

Utilitzaci3 dâ??un Gestor de Contrasenyes Integrat al Navegador

Description

1. Funcionament del Gestor Integrat al Navegador

El gestor de contrasenyes integrat al navegador web   s un sistema encarregat d  emmagatzemar, xifrar i gestionar les credencials d  acc  s (noms d  usuari i contrasenyes) de l  usuari.

- **Emmagatzematge i Xifrat:** Les dades es guarden utilitzant algoritmes de xifrat robustos. La clau de desxifrat est   vinculada a la sessi   de l  usuari o al compte principal associat al navegador.
- **Detecci   i Autocompletat:** Quan es detecta un formulari d  inici de sessi   o de registre, el gestor identifica el domini web i suggereix o omple autom  ticament les credencials corresponents pr  viament desades.
- **Generaci   de Contrasenyes Segures:** En crear un nou compte, el gestor proposa claus aleat  ries d  alta complexitat (combinant lletres maj  scules, min  scules, xifres i s  mbols) per evitar l   s de contrasenyes febles.

2. Justificaci   de la Configuraci   a Casa i al Centre Educatiu/Laboral

La configuraci   i sincronitzaci   del gestor tant a l  entorn dom  stic com al centre respon a necessitats d  efici  ncia i seguretat:

- **Sincronitzaci   i Continu  tat de Treball:** En mantenir el perfil del navegador vinculat entre l  equip de casa i el del centre, es garanteix un acc  s fluid a totes les plataformes, eines educatives i serveis web sense haver de recordar ni introduir manualment les credencials a cada ubicaci  .
- **Actualitzaci   Din  mica i Manteniment:** Cada vegada que es genera o es modifica una contrasenya en un dels entorns, aquesta s  actualitza autom  ticament al n  vol i queda disponible immediatament en l  altre navegador.
- **Homogene  tzaci   de la Seguretat:** Permet mantenir els mateixos est  ndards d  alta seguretat i contrasenyes complexes independentment de la ubicaci   des de la qual s  accedeixi.

3. Riscos i Mesures de Seguretat Associades

Riscos Associats

1. **Acc  s No Autoritzat al Dispositiu:** Si un tercer accedeix a l  ordinador desbloquejat, podria utilitzar l  autocompletat per accedir als serveis web o veure les contrasenyes desades.

2. **Compromís del Compte Principal:** Si es vulnera el compte principal associat al navegador (per exemple, el compte de Google o Firefox), un atacant podria accedir a totes les credencials sincronitzades.
3. **Programari Maliciós (Malware):** L'existència de troians o *keyloggers* a l'equip pot posar en risc la seguretat de les dades.

Mesures de Seguretat

- **Autenticació per a la Visualització:** El navegador requereix la contrasenya o PIN del sistema operatiu per poder mostrar o exportar les contrasenyes desades.
- **Autenticació de Doble Factor (2FA):** Activació obligatòria del 2FA al compte principal que sincronitza el navegador.
- **Bloqueig Automàtic de Pantalla:** Configuració del bloqueig de sessió a l'ordinador en cas d'inactivitat.
- **Auditoria de Contrasenyes:** Utilització periòdica de les eines de comprovació integrades (*Password Checkup*) per detectar claus reutilitzades, febles o compromeses en filtracions.

