

PasswordManagementTool

Password Management Guidelines

Core Principles

- Centralized Security: Use KeePassXC to store all credentials and sensitive data. Never store passwords in plain text files (`.txt`, `.docx`, `.xlsx`).
 - Unique Credentials: Use a distinct, strong password for every online account.
 - Multi-Factor Authentication (MFA): Activate MFA (TOTP, Passkeys) wherever possible. While initially inconvenient, it is the single most effective barrier against account takeover.
 - Offline Availability: Ensure you have access to your credentials even without an internet connection. Your password manager must function offline.
-

Frequently Asked Questions

Q: Why must I use different passwords? A: Credential stuffing. If a hacker obtains your password from one breached service, their first step is to automate login attempts on all major platforms (email, banking, social media). Unique passwords contain the breach to a single service.

Q: Should I use an online password service like LastPass or 1Password? A: We do not recommend them. Online services are high-value targets for attackers and have suffered significant breaches (e.g., LastPass in 2022). Furthermore, they introduce vendor lock-in: you surrender control of your sensitive data to a third party's server and terms of service. If the provider changes policies, raises prices, or shuts down, your access is at risk.

Q: Is it safe to save passwords in my browser (Chrome, Firefox, Safari)? A: It is generally discouraged for sensitive or work-related accounts.

- Security Risk: Browsers have a larger attack surface and are frequent targets for malware.
- No MFA Support: Browsers cannot auto-fill TOTP codes, forcing you to use a separate app.
- Lock-in: Passwords are tied to the browser profile. Syncing them relies on the browser vendor's cloud (Google, Apple, Mozilla), reducing data sovereignty.
- Recommendation: Use the KeePassXC Browser Extension instead. It provides the same autofill convenience while keeping your data in your own encrypted vault.

Q: Can I use macOS Keychain or Windows Credential Manager? A: These are acceptable for basic use, provided you maintain a strict offline backup strategy.

- The Risk: Your credentials are tied to your ecosystem account (Apple ID or Microsoft Account). If that account is locked, banned, or compromised, you may lose access to all stored passwords permanently. Recovery is often difficult or impossible.
- Requirement: If you use these tools, regularly export your data to an encrypted offline backup that you control.

Q: What is the recommended workflow?

- Do [this](#).

Revision #4

Created 2026-06-30 10:52:02 CEST by admino

Updated 2026-07-03 12:48:19 CEST by Jonas Valentin Rose