
RESOURCE 01 | DON'T CLICK YET COMPANION RESOURCE**Password Manager Comparison Worksheet**

Companion resource for Don't Click Yet. Referenced on page 68.

Purpose: Compare password manager options and choose a safer way to store and use strong, unique passwords.

Storage reminder: If you complete this worksheet with sensitive information, store the finished copy somewhere safe.

A password manager can reduce the burden of remembering dozens of passwords. Its job is to help you create, store, and use strong unique passwords without relying on memory, notebooks, reused passwords, or small variations of the same password.

This worksheet is not meant to tell you which password manager to choose. The best choice depends on your comfort level, devices, family needs, budget, recovery options, and the kind of accounts you protect.

Use this worksheet to compare options before choosing one, switching from one, or helping a family member set one up.

What a Password Manager Should Do

A good password manager should help you:

- Create strong unique passwords.
- Store passwords securely.
- Fill passwords into websites and apps when appropriate.
- Work across the devices you actually use.
- Protect the password vault with a strong master password and MFA.
- Help you recover or prepare for emergencies.
- Allow safe sharing when necessary.
- Make everyday sign-ins easier, not more confusing.

A password manager is not a magic shield. It cannot stop every scam. It cannot protect you if you approve a fake login, read a code to a scammer, or ignore warnings from your own accounts. It works best as part of a larger system: unique passwords, MFA, secure devices, safe recovery information, and the habit of verifying suspicious requests.

Before You Compare Products

Answer these questions first. They will help you understand what you need.

Which devices do I use regularly?

- iPhone
- Android phone
- Windows computer
- Mac
- iPad or tablet
- Chromebook
- Shared family computer
- Work computer
- Other: _____

Which browsers do I use?

- Chrome
- Safari

- Edge
- Firefox
- Brave
- Other: _____

Who needs access?

- Only me
- Me and my spouse or partner
- Me and one trusted family member
- Several family members
- Business or freelance use
- Caregiver or emergency contact may need access

What accounts matter most?

- Email
- Banking
- Credit cards
- Phone provider
- Cloud storage
- Password manager itself
- Apple, Google, or Microsoft account
- Payment apps
- Health portal
- Insurance
- Business or client accounts
- Social media
- Other: _____

How comfortable am I with new tools?

- Very comfortable
- Comfortable with guidance
- Nervous but willing to learn
- I need something very simple
- I will need help setting it up

Comparison Table

Use this table to compare up to three password manager options.

Feature	Option 1	Option 2	Option 3
Name of password manager			
Cost			
Free version available?			
Family plan available?			
Works on my phone?			
Works on my computer?			

Feature	Option 1	Option 2	Option 3
Works with my browser?			
Easy to install?			
Easy to use daily?			
Can generate passwords?			
Can store secure notes?			
Can store passkeys?			
Supports MFA for the vault?			
Emergency access available?			
Family sharing available?			
Password health report?			
Breach or reused password alerts?			
Recovery options are understandable?			
Export option available?			
Customer support available?			
Overall comfort level			

Ease of Use

A password manager that is technically strong but too confusing may not help you. If you avoid using it, work around it, or constantly need help, it may not be the right fit.

Use this section after trying each option, watching a tutorial, or helping someone else test it.

Option 1 name:

- I understand how to unlock it.
- I understand how to save a password.
- I understand how to fill a password.
- I understand how to create a new password.
- I understand how to find a saved password.
- I can use it on my phone.
- I can use it on my computer.
- I know what to do if it does not autofill.
- I would feel comfortable using this daily.

Notes:

Option 2 name:

- I understand how to unlock it.
- I understand how to save a password.
- I understand how to fill a password.
- I understand how to create a new password.
- I understand how to find a saved password.
- I can use it on my phone.
- I can use it on my computer.
- I know what to do if it does not autofill.
- I would feel comfortable using this daily.

Notes:

Option 3 name:

- I understand how to unlock it.
- I understand how to save a password.
- I understand how to fill a password.
- I understand how to create a new password.
- I understand how to find a saved password.
- I can use it on my phone.
- I can use it on my computer.
- I know what to do if it does not autofill.
- I would feel comfortable using this daily.

Notes:

Master Password

The master password protects the vault. It should be strong, unique, and memorable enough that you can use it without writing it in an unsafe place.

A good master password is usually longer than an ordinary password. Many people use a passphrase: several unrelated words, possibly with numbers or punctuation, arranged in a way that is memorable to them but not obvious to others.

Do not use:

- A password used anywhere else.
- A family name.
- A pet name.
- A birthday.
- A street address.

-
- A favorite team.
 - A common quote.
 - A phrase visible on your social media.
 - A simple pattern.

