SUN CITY SUMMERLIN COMPUTER CLUB

Passwords
&
KeePass Password Manager

Jeff Wilkinson
August 12, 2023

- Passwords
  - Creating
  - Lost or forgotten, recovery options
  - 2FA – Two Factor Authentication
- Password Mangers
- Why do you need a password manager?, Benefits.
- Are password managers safe?
- Setting Up and Using KeePass
  - Download and install
  - Local vs Cloud
  - Features
- Final thoughts

Adam Cerious
@Browtweaten
hacker: I have all your passwords
me: omg thank you, what are they

- Passwords are essential - we use them to access social media, email, banking, and other online services.

- Passwords are essential - we use them to access social media, email, banking, and other online services.
- Passwords are your first line of defense against unauthorized access to your computer and personal information.

- Passwords are essential - we use them to access social media, email, banking, and other online services.
- Passwords are your first line of defense against unauthorized access to your computer and personal information.

Passwords should be strong, and unique to protect your privacy and security.

- Passwords are essential - we use them to access social media, email, banking, and other online services.

- Passwords are your first line of defense against unauthorized access to your computer and personal information.

  Passwords should be strong, and unique to protect your privacy and security.

  Reusing, rotating, or using weak passwords can leave you vulnerable to hackers

In 2022, the most common password out of more than 15 billion retrieved from publicly leaked data breaches was 123456, according to a Cybernews.com analysis. No. 2 was 123456789, followed by qwerty and password!!

- Don’t Use Words in the Dictionary

- Don’t Use Words in the Dictionary
- Don’t use kids or pets names

- Don’t Use Words in the Dictionary
- Don’t use kids or pets names
- Don’t use dates such as birthday or anniversary

- Don’t Use Words in the Dictionary
- Don’t use kids or pets names
- Don’t use dates such as birthday or anniversary
- Can use a unique phrase unique to you

Cybercriminals can crack weak passwords easily by purchasing sets of common passwords on the dark web. They sometimes get clues by looking at your social media posts or phishing for information from you through bogus emails.

- To create a strong password:
  - Microsoft says at least 12 characters long, 14 is better!!

- To create a strong password:
  - Microsoft says at least 12 characters long, 14 is better!!
  - This would strongly suggest a password manager

- To create a strong password:
  - Microsoft says at least 12 characters long, 14 is better!!
  - This would strongly suggest a password manager
  - Upper and Lowercase letters, numbers & symbols

- To create a strong password:
  - Microsoft says at least 12 characters long, 14 is better!!
  - This would strongly suggest a password manager
  - Upper and Lowercase letters, numbers & symbols
  - Not a name, word found in dictionary, character, product or organization

- To create a strong password:
  - Microsoft says at least 12 characters long, 14 is better!!
  - This would strongly suggest a password manager
  - Upper and Lowercase letters, numbers & symbols
  - Not a name, word found in dictionary, character, product or organization
  - Unique – don’t repeat passwords
    - May be ok for “throwaway sites” that don’t have any personal info

- To create a strong password:
  - Microsoft says at least 12 characters long, 14 is better!!
  - This would strongly suggest a password manager
  - Upper and Lowercase letters, numbers & symbols
  - Not a name, word found in dictionary, character, product or organization
  - Unique – don't repeat passwords
    - May be ok for "throwaway sites" that don't have any personal info

  Consider a memorable phrase meaningful to you
  - *Itwa$aD@rkday&yEt93pe0plec@me*

- November 2022 Survey*:
- About 30% write their passwords on sticky notes
- Some 40% say they memorize them
- 20% say they use same password for all their sites!!!

*November 2022 online survey Security.org

Password safety tips

Apart from creating a strong password, there are other measures you can take to ensure your password is safe. Here are some tips:

- Never share your password with anyone.
- Use a **password manager** to store your passwords securely.
- Enable two-factor authentication for added security.
- Change your password regularly.
- Avoid using public Wi-Fi to access your critical accounts.

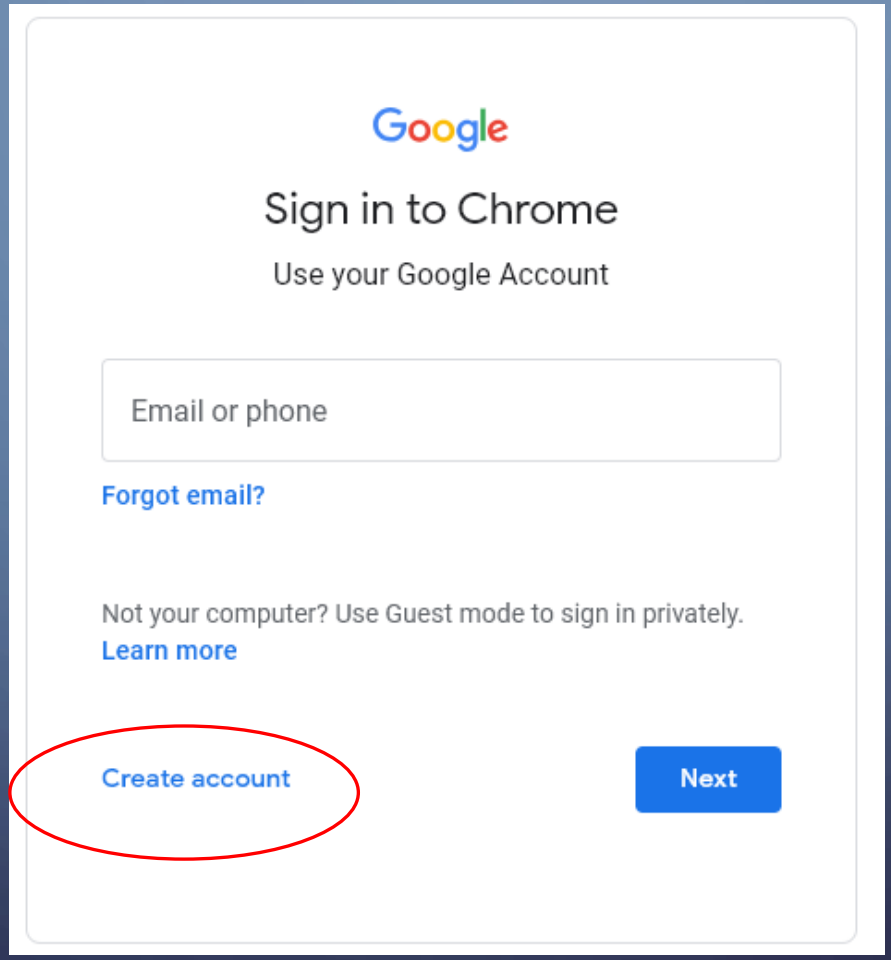
The amount of time it takes to crack a password depends on a number of factors, including the length and complexity of the password, the computing power of the attacker, and the availability of pre-computed rainbow tables or dictionaries.

