



Password Managers

Hillingdon u3a Computer Club

April 2024

Why

- Creating a weak password is too easy.
- Then Reusing that password becomes even easier.
- **What must we not do is..... *Reuse Passwords!***
- Password leaks occur a lot, even on large websites.
- These can provide malicious individuals with your email address, username, and password.
- If you use the same login information everywhere, one leak could give the hacker access to other accounts.
- With this they could reset access other websites, like your online banking or PayPal account.

Why

- So how are you supposed to use strong, unique passwords on all the websites you use?
-The solution is a **Password Manager**.
- You can then prevent password leaks from being so damaging as you can use a unique password on every website.
- Of course, these would be strong passwords i.e. long, unpredictable combination of letters that also contain numbers and symbols.

What is it

From Wikipedia.....

- A password manager is a computer program that allows users to store and manage their passwords for local applications or online services such as web applications, online shops or social media.
- Password managers can generate passwords and fill online forms
- The main purpose of password managers is to alleviate the issue known as password fatigue, where a user can become overwhelmed from remembering multiple passwords
- Password managers typically only require one "master" password which unlocks and gives access to the data.

What Do You Do ?

- Only use one Password for everything
- Perhaps 5-6 passwords. A bit of trial & error to get the right one.
- Post-It Notes
- Spiral Notebook 3"x 5", possibly in sections, perhaps over a couple of books
- Saving passwords in the browser
- Perhaps a combination of Notebook and Browser
- Word document or Spreadsheet (No password or backed up)
- If you can remember a password, it's easy to crack

The Better Solution

- A Password Management application on your device (or in the cloud)
- Available in Free or Paid for options
- They include Radom Password Generators
- Only One Password to remember *
- Some managers allow database sync across devices

The Better Solution

Any password manager you choose should be easy for you to use.

If you find yourself going back to your old, insecure password habits, maybe it's time to find a password manager that better fits your needs.

There are many products to choose from, and taking a little time to find the right password manager to protect your logins can save you a lot of frustration in the future.

LastPass

- We have to mention the Cloud based Password Manager Service – Last Pass
- They had a major data breach August 2022
- Certificates, secret scripts used to access backup storage and encrypted customer data.
- If the recommended setups were used then password hash data would be safe.
- The Computer media all recommended resetting the master password to very complex, other key passwords and withdrawing from the service.

Options 1

- All password managers have a unique interface. Use free trials to assess which is best for you.
- I use KeePass on both my devices Win10 & Mac
- Completely Free
- Extensive plugin support
- Full Control of your Data
- Old Interface Design (since 2003)
- It's the best password manager option if you want to maintain complete control of your data.

Keepass



Create Composite Master Key

C:\Users\Sean\Documents\Keepass Database\Database.kdbx

Specify the composite master key, which will be used to encrypt the database.

A composite master key consists of one or more of the following key sources. All sources you specify will be required to open the database. If you lose one source, you will not be able to open the database anymore.

