
NAPLES COMPUTERS HOW-TO · SECURITY & SAFETY

Password Managers: Why You Need One and How to Start

Reusing passwords is one of the easiest ways to get hacked. A password manager creates and remembers a strong, unique password for every account. This guide explains the options (Apple Passwords, Google Password Manager, Microsoft Edge, Bitwarden, 1Password), shows how to save strong passwords and run a password checkup in Chrome and in Apple's Passwords app, and covers passkeys and shared vaults for businesses.

Why reusing passwords is risky

- ☐ One leak unlocks everything
Criminals try a leaked password on email, banks and shopping sites
 - ☐ Every account needs its own
A strong, unique password for each one
 - ☐ Nobody can remember 100 passwords
So let a password manager remember them for you
-

Step by step

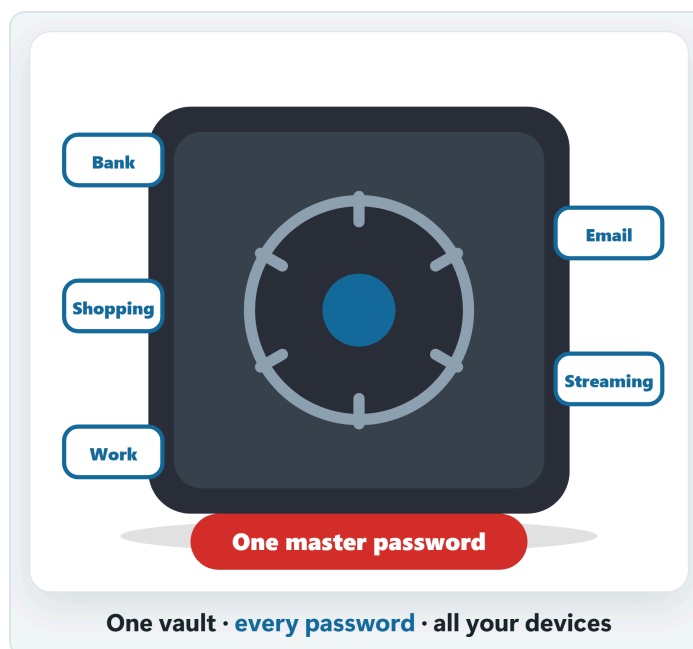
HOW IT WORKS

? A secure vault for all your passwords

A password manager stores your passwords in an encrypted vault, fills them in for you, creates strong new ones, and syncs them across your phone, tablet and computer.

WHAT TO DO

You remember just one strong master password, or unlock it with your fingerprint or face.

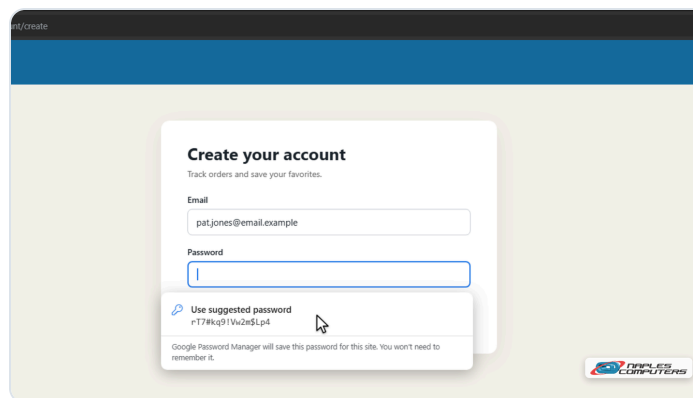


1 Step 1: Let it create a strong password for you

When you create an account in Chrome, click the password box. Chrome offers a strong, random password.

WHAT TO DO

Click Use suggested password. It's saved in Google Password Manager, so you never type or remember it.

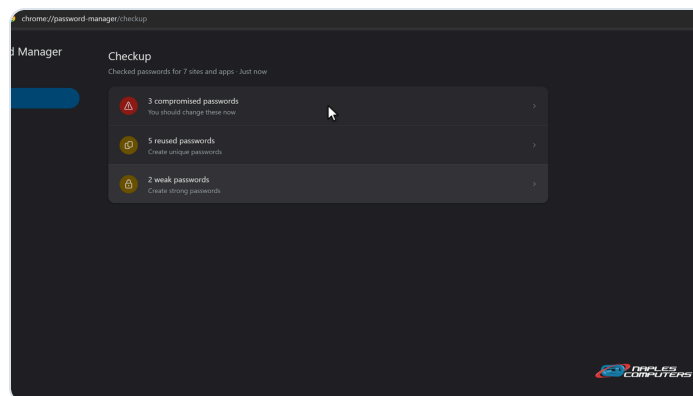


2 Step 2: Run a password checklist

Chrome menu (:) → Passwords and autofill → Google Password Manager → Checkup.