In general, longer and more complex passwords are more difficult to crack. For example, a 12-character password that uses a mix of upper and lowercase letters, numbers, and symbols can take over 34,000 years to crack, even with a powerful computer!

Password Recovery

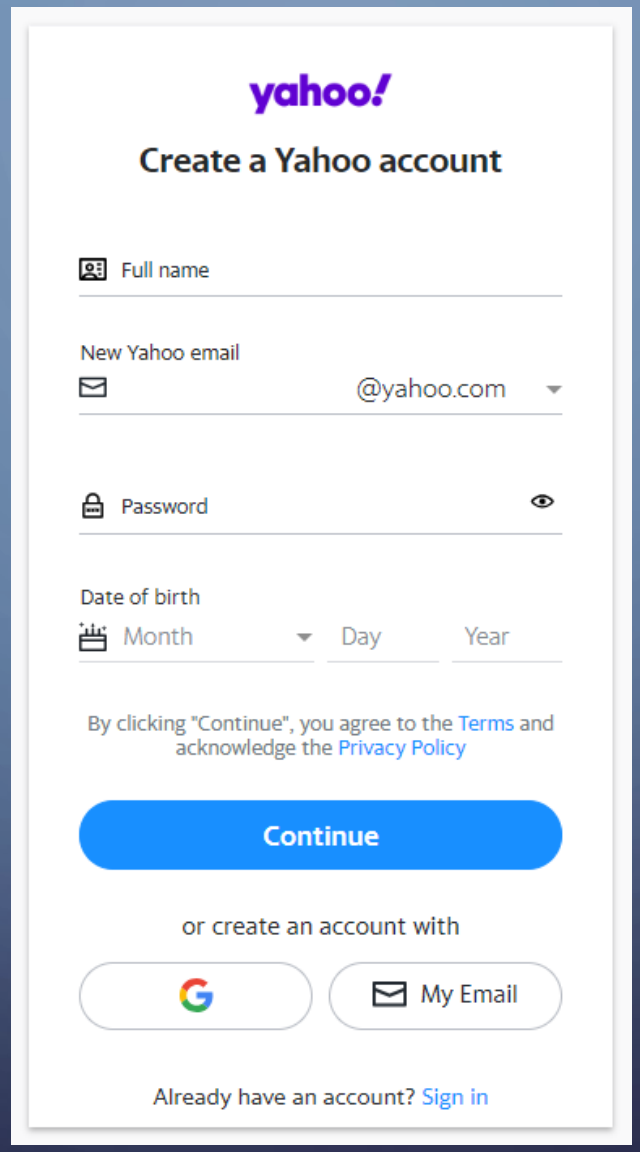
- Use or create recovery email account
  - Gmail, Yahoo, Outlook, AOL
  - Provide recovery email for this new account also
  - Provide phone number that is able to receive texts

