





	<div><h1>Keeping passwords safe</h1><div></div><div><p>Chris Taylor President, OPCUG 2021-03-10</p></div><div><p>This deck available at: https://opcug.ca/presentations/keeping-passwords-safe.pdf</p></div><div></div></div>

	<div><p>How many web sites do you use that require a password?</p><p>Are they all <i>good</i> passwords?</p><p>Do you remember all of them?</p><div></div></div>

What makes a bad password?



Bad passwords

Short

- under 12 characters

Dictionary word

- attackers try every word in *many* dictionaries

Info about you

- name / nickname / partner's name
- pet's name
- birthplace
- email address
- zodiac symbol
- phone number

Common words / phrases

- password, password1, passw0rd
- MyPasswordIsSecret
- LuckOfTheDraw
- LiveAndLetDie
- FranklyScarletIDon'tGiveADamn

Pattern matching

- qwerty
- 12345678
- qazwsxedc

Re-used


- compromised one place, compromised everywhere

Written down

Shared with someone else

- trusted today, maybe not tomorrow

Saved in browser



Password saved in browser

Can someone else access them?

- if not logged into computer?
- probably not
- if logged in to computer
- that depends...

will display all stored passwords by default

- Firefox
- can set a *primary password*

prompts for Windows login password


- Google Chrome
- Microsoft Edge
- Internet Explorer
- Opera
- Brave

without a primary password


if you leave your computer unlocked and logged on, anyone can access *all* your online accounts that have password saved in browser

does *anyone* know your Windows password?

they can access *all* your online accounts that have password saved in browser



What makes a good password?



Good passwords

Long

- *at least* 12 characters

Multiple words


- *passphrase* rather than *password*
- 3 or more
- not a common phrase

Unique


- not used anywhere else


But ...


- can you remember 5 ... 10 ... 50?



A solution



	<h2>Password manager</h2>
	<ul style="list-style-type: none">■ Encrypted database<ul style="list-style-type: none">– <i>password vault</i> or <i>password safe</i>■ Create entries for each site/service<ul style="list-style-type: none">– each entry stores<ul style="list-style-type: none">■ logon names & passwords■ related notes, and more■ Master password opens database<ul style="list-style-type: none">– <i>one</i> password to remember– entries within the database are safe 

	<h2>Password manager</h2>
	<ul style="list-style-type: none">■ Many to choose from<ul style="list-style-type: none">– free and paid■ One security forum listed 75■ How to choose? 

KeePass Password Safe

- Free & open source
- Good feature set
- Started in 2003
 - long history is good with security
- Frequently updated (over 80 times)
- Dozens of awards
- Available on many operating systems
 - Windows, macOS, iOS, Android, Linux, etc.



Getting started

<https://keepass.info>

Click Downloads

A screenshot of the KeePass website. The header shows the KeePass logo and "KeePass Password Safe" with an OSI certified badge. The main content area has a "Latest News" section with entries for KeePass 2.45, 2.44, 1.38, and 2.43 releases. A sidebar on the left contains links for Home, Downloads, Translations, Plugins, Information, and Support. An arrow points from the "Click Downloads" text to the "Downloads" link in the sidebar. A small inset image shows the KeePass application interface.

Getting started

https://keepass.info

Installer for Windows

Versions for

- Android
- iPad
- iPhone
- MacOS
- Linux, etc.

Getting KeePass - Downloads

Here you can download KeePass:

KeePass 2.45

Installer for Windows (2.45):

Download Now

KeePass-2.45-Setup.exe

Portable (2.45):

Download Now

KeePass-2.45.zip

KeePass 1.38

Installer for Windows (1.38):

Download Now

KeePass-1.38-Setup.exe

Portable (1.38):

Download Now

KeePass-1.38.zip

Other downloads and links:

Contributed/Unofficial KeePass Ports

- KeepassDroid (for Android)
- Keepass2Android (for Android)
- KeepassDX (for Android)
- KeepShare (for Android)
- Keepassium (for iPhone / iPad)
- SyncPass (for iPhone / iPad)
- Strongbox (for iPhone / iPad / Mac OS X)
- Strongbox (for iPhone / iPad)