4. Configuració i Procediment Pas a Pas

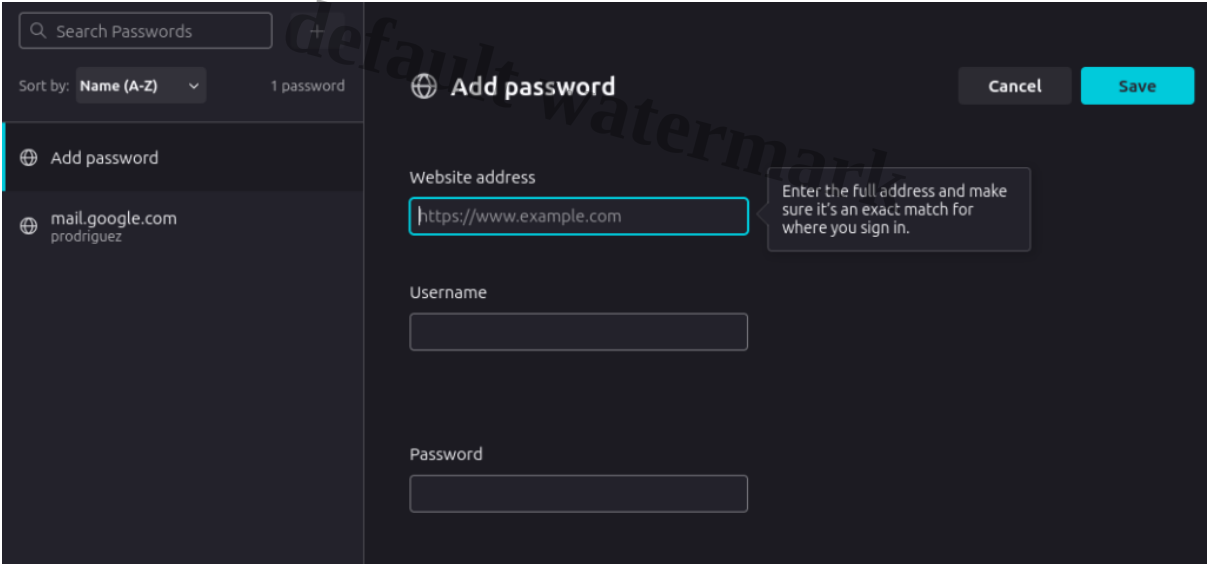
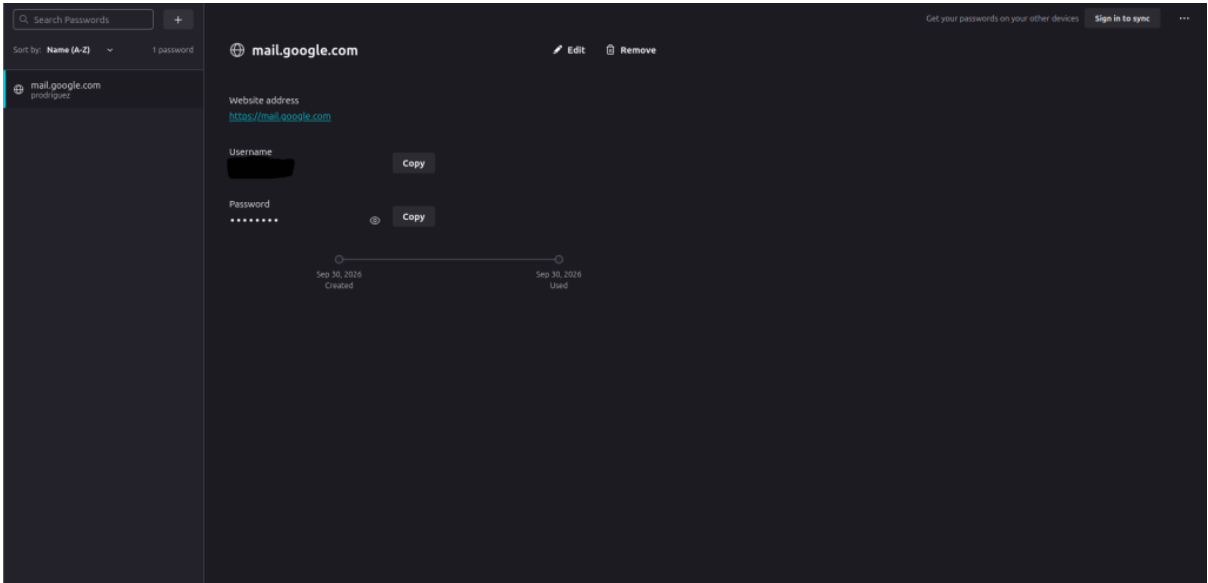
Pas 1: Configuració Inicial i Sincronització

1. Iniciar la sessió amb el compte d'usuari al navegador web tant a l'ordinador de casa com al del centre.
2. Accedir a la secció de **Configuració > Autocompletat i contrasenyes**.
3. Activar les opcions de **Preguntar si es vol desar les contrasenyes i Inici de sessió automàtic**.
4. Habilitar la sincronització de contrasenyes al menü de configuració del compte.

Pas 2: Generació, Emmagatzematge i Actualització

1. Accedir als serveis web habituals utilitzats a casa i al centre.
2. Utilitzar la funció del gestor per generar contrasenyes complexes i desades automàticament.
3. Comprovar que les credencials es van actualitzant i afegint de manera progressiva a mesura que es creen o modifiquen nous comptes.

Evidències



Date Created
2026/10/01
Author
prodriguez