Master password plan:

I will create a master password that is:

- Unique
- Long
- Not used anywhere else
- Not based on obvious personal information
- Memorable enough for me to use
- Stored or documented only through a safe emergency method

Where emergency instructions for the master password are stored:

MFA for the Password Manager

Your password manager should be protected with multi-factor authentication if available. This adds another layer if someone learns or guesses the master password.

MFA method I will use:

- Authenticator app
- Security key
- Device prompt
- Passkey
- Text message
- Other: _____

Backup codes stored where:

What I will do if I lose my phone or MFA device:

Recovery and Emergency Access

Password manager recovery can be different from ordinary account recovery. Some password managers cannot recover the vault if the master password is lost. Others offer recovery methods, emergency access, account recovery contacts, or family-plan recovery options.

Before choosing a password manager, understand what happens if:

- You forget the master password.
- You lose your phone.
- Your MFA device is unavailable.
- You become ill or unavailable.
- A spouse, adult child, executor, or trusted person needs emergency access.
- You stop paying for the service.
- You want to switch to another password manager.

Recovery questions to answer:**Can the company recover my vault if I forget the master password?**

- ☐ Yes
☐ No
☐ Not sure

Is emergency access available?

- ☐ Yes
☐ No
☐ Not sure

Can I export my passwords if I need to switch later?

- ☐ Yes
☐ No
☐ Not sure

Do I understand the recovery process?

- ☐ Yes
☐ No
☐ Not yet

Where will I store recovery codes or emergency instructions?

Who, if anyone, should know how to help in an emergency?

Family Sharing

Some households need to share certain passwords safely. Examples may include streaming accounts, utilities, home Wi-Fi information, shared financial accounts, insurance portals, or accounts connected to caregiving.

Do not share passwords by text message, email, sticky notes, or casual chat unless there is no safer option and the risk is understood.

A password manager with sharing features may allow one person to share a password without revealing it in an unsafe way and may allow access to be removed later.

Do I need family sharing?

-
- Yes
 - No
 - Not sure

Who needs shared access?

1. _____
2. _____
3. _____

Which accounts may need to be shared?

Which accounts should remain private?

Secure Notes and Documents

Some password managers allow secure notes or document storage. This may be useful for:

- Backup codes
- Router information
- Software license keys
- Emergency instructions
- Passport or identity document notes
- Insurance details
- Account recovery notes
- Family verification phrase reminder
- Device passcode emergency notes, if appropriate

Be careful with highly sensitive documents. A password manager can be a secure place for some information, but you should understand how it is protected, backed up, and recovered.

Information I may store as secure notes:

Information I should store somewhere else:

Built-In Browser Password Managers

Browsers and device ecosystems often include built-in password managers. These may be convenient and may be appropriate for some users, especially if they stay within one device ecosystem and protect that account carefully.

Before relying only on a built-in option, consider:

- Does it work across all devices I use?
- Does it work across all browsers I use?
- Is the account protecting it secured with MFA?
- Can I share passwords safely if needed?
- Can I export passwords if I switch later?
- Do I understand how recovery works?
- Is it clear where my passwords are stored?

Built-in option I currently use, if any:

Do I want to continue using it?

- Yes
- No
- Not sure

Reason:

Switching From an Old System

You may currently use a notebook, browser-saved passwords, memory, reused passwords, a spreadsheet, or a mix of several methods. Do not try to move everything in one day unless you are comfortable doing so.

Start with the most important accounts:

1. Main email
2. Bank and credit cards
3. Phone provider
4. Password manager account itself
5. Apple, Google, or Microsoft account
6. Cloud storage
7. Payment apps
8. Health portal
9. Insurance and tax accounts
10. Business or freelance accounts

My first five accounts to move into the password manager:

1. _____
2. _____

3. _____
4. _____
5. _____

Date started:

Trusted person helping, if any:

Trial Period Notes

Use the password manager for at least a few days before making a final decision if possible. Try it on your phone, computer, browser, and a few common accounts.

What worked well:

What confused me:

What I need help with:

Would I recommend this to someone like me?

- Yes
- No
- Maybe

Why:

Final Decision

Password manager chosen:

Plan type:

- Free
- Individual paid
- Family
- Business
- Not sure

Date chosen:

Master password created and stored safely?

- Yes
- No
- Not yet

MFA turned on?

- Yes
- No
- Not yet

Backup codes saved?

- Yes
- No
- Not yet

Emergency access or recovery plan created?

- Yes
- No
- Not yet

First five important accounts moved?

- Yes
- No
- In progress

Final Reminder

The best password manager is the one you can use correctly and consistently.

Do not wait for the perfect system before improving the accounts that matter most. Start with your main email, financial accounts, phone provider, cloud storage, and payment apps. Every unique password you create reduces the chance that one stolen password becomes a larger problem.