Users helping users

Getting started

Only

- New
- Open

available

File

Click New

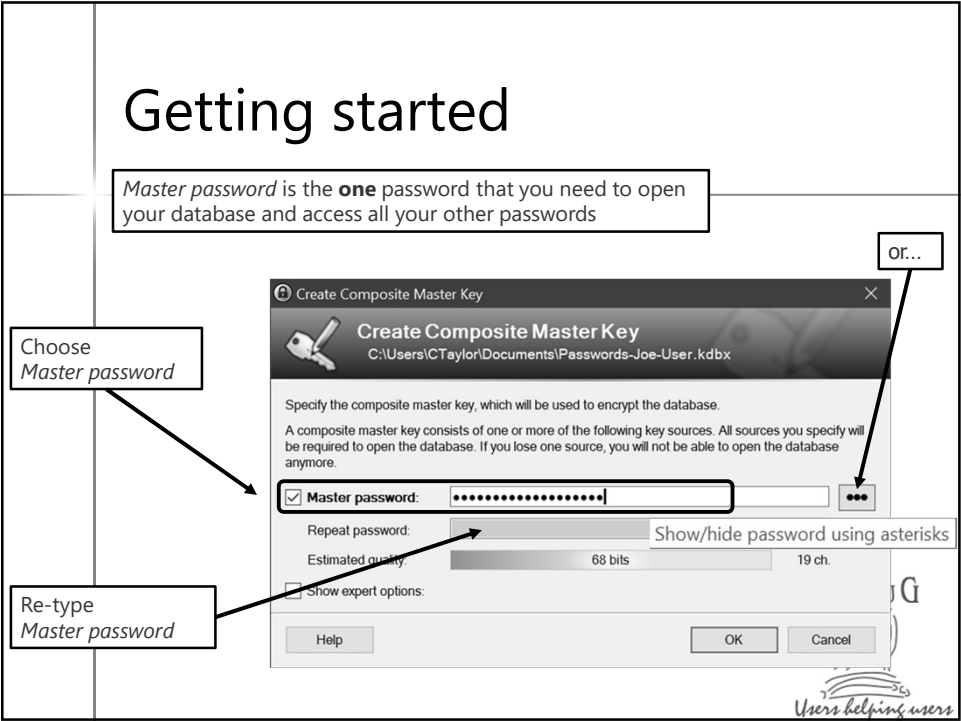
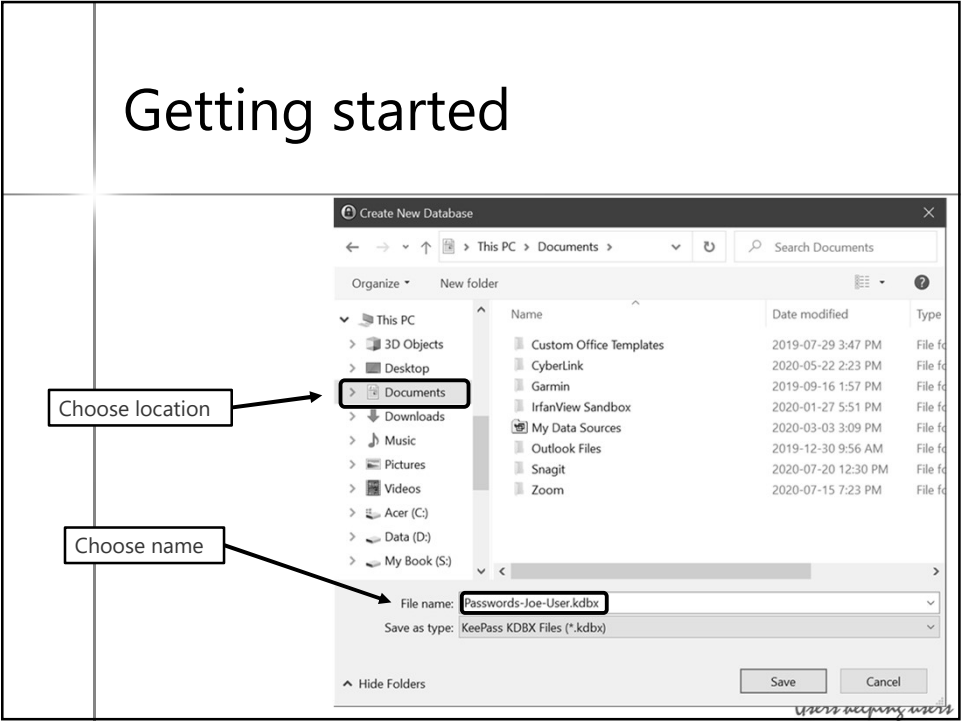
File

Entry Find View Tools Help

Title	User Name	Password	URL	Notes

0 of 0 selected Ready.

Users helping users



Getting started

Choose
Master password

Create Composite Master Key

C:\Users\CTaylor\Documents\Passwords-Joe-User.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: BlueSkiesAreFalling

Repeat password:

Estimated quality: 68 bits 19 ch.

☐ Show expert options:

Help OK Cancel

OPCUG
Users helping users

Good Master password

Long
- at least 12 characters

Multiple words
- *passphrase* rather than *password*
- 3 or more
- not a common phrase

Unique
- not used anywhere else

Something you can remember
- BlueSkiesAreFalling
- ParisMadeOfCheese!
- Ran*Faster*Than*Snail
- Barking-Down-Well
- Shoe.Leather.Hat

- but none of the above

OPCUG
Users helping users

Master password

- Remember your Master password
 - if you forget
 - can never open the password database!
 - if you think you may forget it
 - write it down
 - store in secure, accessible location
 - eg. a lock box
 - if someone else might come across it
 - store without context or misdirected context



Master password



Getting started

Optional
I leave blank

Create New Database - Step 3

Database Settings

C:\Users\CTaylor\Documents\Passwords-Joe-User.kdbx

General Security Compression Recycle Bin Advanced

Database name: Enter a name for the database or leave it empty.

Database description: Enter a short description of the database or leave it empty.

Default user name for new entries:

☐ Custom database color:

Help OK Cancel

Avoid other tabs
- defaults are fine

Getting started

Emergency Sheet

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.

It is recommended that you create an emergency sheet for your database.

Do you want to print an emergency sheet now?

→ Print
KeePass will print an emergency sheet, which you can then fill out.

→ Skip

KeePass
Emergency Sheet

Database

2020-07-20

Database file:
C:\Users\CTaylor\Documents\Passwords-Joe-User.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 is:

Master password:

Instructions and General Information

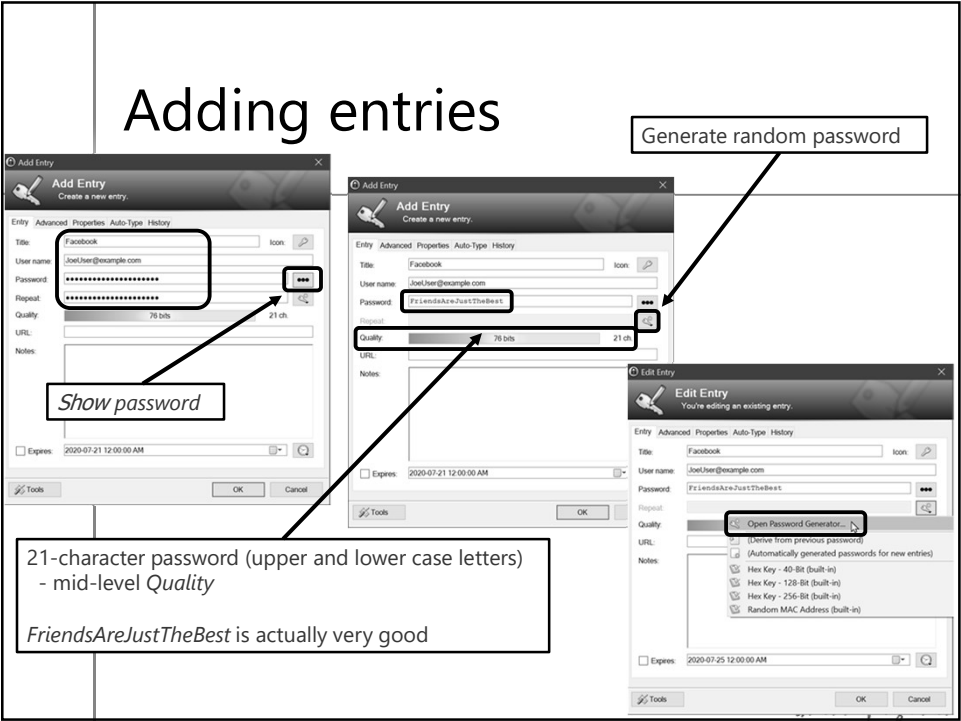
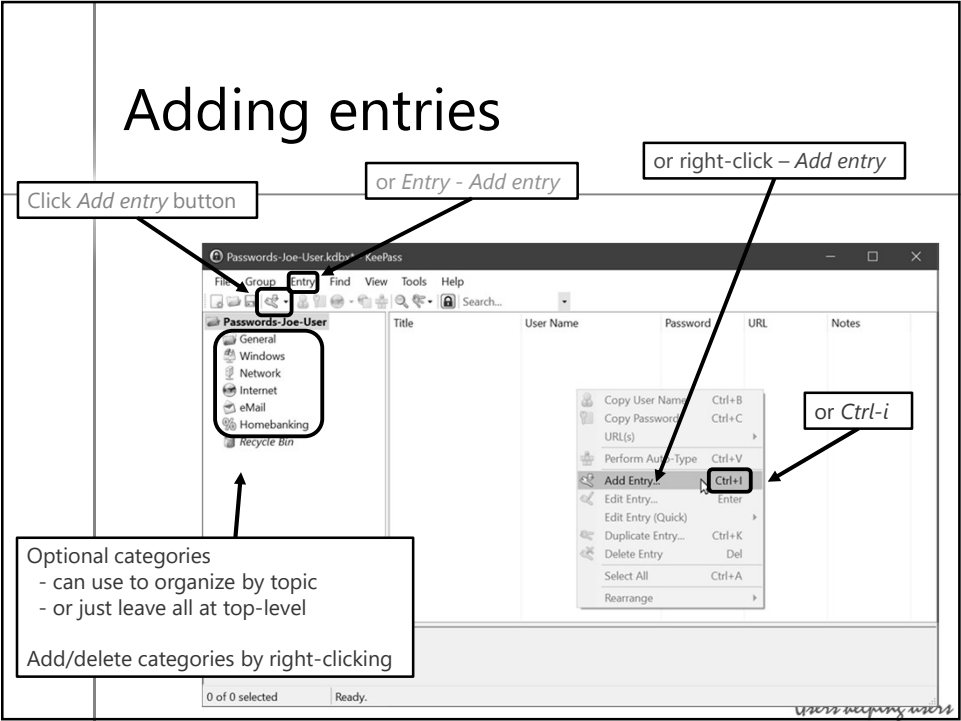
A KeePass emergency sheet contains all important information that is required to open your database. It should be printed, filled out and stored in a secure location, where only you and possibly a few other people that you trust have access to.

If you lose the database file or any of the master key information (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/>

Maybe username/password to sign into your computer!

Master password



Password generator

Length

Commonly required

OPCUG
Users helping users

Password generator

Random password

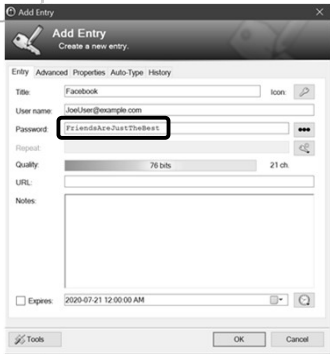
Quality jumped to high

OMG! I never want to remember or type that in!!!!

With KeePass you don't have to
- remember or
- manually type your password!
I will show you how later

OPCUG
Users helping users

Adding entries



I prefer;
- a password I *might* remember
- don't have to always look up my password

But it has to be strong;
- more than 12 characters
- not a dictionary word
- not a common phrase
- not a keyboard pattern
- etc.




Notes

■ Any related info



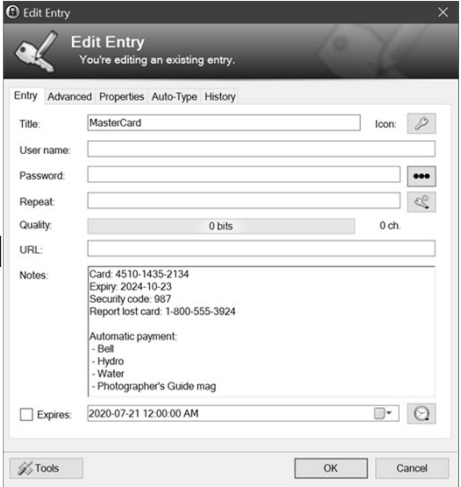
Other uses

- Store any information
 - phone numbers
 - expiry dates for subscriptions
 - confirmation codes
- Including sensitive info
 - credit card
 - passport
 - answers to security questions