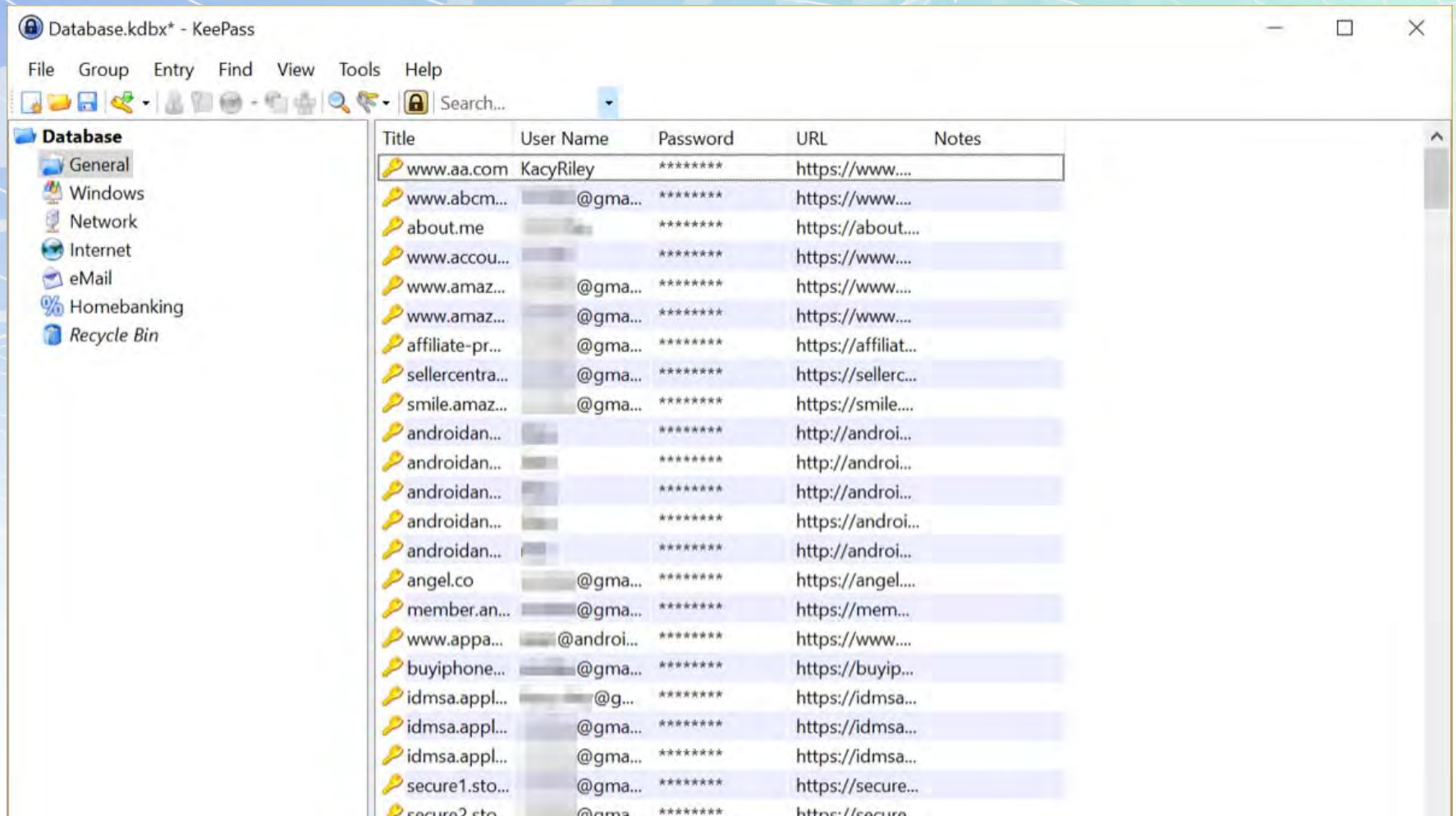
☒ **Master password:** 

Repeat password:

Estimated quality:  81 bits 16 ch.

☐ Show expert options:

KeePass



Keepass



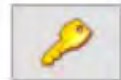
Add Entry

Create a new entry.

Entry Advanced Properties Auto-Type History

Title:

Icon:



User name:

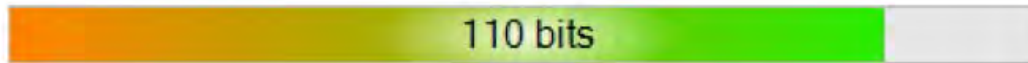
Password:



Repeat:



Quality:



20 ch.

URL:

Notes:

KeePass

Supports.....

- Sync with online storage i.e. Dropbox to host the database
- Password generation management
- Syncing via local hard disks or network shares
- Auto-type form-filling and auto-type hot-key form filling.

To unlock the full power of KeePass, you really need to install plugins and extensions.

