personal ens tornarà la informació de les filtracions públiques.

https://haveibeenpwned.com/

1.3.2. Gestors de paraules de pas

Entre la multitud de gestors de paraules de pas podem trobar-ne de codi lliure o amb subscripció. Entre aquests gestors podem trobar diferents característiques que s'adapten a les necessitats de cada usuari com ara versió mòbil, allotjament al núvol, etc.

Alguns dels gestors que podem trobar al mercat són:

- Keepass – Totalment gratuït.
- Dashlane – Quota de subscripció.
- LastPass – Modalitat gratuïta amb funcions extres de pagament.
- 1Password – Quota de subscripció.