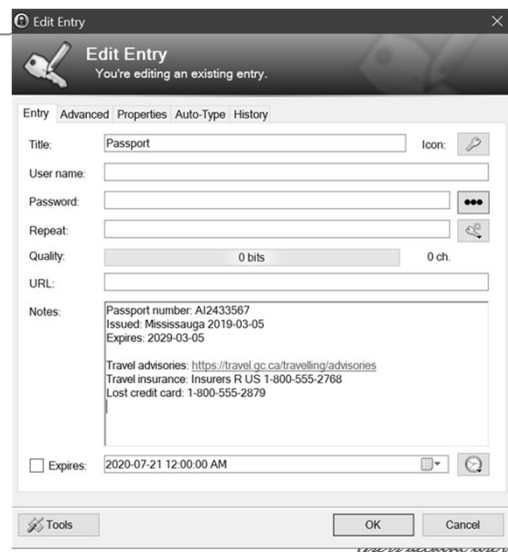
Credit card

- number
- expiry date
- security code
- phone number to report lost card
- automatic payments



Passport

- number
- issue date
- expiry date
- city of issue
- travel advisory site

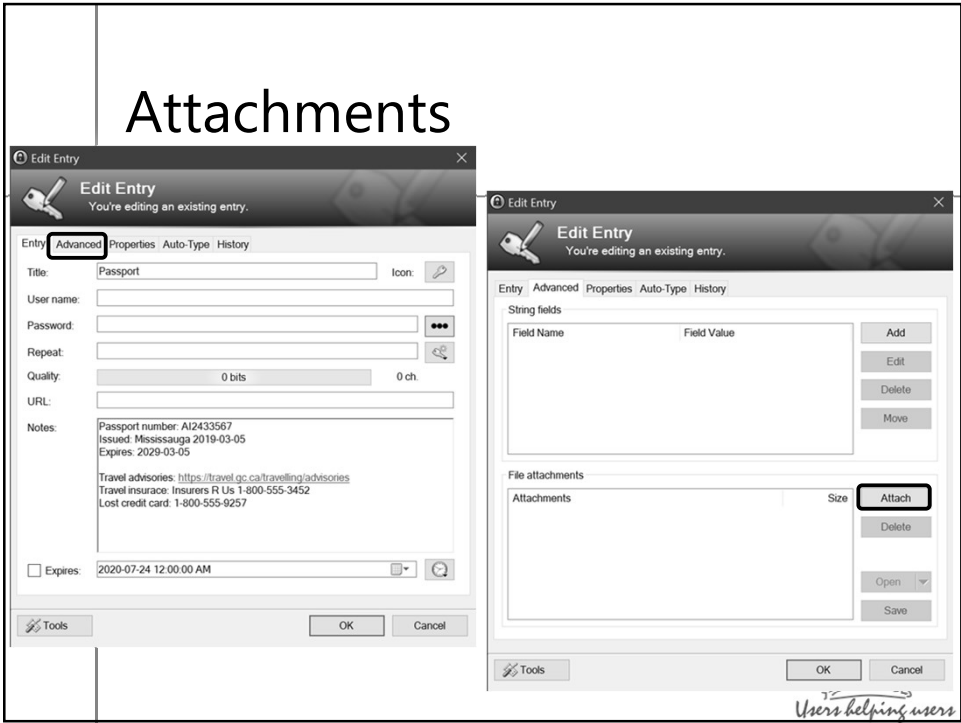


When traveling

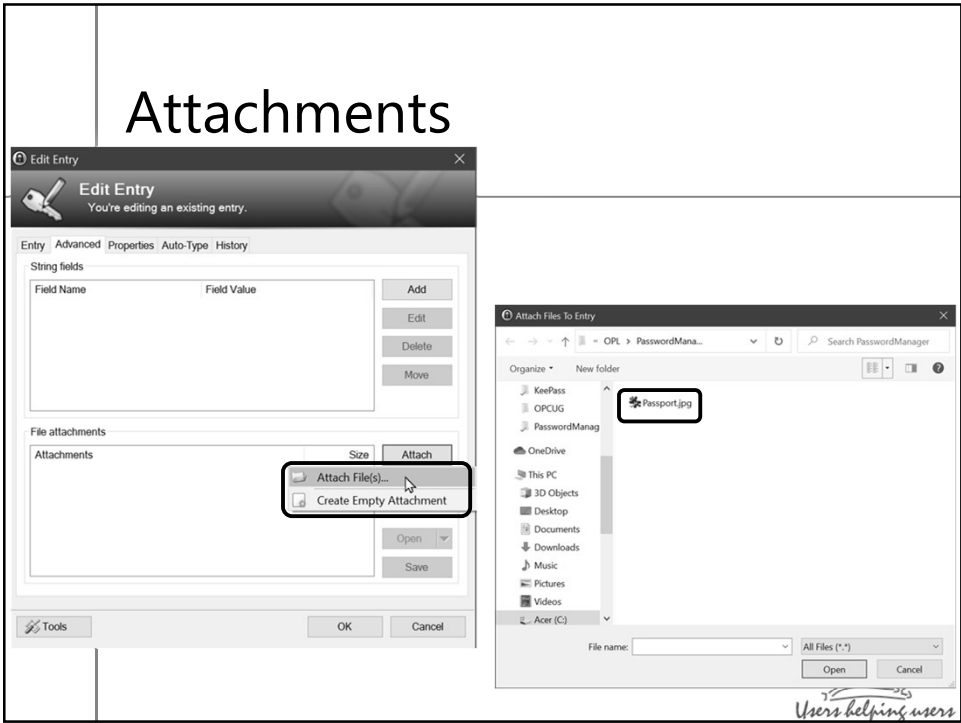
- But hang on...
 - KeePass is on Windows computer at home
 - I need info while traveling...
- KeePassDroid
 - can have KeePass database on phone
 - details later...



Attachments



Attachments



Attachments



Now you have entries in KeePass

How do you use them?