KeePass



KeePass
Password Safe

Home

- Home & News
- Forums
- Feature List
- Screenshots

Getting KeePass

- Downloads
- Translations
- Plugins / Ext.

Information / WWW

- Help
- FAQ
- Security
- Awards
- Links

Support KeePass

- Donate

KeePass Plugins and Extensions

Information about the plugin framework (installing plugins, security, ...) can be found on the help pages '[KeePass 1.x Plugins](#)' and '[KeePass 2.x Plugins](#)'.

I/O & Synchronization

IOProtocolExt [?](#)
Adds support for SCP, SFTP and FTPS.

SftpSync [?](#)
Adds support for SFTP and SCP.

KeeAnywhere [?](#)
Adds support for online storage providers.

KeeCloud [?](#)
Adds support for online storage providers.

KeePassSync [?](#)
Synchronize using online storage providers.

KPDataSave (Dropbox) [?](#)
Save your database in Dropbox.

KPGoogleSync [?](#)
Synchronize using Google Drive.

KeePassOneDriveSync [?](#)
Synchronize using OneDrive.

CyberGate Password Vault Plugin [?](#)
Adds support for communicating with CyberGate Password Vault.

Backup

Another Backup Plugin [?](#)
Creates backups of databases.

DB_Backup [?](#)
Creates backups of databases.

DataBaseBackup [?](#)
Creates backups of databases.

KPSimpleBackup [?](#)
Creates backups of databases.

SimpleDatabaseBackup [?](#)
Creates backups of databases.

Integration & Transfer

KeeForm [?](#)
Opens websites and fills in the login data automatically.

Kee [?](#)
Bridge between KeePass and web browsers.

PassIFox [?](#)
Replaces the built-in Firefox password storage by KeePass.

ChromeIPass [?](#)
Integrates KeePass and the Google Chrome browser.

Passafari [?](#)
Integrates KeePass and the Safari browser.

URL in Title Bar [?](#)
Browser extensions that show the current URL in the title bar (for multiple browsers).

KeePasser [?](#)
Allows auto-typing into webforms based on URLs (Internet Explorer and Maxthon).

KPFloatingPanel [?](#)
Displays an always on top KeePass floating panel.

KeePassHelper [?](#)
Browser extension that retrieves credentials from KeePass.

WebAutoType [?](#)
Allows auto-typing into webforms based on URLs (multiple browsers).

RDCAutoTypeAndTCATO [?](#)
RDC auto-type support and improved TCATO selection.

TCATO Placeholder [?](#)
Allows to enable/disable TCATO per auto-type sequence.

HotKeyEnabler [?](#)

Import

1P2KeePass [?](#)
Imports 1Password 1PIF files.

AnyPassword Import [?](#)
Imports CSV files exported by 'AnyPassword'.

CardFileKPPlugin [?](#)
Imports CRD files created by 'Cardfile'.

CodeWallet 3 Import [?](#)
Imports TXT files exported by 'CodeWallet 3'.

CodeWallet 6 Konverter [?](#)
Converts TXT files exported by 'CodeWallet 6' to importable CSV files.

eWallet Import [?](#)
Imports TXT files exported by 'eWallet'.

eWallet Data Liberator [?](#)
Export data from 'eWallet' and import it into KeePass.

eWallet2KeePass [?](#)
Migrate 'eWallet' data to KeePass.

KeePassBrowserImporter [?](#)
Imports credentials from various browsers.

KeePassFirefoxImporter [?](#)
Imports passwords from Firefox.

MSDN/TechNet Key Importer [?](#)
Imports MSDN/TechNet key files.

OnePIF [?](#)
Imports 1Password 1PIF files.

Oubliette Import [?](#)
Imports Oubliette password database files.

PasscommImport [?](#)
Imports Password Commander CSV files.

Password Minder Import [?](#)
Imports Password Minder data.

PINs Import [?](#)
Imports text files exported by 'PINs'.