WHAT TO DO

Change compromised passwords first, then reused ones, then weak ones.



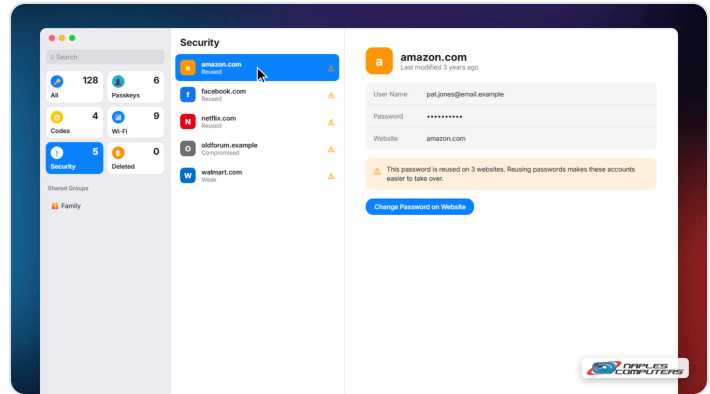
MAC & IPHONE

3 Mac, iPhone & iPad: the Passwords app

Open the Passwords app and click Security to see passwords that are reused, weak, or found in a data leak.

WHAT TO DO

Select one and click Change Password on Website. Safari suggests a strong new password.



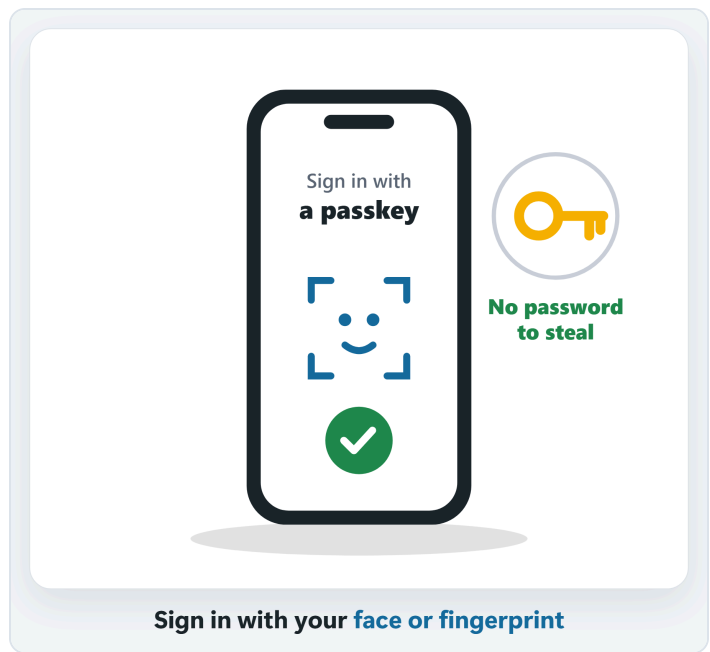
EVEN BETTER

★ Say yes to passkeys

More and more sites offer passkeys. You sign in with your phone or computer's face, fingerprint or PIN unlock, and there's no password to steal or phish.

WHAT TO DO

When a site offers to create a passkey, say yes. Your password manager keeps it in sync.



Which one should you use?

- ☐ Apple Passwords
Built into iPhone, iPad and Mac, and on Windows with iCloud. Free.
- ☐ Google Password Manager
Built into Chrome and Android. Free.
- ☐ Microsoft Edge
Saves passwords to your Microsoft account. Free.
- ☐ Bitwarden or 1Password
Dedicated managers for every device and browser. Bitwarden has a free plan.

The best one is the one you'll actually use.

Keep your vault safe

- ☐ A long master passphrase
Four or more random words, used nowhere else
- ☐ Turn on two-factor authentication
For the password manager and your email
- ☐ Save the recovery key
Print it, and keep it somewhere safe at home
- ☐ No notebooks or spreadsheets
Not next to the computer, not in a file called Passwords

Business tip: shared vaults

- ☐ Share logins securely
No more passwords in emails, texts or sticky notes
- ☐ Each person sees only what they need
Vaults for the office, accounting, management
- ☐ Remove access in one click
When someone leaves, their access goes with them
- ☐ Business plans with admin control
For example Bitwarden Teams or 1Password Business

Recap: password managers

- | | |
|---|---|
| ☐ Never reuse passwords | ☐ Run a checkup, fix the worst first |
| ☐ Pick a password manager | ☐ Say yes to passkeys |
| ☐ Let it create strong passwords | ☐ Protect it with 2FA |

Start small: let your password manager save passwords as you log in, change your email and banking passwords first, and turn on two-factor authentication. For businesses, we set up shared vaults with admin control, so access leaves when an employee does.



Want help setting up a password manager for your family or business?

Call 239-513-1960

naplescomputers.com · **We Make I.T. Happen!**