I said you don't have to

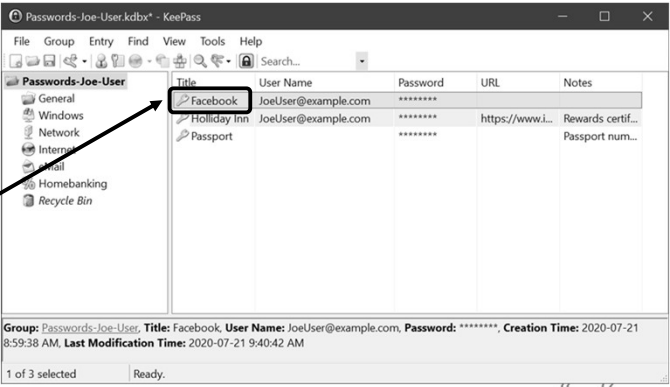
- remember or
- manually type your password!



Using KeePass

Open KeePass

Double-click
Title of entry
to open

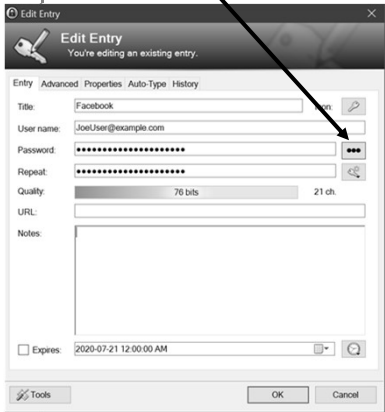


Users helping users

Using KeePass

Click to show password

Can
- copy to clipboard
- paste at web site



Users helping users

Double-clicks

Copy user name to clipboard

Copy password to clipboard
* actual password copied, not dots

Open browser to URL


Copy notes to clipboard

Hint: Anything copied...
can be pasted
- user name
- password

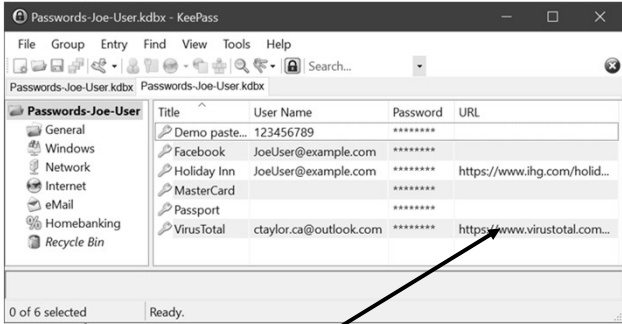
Title	User Name	Password	URL	Notes
Facebook	JoeUser@example.com	*****		
Holiday Inn	JoeUser@example.com	*****	https://www...	Rewards certifi
Passport		*****		Passport num...

Group: Passwords-Joe-User Title: Facebook User Name: JoeUser@exam...
8:59:38 AM Last Modification Time: 2020-07-21 9:40:42 AM
1 of 3 selected Ready.


Items copied to clipboard for 12 seconds *
* customizable in Tools | Options | Security