Enterprise Version of KeePass

KeePass with LDAP/ AD Integrations.

Simple & Easy setup with Free demo.

Experience It

Synchronize KeePass to a Server.

There are more than 100 KeePass plugins and extensions

Options 2

- All password managers have a unique interface. Use free trials to assess which is best for you.
- I now recommend Bitwarden
- Free and Premium versions
- Open Source and very secure
- Windows, Mac, iOS, Android, Linux
- Unlimited syncing across all devices on free version

Bitwarden

 Password Manager

Vaults

Send

Tools

Reports

Settings

My account

Security

Preferences

Subscription

Domain rules

Emergency access

Security

Master password

Two-step login

Keys

Change master password

 **WARNING**

Proceeding will log you out of your current session, requiring you to log back in. Active sessions on other devices may continue to remain active for up to one hour.

Current master password

New master password

Confirm new master password

Important: Your master password cannot be recovered if you forget it! 12 character minimum

☒ Check known data breaches for this password

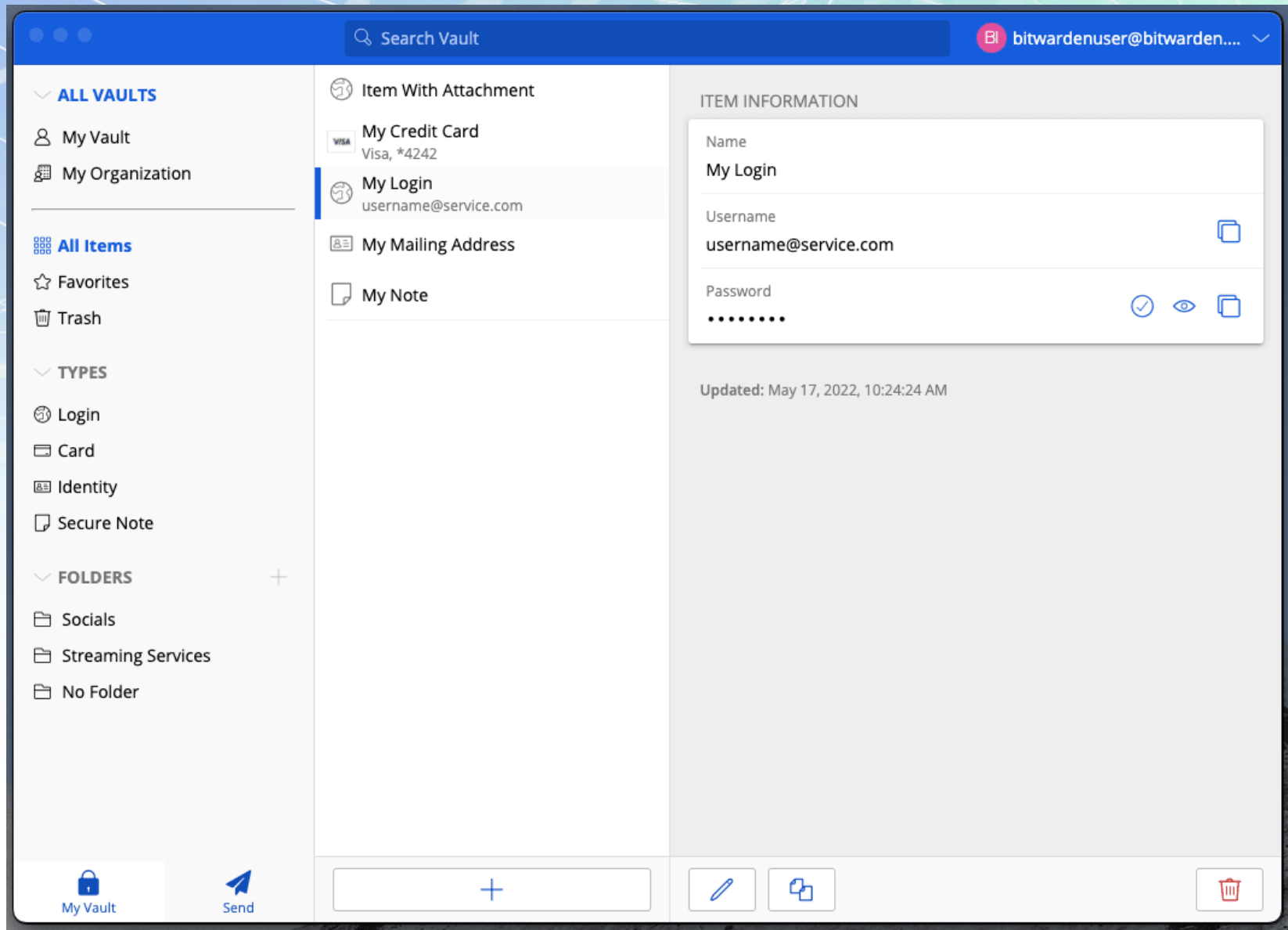
☐ Also rotate my account's encryption key 

