

Bitwarden Cheat Sheet: Getting Started and Best Practices

A quick-reference handout for new Bitwarden users.

The big idea

Bitwarden is a locked vault for all your logins. You remember **one** strong master password, and Bitwarden creates and remembers a unique password for everything else.

Important: Bitwarden cannot recover or reset your master password. If you forget it and have no recovery plan, the vault cannot be opened.

Set up in 6 steps

1. **Create your account** at bitwarden.com and confirm the verification email.
2. **Choose a master password.** Use a passphrase of 4 or more random words, at least 14 characters long, never used anywhere else (example style: candle-orbit-tractor-melon-sandwich).
3. **Turn on two-step login (2FA)** with an authenticator app or a security key. Save the recovery code somewhere offline.
4. **Install Bitwarden** as a browser extension (official listing by Bitwarden Inc.) and as a mobile app. Pin the extension to your toolbar.
5. **Turn off your browser's built-in password manager** so Bitwarden is the only one in use.
6. **Import your old passwords** from another manager or browser, then delete the exported file, because it is unencrypted.

Everyday skills

- **Log in:** click the Bitwarden icon on a login page and pick the entry, or use autofill.
- **Save a login:** accept Bitwarden's prompt when you sign in or sign up.
- **Generate a password:** use the generator on signup and password-change forms. Aim for 16 or more characters.
- **Organize:** use folders (Banking, Work, Shopping) and favorites.

- **Lock the vault:** lock it when you step away.
- **Store more than logins:** secure notes, cards, and identities.
- **Share safely:** use Bitwarden Send instead of email or chat.

Best practices

Master password and account

- Never share your master password or put it in an email or in the vault.
- If you write it down, keep that copy offline in a safe place.
- Never type it into a website or in response to an unexpected message.
- Change it right away if you suspect it was exposed.

Your passwords

- Every account gets a unique, generated password. No reuse.
- Start replacing old passwords with email, banking, and work accounts. Email comes first because it can reset everything else.
- Use the Vault Health reports to find reused, weak, or exposed passwords, and accounts missing 2FA.

Devices and sessions

- Set a vault timeout of 5 to 15 minutes, with the action set to Lock or Log out.
- Use biometric unlock on phones and laptops, but keep your master password memorized.
- Always use a screen lock on every device.
- Keep the extension and apps up to date.
- Use clipboard auto-clear when copying passwords.
- Never stay logged in on shared or public computers.

Extra protection

- Use 2FA on your email, bank, and Bitwarden account itself. A security key or passkey is strongest where supported.
- Store the 2FA recovery code offline.
- Consider an occasional encrypted export as a backup, kept somewhere secure.

Watch out for

1. A weak or reused master password
2. Forgetting the master password with no recovery plan
3. Skipping 2FA
4. Running the browser's password manager alongside Bitwarden
5. Leaving an unencrypted export file on the desktop
6. Phishing pages. **If autofill does not offer your login, stop and check the web address.**
7. Staying logged in on shared computers

Quick self-check

- What happens if I forget my master password?
- Where is my 2FA recovery code?
- What do I do if autofill does not appear on a login page?
- Is every important account using a unique password and 2FA?

Suggested 45-minute training plan

- **5 min:** why reused and weak passwords are risky
- **10 min:** create the account and master password together
- **5 min:** set up 2FA and save the recovery code
- **10 min:** install the extension and mobile app
- **10 min:** hands-on practice (save a login, autofill one, generate a new password)
- **5 min:** review best practices and answer questions