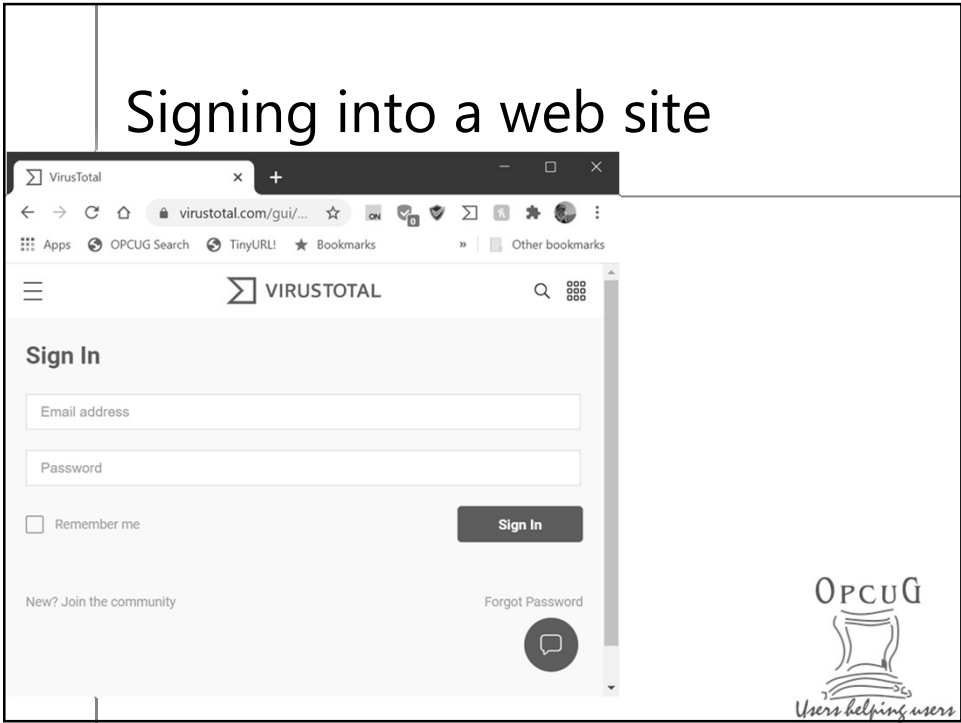
Signing into a web site



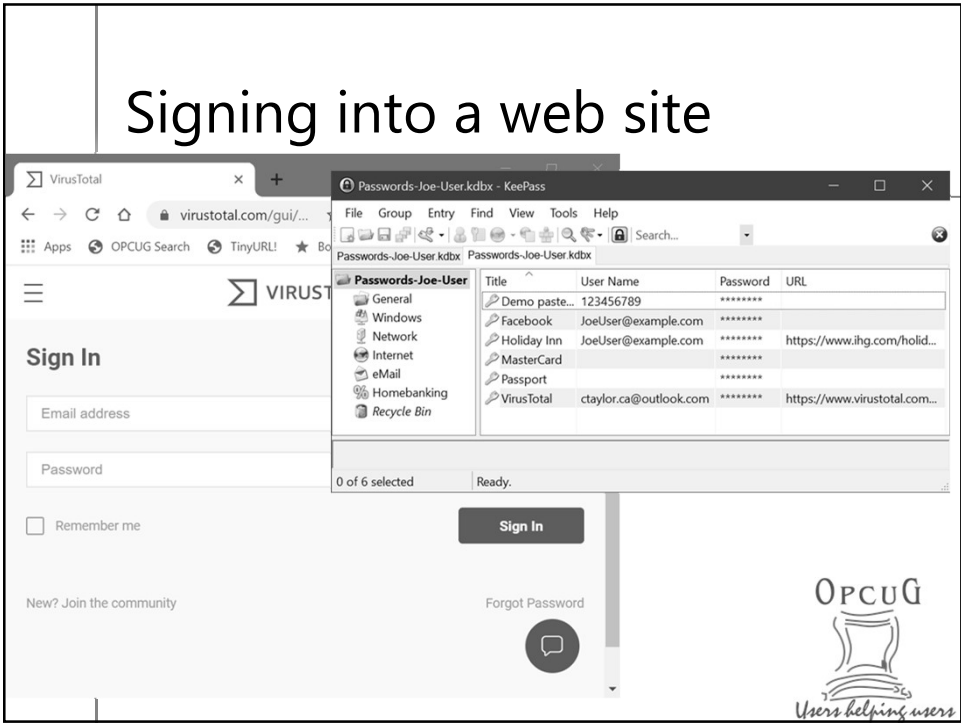
Double-click URL to open browser to sign in page
- or browse to site by yourself..



Signing into a web site



Signing into a web site



Signing into a web site

The screenshot shows a web browser window with the VirusTotal sign-in page. The page has fields for 'Email address' and 'Password', a 'Remember me' checkbox, and a 'Sign In' button. Overlaid on this is a KeePass password manager window showing a list of saved passwords. An arrow points to the 'User Name' column in the list, with a callout box that says 'Double-click User Name to copy it to clipboard'.

Title	User Name	Password	URL
Demo paste...	123456789	*****	
Facebook	JoeUser@example.com	*****	
Holiday Inn	JoeUser@example.com	*****	https://www.ihg.com/holid...
MasterCard		*****	
Passport		*****	
VirusTotal	ctaylor.ca@outlook.com	*****	https://www.virustotal.com...

Signing into a web site

The screenshot shows the same web browser window with the VirusTotal sign-in page. An arrow points to the 'Email address' field, with a callout box that says 'Right-click Email address field and choose Paste or Click in the Email address field and press Ctrl-v'.

Signing into a web site

Sign In

ctaylor.ca@outlook.com

Password

☐ Remember me

New? Join the community


Sign In

Forgot Password

Passwords-Joe-User

Title	User Name	Password	URL
Demo paste...	123456789	*****	
Facebook	JoeUser@example.com	*****	
Holiday Inn	JoeUser@example.com	*****	https://www.ihg.com/holid...
MasterCard		*****	
Passport		*****	
VirusTotal	ctaylor.ca@outlook.com	*****	https://www.virustotal.com...

Double-click *Password* to copy it to clipboard



Signing into a web site

Sign In

ctaylor.ca@outlook.com

Password

☐ Remember me

New? Join the community


Sign In

Forgot Password

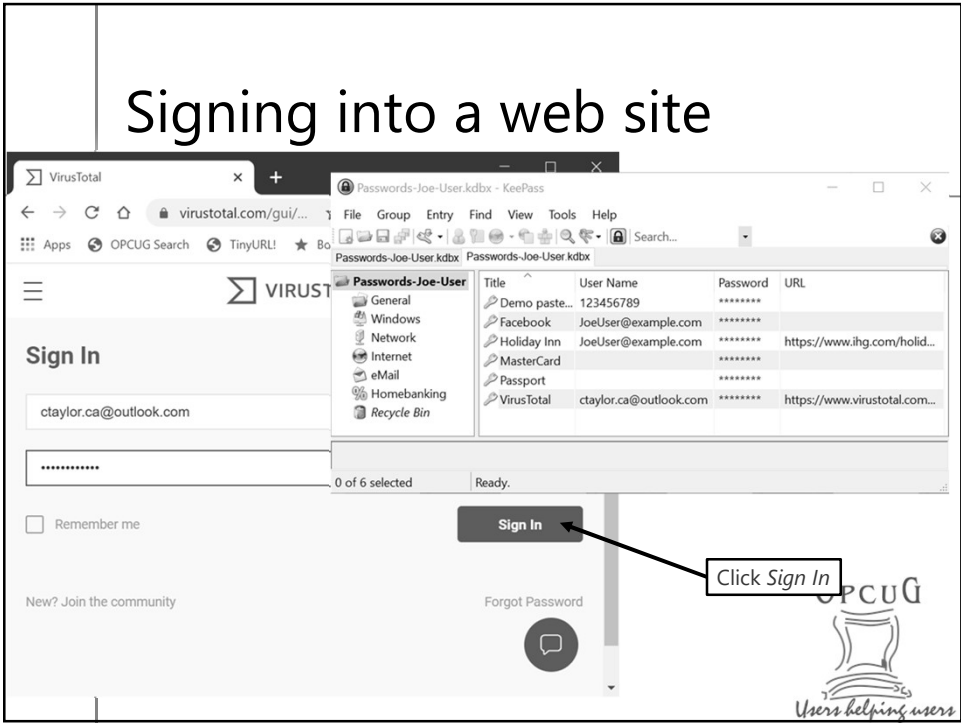
Passwords-Joe-User

Title	User Name	Password	URL
Demo paste...	123456789	*****	
Facebook	JoeUser@example.com	*****	
Holiday Inn	JoeUser@example.com	*****	https://www.ihg.com/holid...
MasterCard		*****	
Passport		*****	
VirusTotal	ctaylor.ca@outlook.com	*****	https://www.virustotal.com...