Create Gmail account



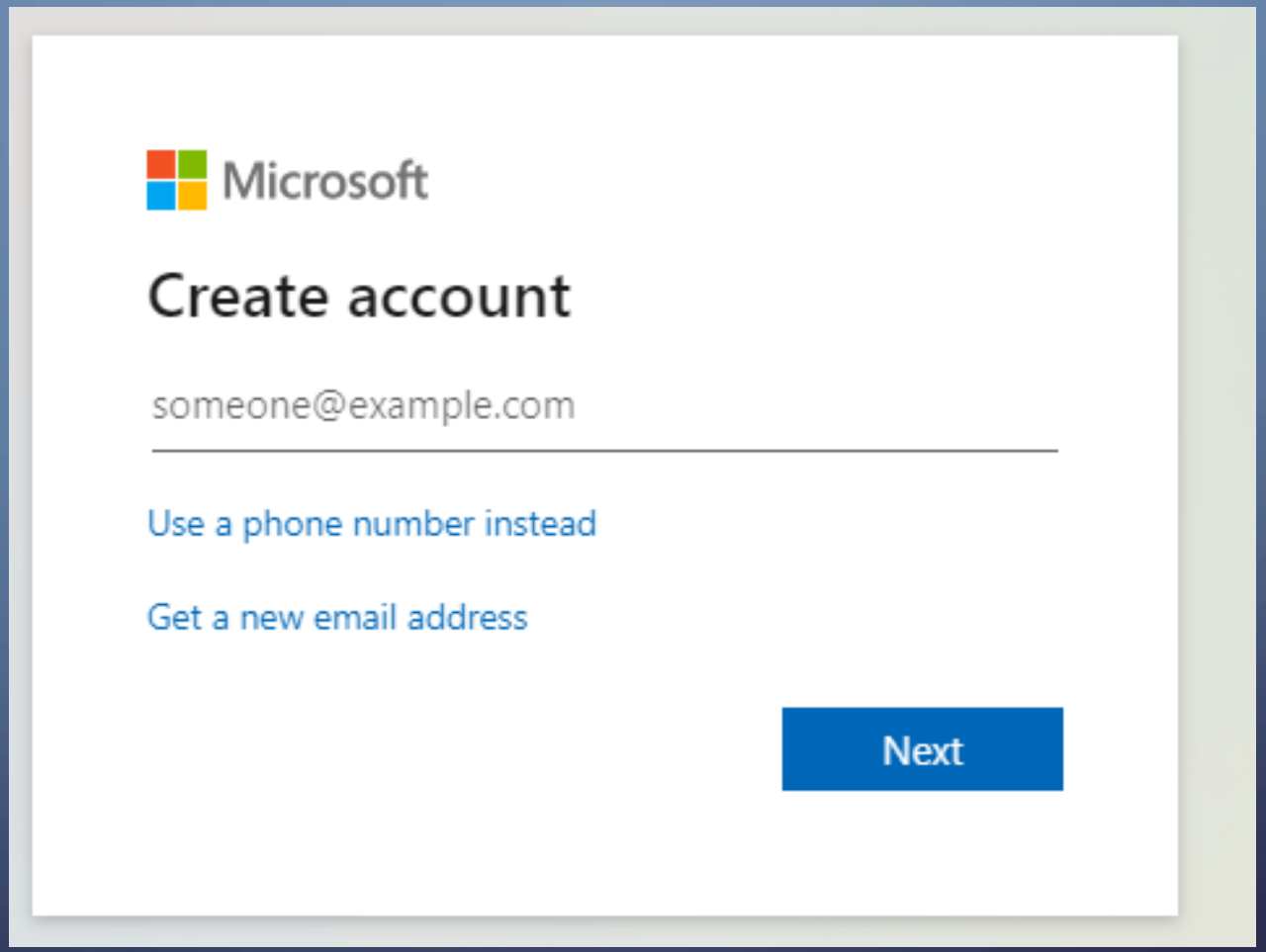
SUN CITY SUMMERLIN COMPUTER CLUB

https://login.yahoo.com/account/create



SUN CITY SUMMERLIN COMPUTER CLUB

https://signup.live.com/signup



Two-factor authentication, adds a layer of security on top of your password with a one-time code that's sent to your mobile phone.

Even with 2FA, it a good habit to change your critical passwords regularly.

Another reason to get your accounts organized and your passwords secure is that it will help your loved ones deal with your affairs when necessary.

PLAN AHEAD

So, it takes some organization to follow these suggestions religiously.

Take it one step at a time

What is a Password Manager?

A **password manager** is an efficient and secure searchable database which can keep track of all your log-in details for multiple accounts.

Why do you need a Password Manager

Most people tend to use weak passwords that are easily guessed and to reuse them on several different websites, making them targets for hacking and identity theft. If you use the same password for your email, bank, social media, and healthcare accounts, an identity thief who found your login info on the **dark web** would be able to access all kinds of sensitive information with a single username and password.

Using a password manager to store strong, unique passwords you don't have to commit them all to memory, keep a tattered notebook or multiple post-it notes.

Access your stored passwords with a **master password** that lets you into the manager to access your saved information.

Use of a password manager allows you to create the most effective passwords and store them for easy retrieval and use in an encrypted file accessible with a single strong password.

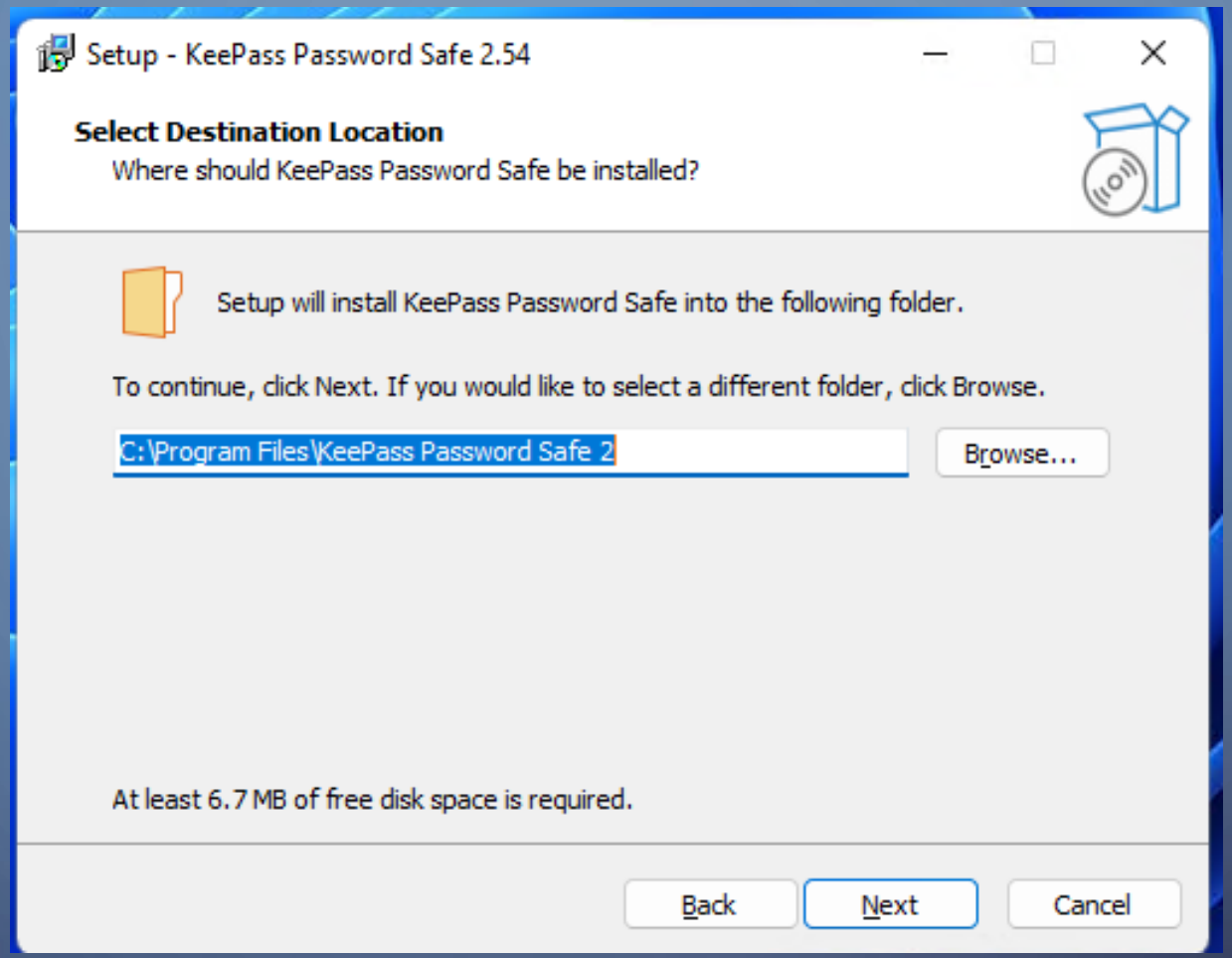
- I have used a product called KeePass for over 25 years
- It is an Open Source, FREE program which stores your encrypted data locally.
- You can choose to store in the cloud, such as Google Drive, for access across platforms.
- Apps are available for all platforms

- There are many other password managers available
- Some are cloud based and require an annual subscription
- Many are part of a total package
- We will focus on KeePass since it's FREE and I used it for a long time.

