

CONTRASENYES



Recepta per a crear una contrasenya segura que recordar:

1



4 paraules inconnexes

2



convertir alguna lletra a majúscula

3



convertir alguna lletra a número

4



afegir algun caràcter especial

Exemple: xampinyo-capçalera-Reptil-99camions



Una contrasenya segura ha de tindre mínim 12 caràcters.

Mai repetir la mateixa contrasenya en diferents comptes.

Com puc recordar-me de tantes contrasenyes?

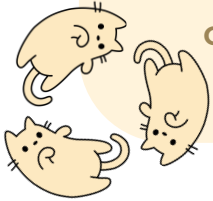


Seria impossible recordar-se de totes! Per això, aconsellem utilitzar un gestor de contrasenyes com KeePassXC. Aquesta aplicació emmagatzema en local les teues contrasenyes dins d'un arxiu xifrat amb una contrasenya maestra. Només hauràs recordar-te d'aquesta contrasenya maestra per a accedir a la resta.

QUÈ ÉS LA CULTURA DE LA SEGURETAT?

COMUNITAT

Són pràctiques compartides per una comunitat per a protegir-se de la vigilància o repressió de l'Estat o grups feixistes.



CURES COL·LECTIVES

No es tracta únicament de protegir-te a tu, sinó de protegir també a les teues amigues i el teu entorn.



CONSISTÈNCIA

No hi ha divisió entre allò personal i polític: les nostres vides són polítiques.

S'ha d'incorporar com una mentalitat en la nostra rutina.



CULTURA

Es diu cultura perquè amb la pràctica diària es torna inconscient i instintiva i, per tant, sense esforç.



TRANQUIL·LITAT

L'objectiu no és augmentar la paranoia de vigilància, sinó disminuir-la.

Aplicar un mínim de pràctiques més segures disminueix el risc.



AUTOGESTIÓ I COMUNOGESTIÓ

Les nostres vides han sigut digitalitzades forçadament i, mentre que combatim aquesta situació, hem de decidir de manera conscient com habitem el món digital.

Delegar el poder a les grans empreses tecnològiques i feixistes ens deixa vulnerables als seus dominis.



COM COMENÇE A INCORPORAR UNA CULTURA DE LA SEURETAT?

Realitzeu un anàlisi previ del **model de riscos del col·lectiu**:

-  **Identifiqueu què vols protegir:** dades personals, documents, dispositius, comunicacions, etc.
-  **Identifiqueu de qui vols protegir-te:** persones, organitzacions o cossos de l'Estat que puguin tindre interès en censurar o reprimir el vostre activisme.
-  **Identifiqueu la capacitat real dels teus adversaris:** els recursos econòmics, socials i tecnològics als que puga tindre accés.
-  **Identifiqueu possibles amenaces o atacs que podrien succeir:** perdre un ordinador, un mòbil confiscat en mans de la policia, una infiltració policial a una assemblea, un atac d'un grup feixista, etc.
-  **Mesureu cada risc concorde a la possibilitat de que l'amenaça es torne real.**
-  **Feu un pla de seguretat digital i treballeu en protocols formacions internes, rutines, etc.**

Més info:



<https://hiperderecho.org/tecnorestencias/resiste/#plan-seguridad-digital>