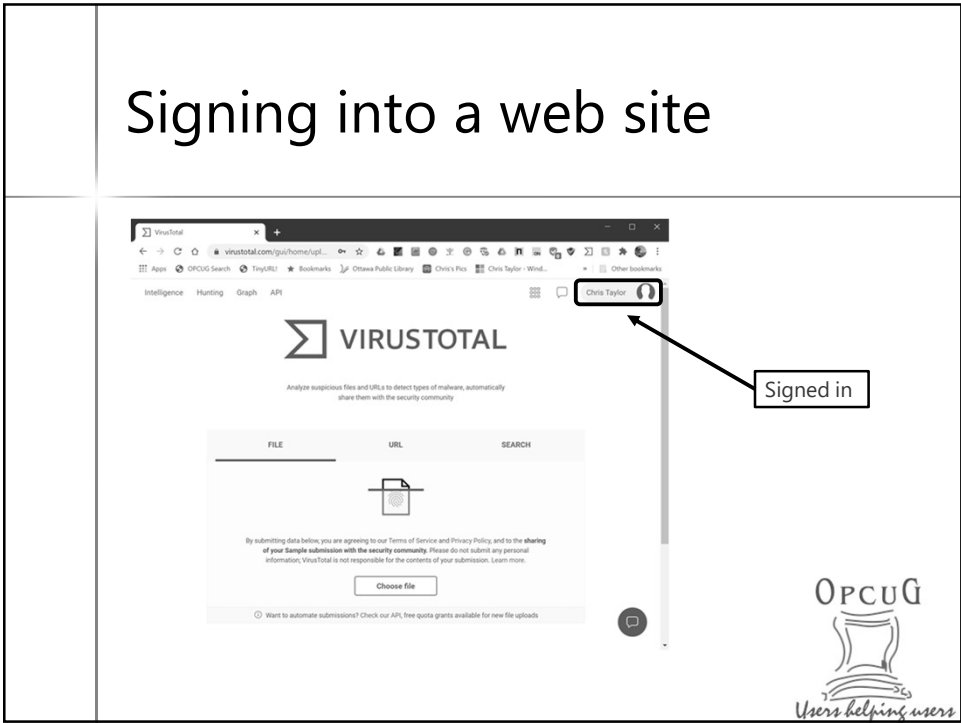
Right-click *Password* field and choose *Paste* or
Click in the *Password* field and press *Ctrl-v*





Signing into a web site



Signing into a web site



	<div>Auto-type</div> <div></div>

	<div>Auto-type</div> <div><div><div>KeePass optional feature</div><div>- pass username and password to web site in one operation</div></div><div><div>Defaults often work</div><div>- test - if it doesn't work ... customize!</div></div></div> <div></div>
--	---

Auto-Type testing

Go to sign in page

URL (in this example) is `https://www.virustotal.com/gui/sign-in`
note the URL
- you will need it later

Auto-type testing

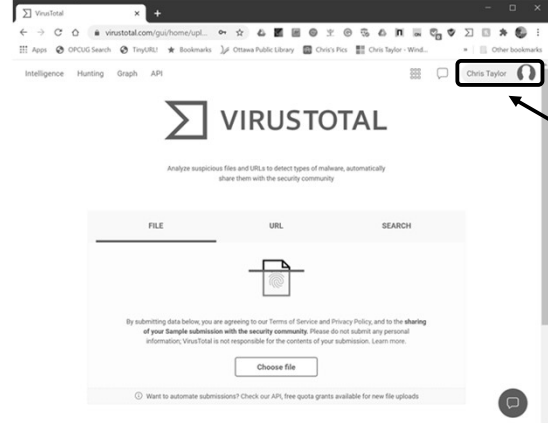
Type in *username/account*

Press *Tab* once

Type in *password*

Press *Enter*


KeePass signs you in



Signed in?

If so, *success!*
- defaults work fine

If not
- note exact keystrokes;
- tabs, arrow keys ...
needed to log on to the site



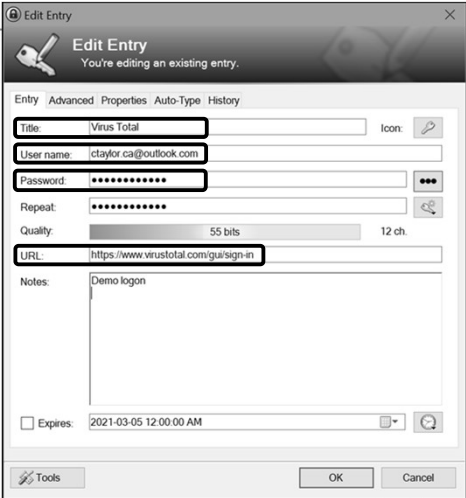
Auto-type setup


Create KeePass entry for site

Set **User name:** to account name on site
- ctaylor.ca@outlook.com

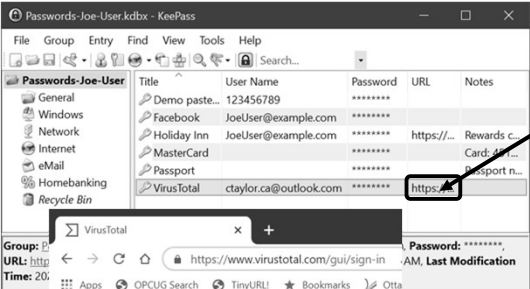
Set **Password:** to password for account on site

