How to Secure Your Online Accounts With a Password Manage

Computers and Electronics · about 27 minutes · 2026-11-06

Move important accounts to unique generated passwords without losing access to your own data. These 24 steps cover account inventory, manager selection, a strong primary passphrase, MFA, passkeys, safe migration, recovery codes, emergency access, vault backups, updates, and recovery drills.

Things you will need

- A prioritized inventory of important accounts and reset hubs
- A reputable password manager that supports your devices
- A long, unique primary passphrase
- MFA methods and a secure second device where appropriate
- Protected offline storage for recovery codes and instructions
- A schedule for updates, vault reviews, and recovery drills

Assessing Accounts and Choosing a Password Manager

1. **List the accounts that hurt most if lost**
   Inventory the accounts that would cause the greatest harm if compromised.
2. **Find weak, reused, and exposed logins safely**
   Identify weak, reused, and already exposed credentials safely.
3. **Compare managers against the devices you use**
   Compare built-in and independent password managers against your devices.
4. **Read the provider's security and recovery terms**
   Verify the provider's security model and recovery terms before committing.
5. **Plan a migration with a way back**
   Plan a gradual migration that preserves a way back into every account.

Creating and Securing the Main Vault

6. **Install only from official sources**
   Install the manager only from official sources and prepare your devices.
7. **Choose a long unique primary passphrase**
   Create a long, random, and unique primary passphrase.
8. **Protect the vault account with a second factor**
   Turn on multi-factor authentication for the password manager itself.
9. **Set lock intervals on trusted devices only**
   Configure automatic locking and convenient unlock only on trusted devices.
10. **Test autofill and sync on one account**
    Test autofill and synchronization with a low-risk account first.

Migrating to Unique Passwords and Stronger Sign-Ins

11. Import credentials and delete the plaintext files

Import existing credentials without leaving a plaintext trail.

12. Secure your reset hub accounts first

Secure the primary email and other reset hubs before lower-value accounts.

13. Replace reused passwords in priority batches

Replace reused and weak passwords in manageable priority batches.

14. Add passkeys where the service supports them

Add passkeys where a trusted service and your devices support them.

15. Record the second-factor method, not the code

Enable MFA on other important accounts and record only the method metadata.

Building a Tested Account-Recovery Plan

16. Print recovery codes and store them offline

Generate recovery codes and store them offline in a protected location.

17. Keep two legitimate recovery routes

Maintain more than one legitimate recovery route where the service allows it.

18. Set clear limits with trusted contacts

Use trusted-contact or emergency-access features with clear boundaries.

19. Back up the vault with a separate secret

Back up the vault or its essential recovery information using an encrypted method.

20. Test the recovery path before you need it

Practice recovery before a real emergency and record official support routes.

Maintaining the Vault and Reviewing Access

21. Review vault health on a calendar

Review vault health and breach alerts on a regular schedule.

22. Revoke old devices and shared access

Remove devices, sharing, and entries that are no longer needed.

23. Keep every security app updated

Keep the operating system, browser, manager, and authentication apps updated.

24. Repeat the full access review each year

Repeat a full access and recovery review every year and after major changes.

Sources

1. Trusting the Tech: Using Password Managers and Passkeys
   https://www.ncsc.gov.uk/blog-post/trust-the-tech-using-password-managers-passkeys-to-help-you-stay-secure-online
2. Use Strong Passwords
   https://www.cisa.gov/secure-our-world/use-strong-passwords
3. Turn On MFA
   https://www.cisa.gov/secure-our-world/turn-mfa
4. Passkeys: What You Need to Know
   https://www.ncsc.gov.uk/passkeys
5. Update Software
   https://www.cisa.gov/secure-our-world/update-software