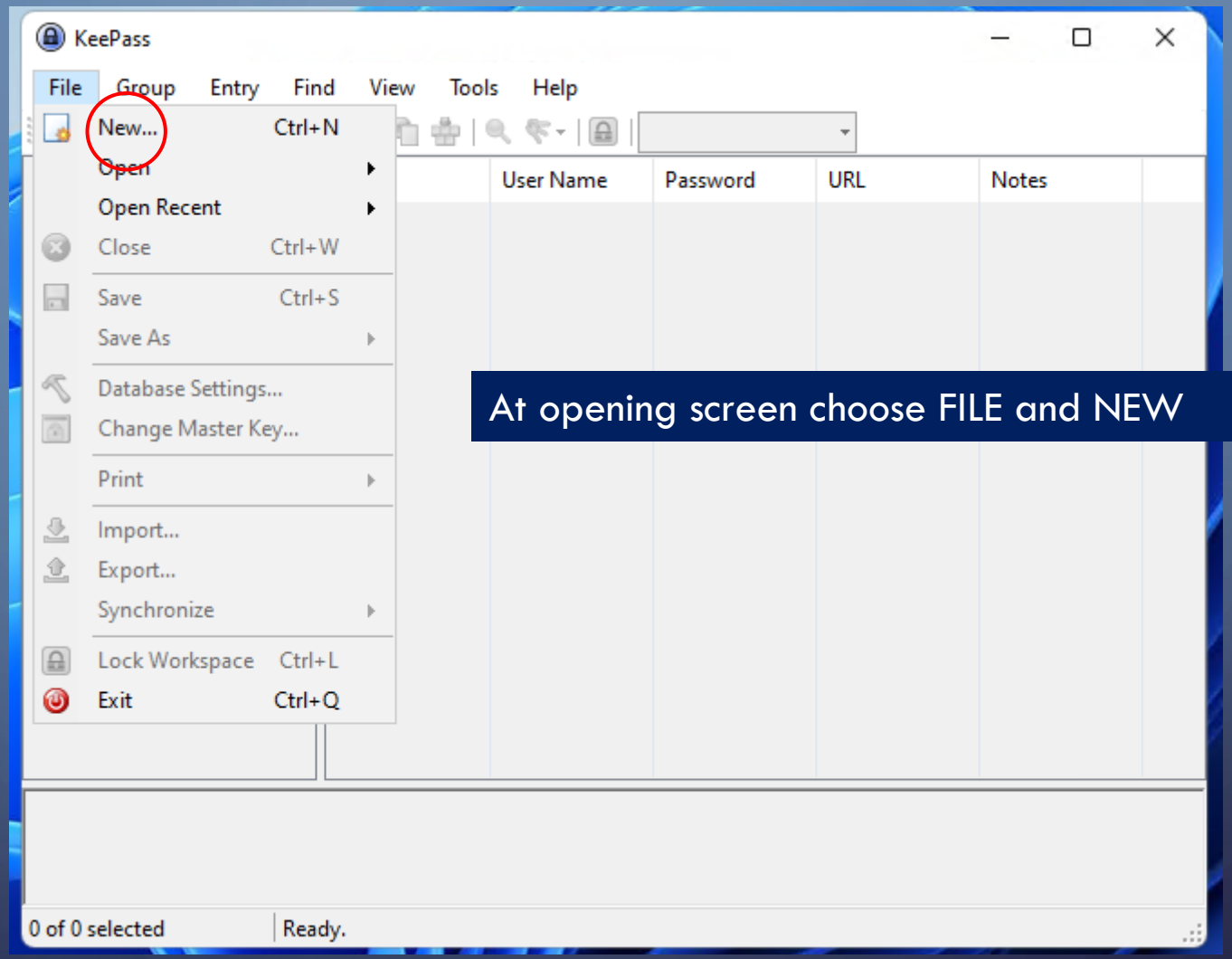
- Download from http://keepass.info/download.html