Master password hint

Change master password

fppt.com

Bitwarden



Bitwarden

Bitwarden Password Manager interface showing the "NEW ITEM" dialog box.

Left Sidebar (Navigation):

- Password Manager
- Vaults
- Send
- Tools
- Reports
- Settings

Background (All vaults):

- FILTERS**
- Search vaults
- All vaults**
 - My vault
 - My Organ
 - New orga
- All items**
 - Favorites
 - Login
 - Card
 - Identity
 - Secure no
- Folders**
 - My Folder
 - No folder

NEW ITEM Dialog Box:

What type of item is this?
Login

Name: My login item
Folder: My Folder

Username: my_username
Password: [Masked] [Copy] [Eye] [List]

Authenticator key (TOTP): otpauth://totp/..... [15] [Copy]

URI 1: https://www.website.com [Copy] [List]
Match detection: Default match detection [Info] [Close]

+ New URI

Bitwarden

 Password Manager

Vaults

Send

Tools

Generator

Import data

Export vault

Reports

Settings

Generator

T8\$rDV@5we*Ch3t^m6

What would you like to generate?

☒ Password ☐ Username

Password type

☒ Password ☐ Passphrase

Length	Minimum password length	Minimum numbers
18	18	2

Minimum special

Options

☒ A-Z

☒ a-z

☒ 0-9

☒ !@#\$\$%^&*

☒ Avoid ambiguous characters

Regenerate password

Copy password



Bitwarden

The screenshot shows the Bitwarden web application interface. At the top is a blue navigation bar with the Bitwarden logo and links for 'Vaults', 'Send', 'Tools', and 'Reports'. On the right of this bar are icons for account settings, a team icon, and a help icon. A left-hand sidebar contains a 'TOOLS' section with links for 'Generator', 'Import data' (which is highlighted with a blue bar), and 'Export vault'. The main content area is titled 'Import data'. It contains three dropdown menus: 'Import destination' (set to 'My vault'), 'Folder' (set to '-- Select a folder --'), and 'File format' (set to '-- Select --'). Below the 'Folder' dropdown is a text instruction: 'Select this option if you want the imported file contents moved to a folder.' The 'File format' dropdown menu is currently open, displaying a list of supported formats: Bitwarden (json), Bitwarden (csv), Chrome (csv), Dashlane (csv), Firefox (csv) (which is highlighted), KeePass 2 (xml), and LastPass. At the bottom of the form is a blue button labeled 'Import data'.

TOOLS

- Generator
- Import data**
- Export vault

Import data

Import destination ⓘ (required)

My vault

Folder

-- Select a folder --

Select this option if you want the imported file contents moved to a folder.

File format (required)

-- Select --

- Bitwarden (json)
- Bitwarden (csv)
- Chrome (csv)
- Dashlane (csv)
- Firefox (csv)
- KeePass 2 (xml)
- LastPass

Import data