When the download is complete, run the

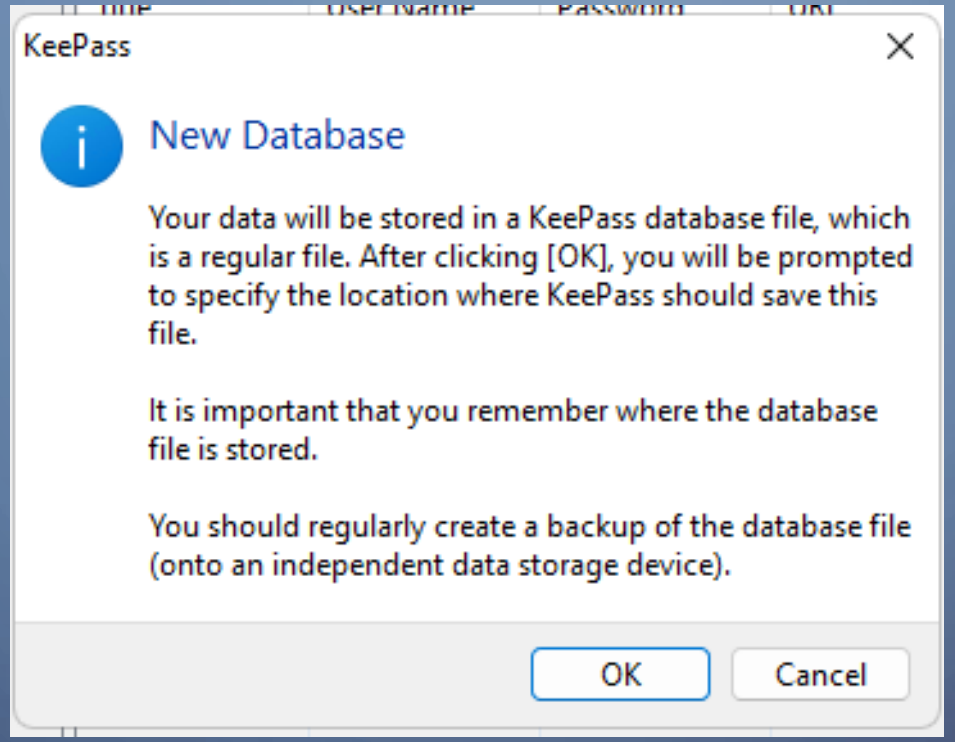
KeePass-2.54-Setup.exe file



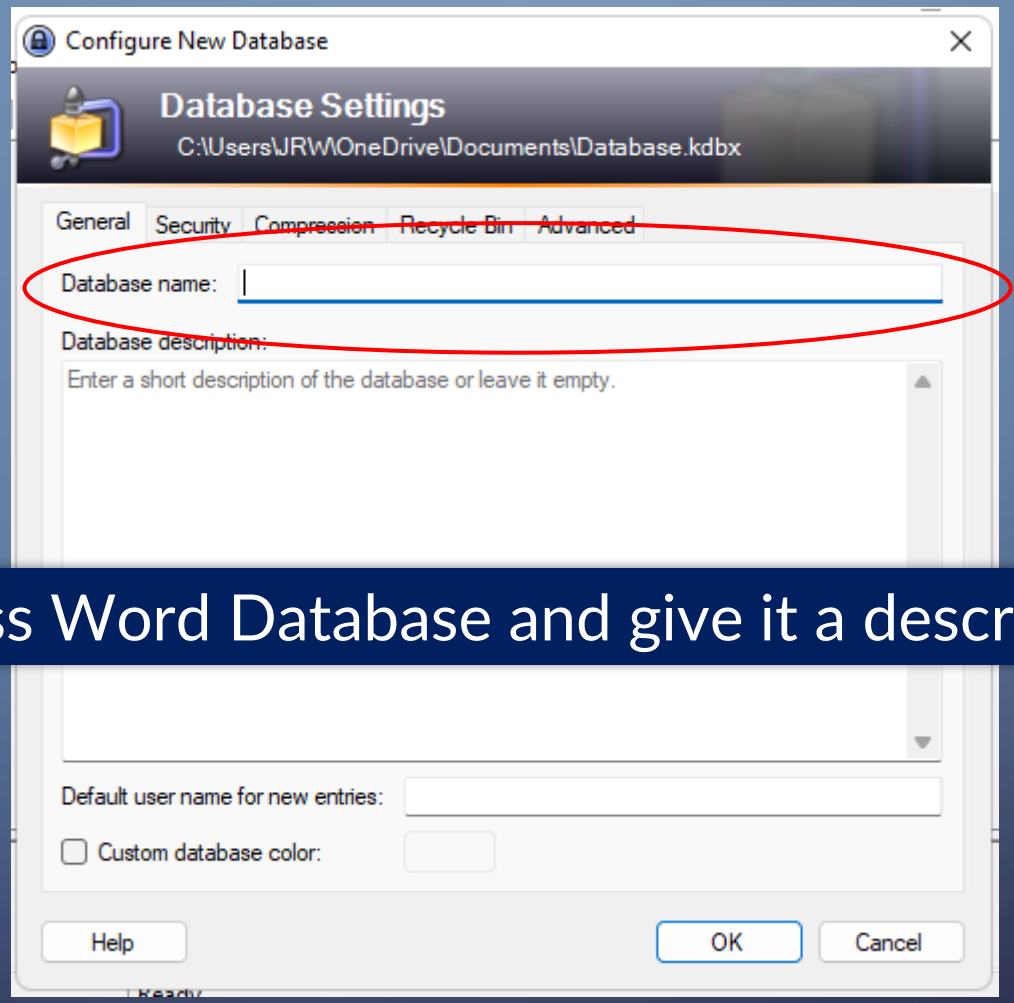
Choose defaults for all options and continue to complete installation



At opening screen choose FILE and NEW


KeePass
New Database
Your data will be stored in a KeePass database file, which is a regular file. After clicking [OK], you will be prompted to specify the location where KeePass should save this file.
It is important that you remember where the database file is stored.
You should regularly create a backup of the database file (onto an independent data storage device).
OK
Cancel

Create a master password – these are the "keys to the kingdom" Use care in creating this, if you forget this, you will not be able to access any of your saved passwords!!



Name your Pass Word Database and give it a description if you like

KeePass
Emergency Sheet

7/15/2023

Database file:

F:\Data\Computer Club\Password Managers and Info\Sample Keepass db file\Passwords Class Sample Database.kdbx

You should regularly create a backup of the database file (onto an independent data storage device). Backups are stored here:

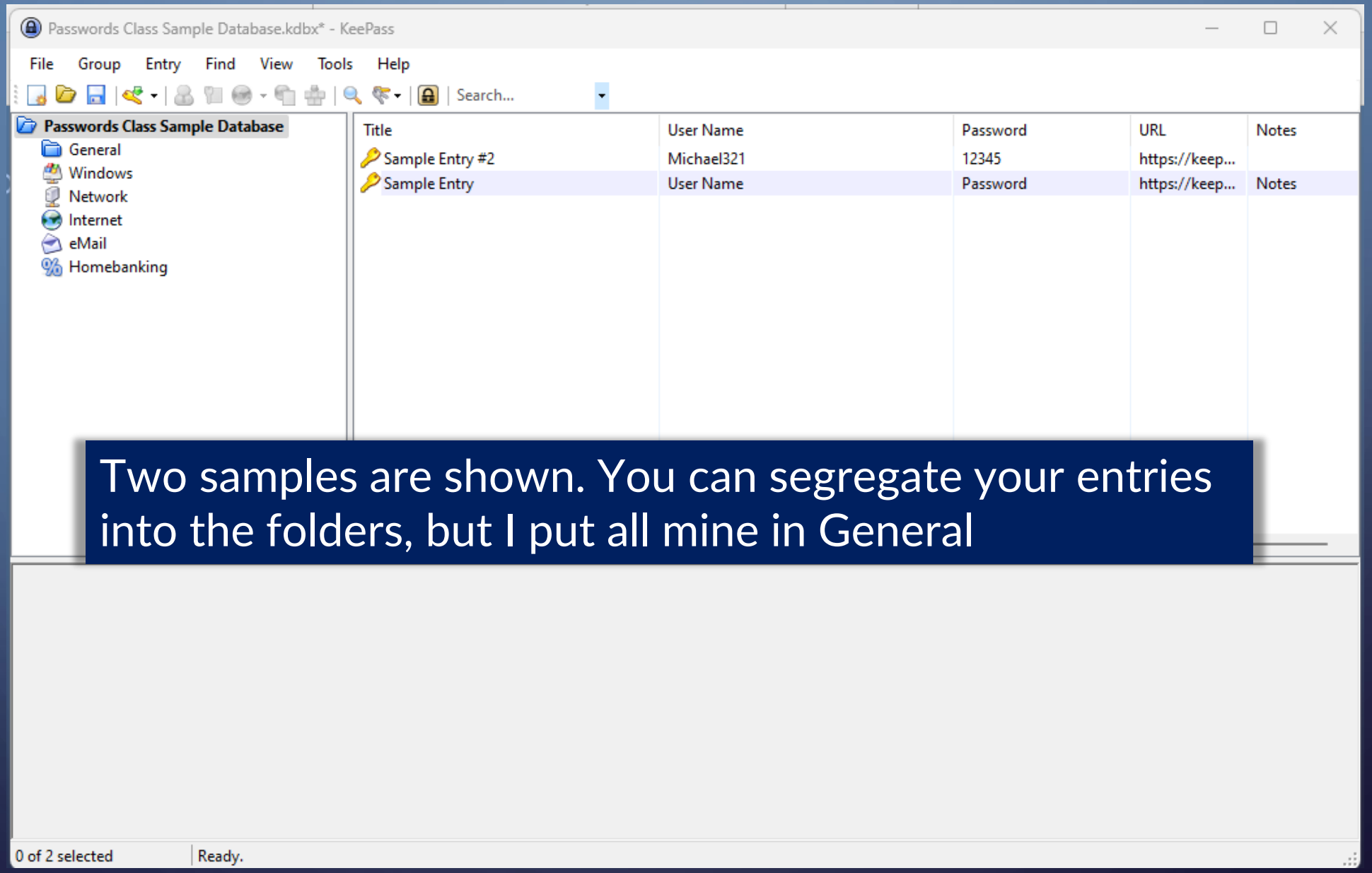
Master Key

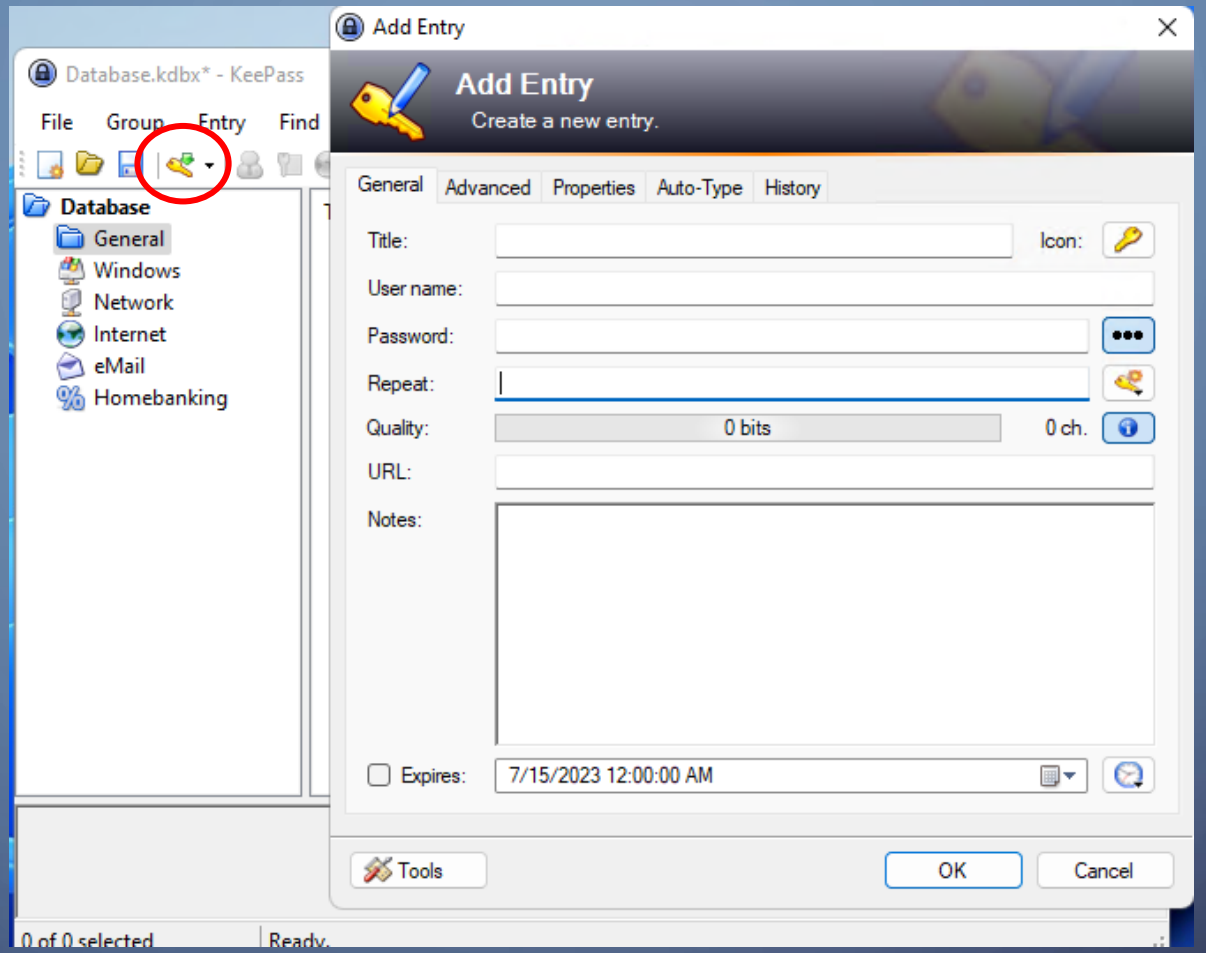
The master key for this database file consists of the following components:

- **Master password:**

Instructions and General Information

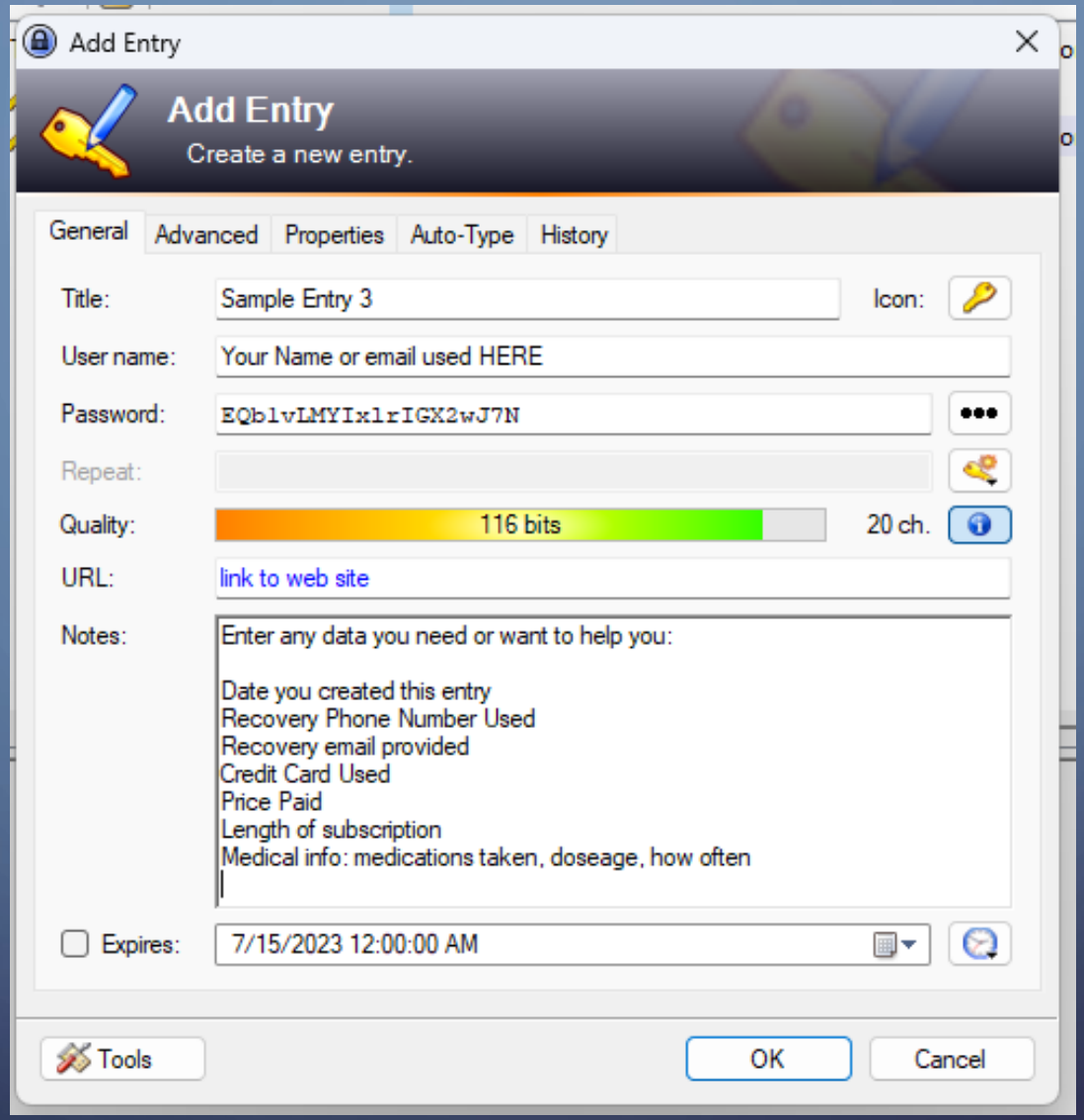
- A KeePass emergency sheet contains all important information that is required to open your database. It should be printed, filled out and stored in a secure location, where only you and possibly a few other people that you trust have access to.
- If you lose the database file or any of the master key components (or forget the composition), all data stored in the database is lost. KeePass does not have any built-in file backup functionality. There is no backdoor and no universal key that can open your database.
- The latest KeePass version can be found on the KeePass website: https://keepass.info/.


Passwords Class Sample Database.kdbx* - KeePass
File Group Entry Find View Tools Help
Search...
Passwords Class Sample Database
General
Windows
Network
Internet
eMail
Homebanking
Title User Name Password URL Notes
Sample Entry #2 Michael321 12345 https://keep...
Sample Entry User Name Password https://keep... Notes
Two samples are shown. You can segregate your entries into the folders, but I put all mine in General
0 of 2 selected
Ready.

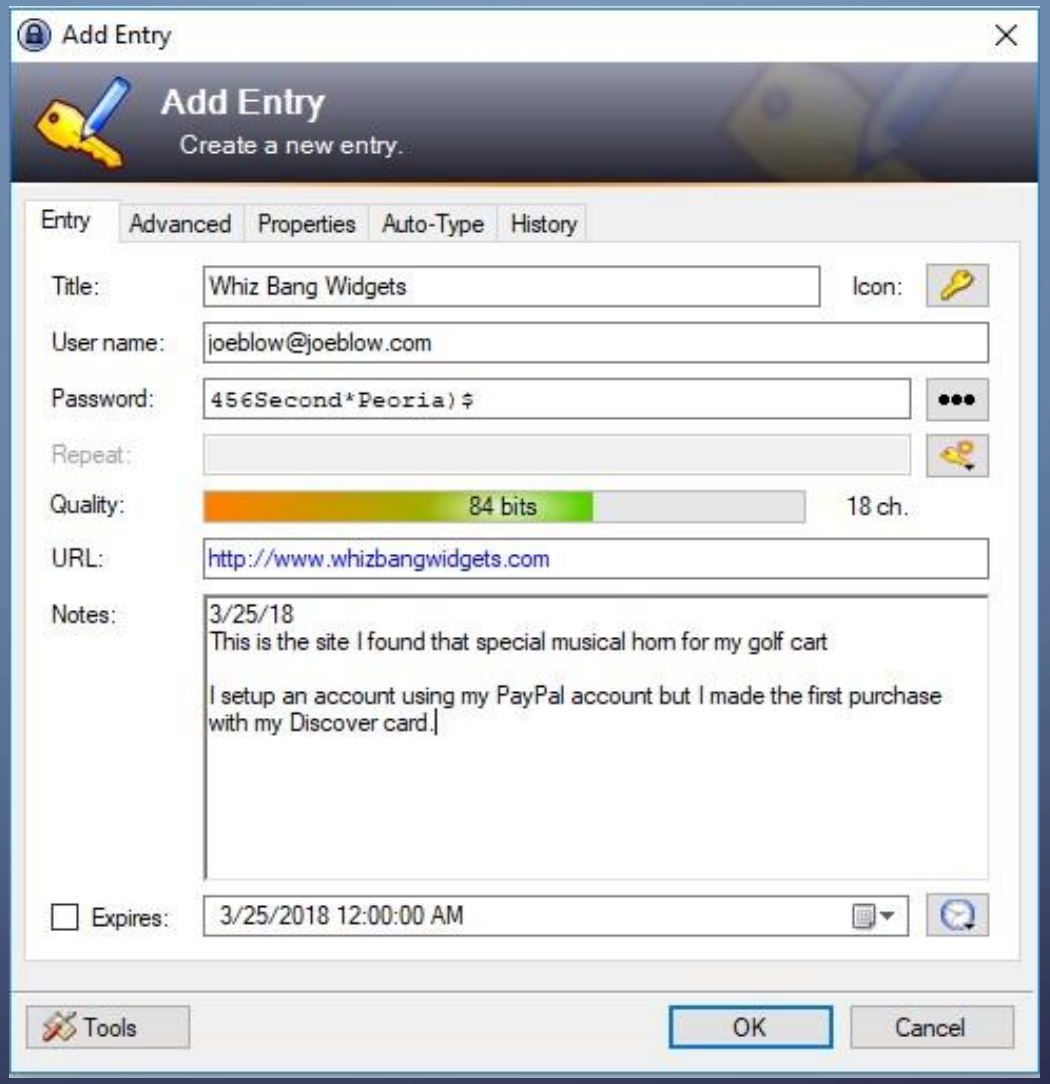


Left click on the Yellow Key icon to add an entry.

SUN CITY SUMMERLIN COMPUTER CLUB



SUN CITY SUMMERLIN COMPUTER CLUB

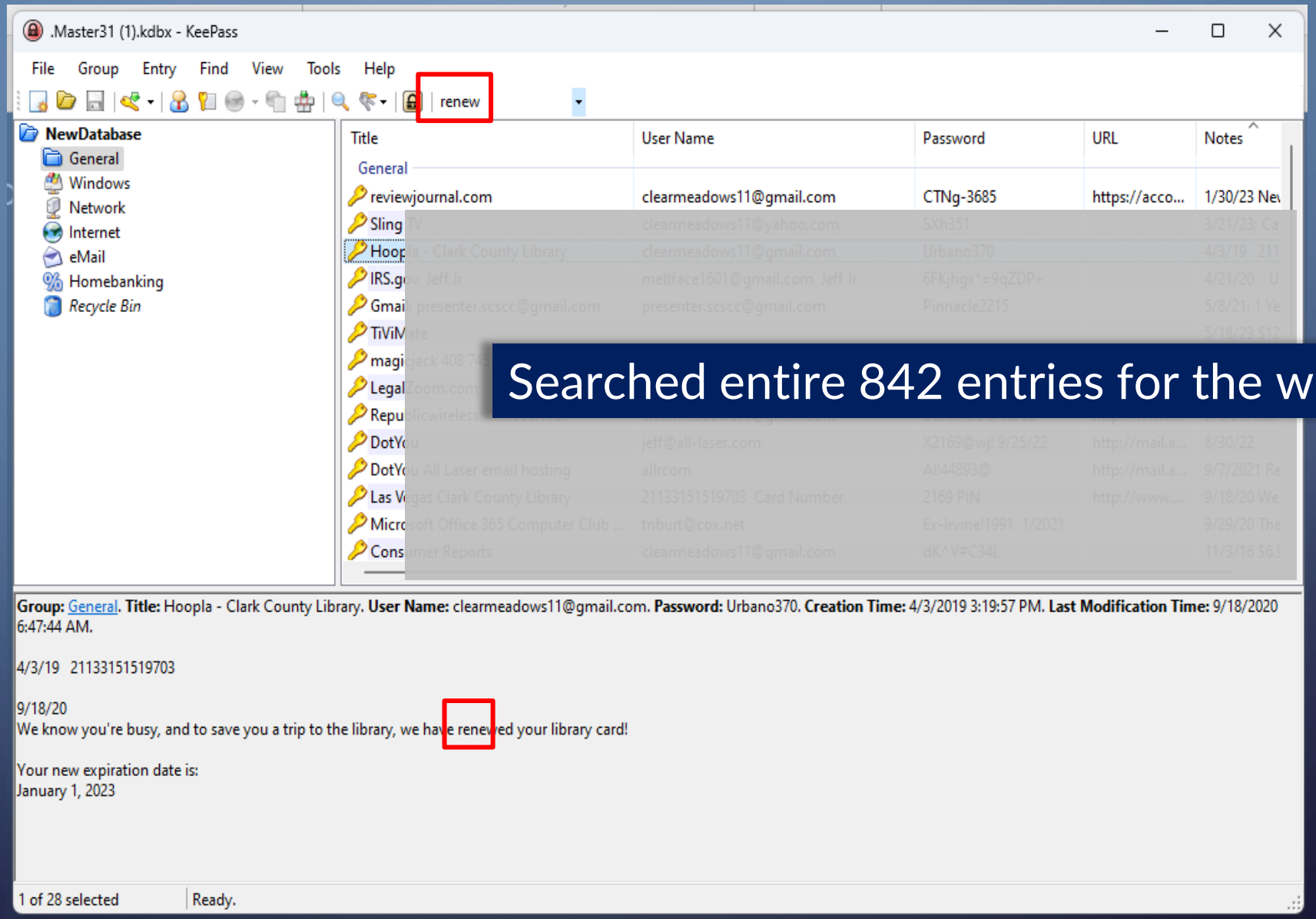


While all this may seem a bit overwhelming at first, the difficult part is done!

You can now add entries or revise existing entries.

When you finish adding an entry be sure to click the BLUE disk icon to save your work.

You can use the search box to search all your entries – this will search any field including the notes field and is very useful.



Searched entire 842 entries for the word “renew”

KeePass has many other features and options – I have chosen to show only the basic use as an easy to use free database for your passwords.

Passwords and their associated information are a major problem and this is a solution to that problem.

Be sure to make a backup of your database file!

- Many other password managers are available
- Paid and Free, many with cloud storage

- Questions?