Set **URL:** to sign-in page for site
- https://www.virustotal.com/gui/sign-in

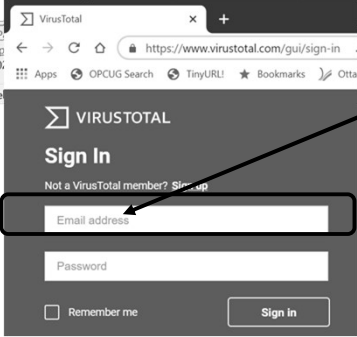





Auto-type in operation

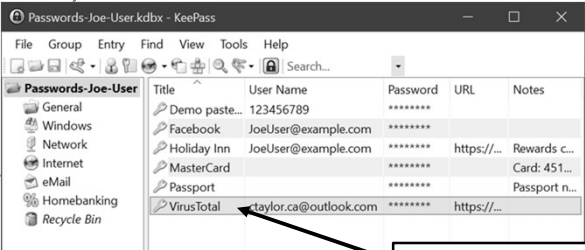


Double-click URL to open browser at logon page

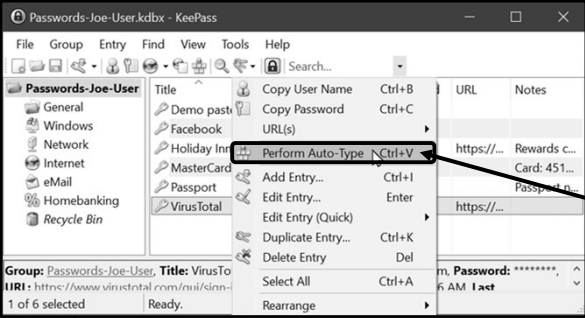


Click in field for sign in name (if cursor not there already)

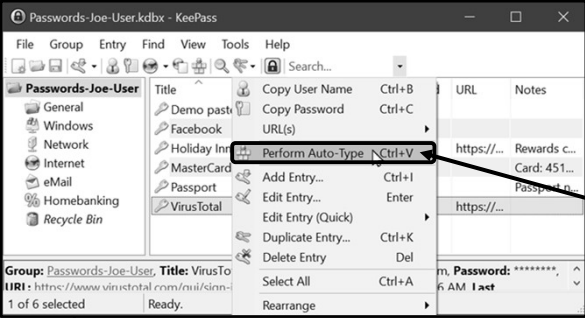




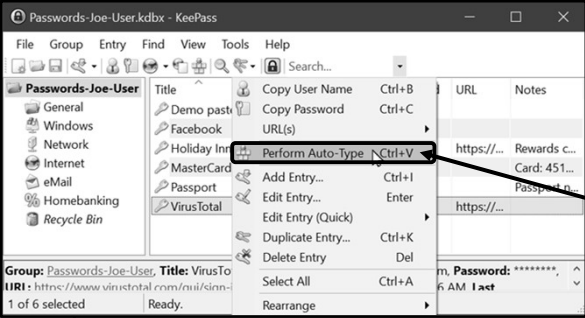
With VirusTotal entry highlighted



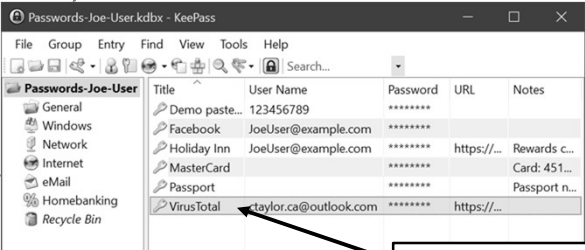
Choose Perform Auto-Type



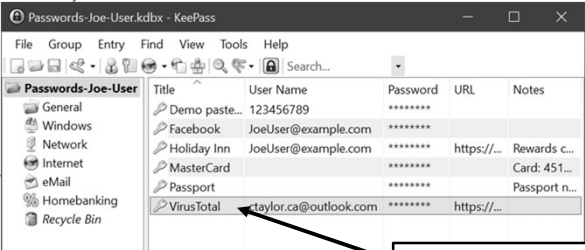
Right-click the VirusTotal line




press Ctrl-v or...



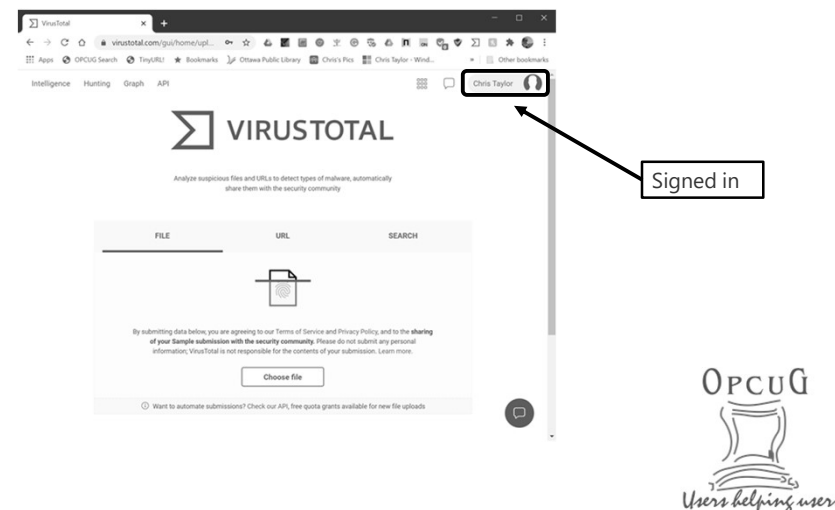
Switch back to KeePass



Tip for easier switch back to KeePass
- press Ctrl-Alt-K
- or set KeePass to View | Always on Top



KeePass signs you in



Auto-type customization

- If keystrokes to sign in to site are *not*; username{tab}password{Enter}
- Figure out correct keystrokes to sign in
- Customize KeePass for that entry



Edit Entry

You're editing an existing entry.

Entry Advanced Properties **Auto-Type**

☒ Enable auto-type for this entry

☐ Inherit default auto-type sequence from group

☒ **Override default sequence**

(USERNAME)(TAB)(PASSWORD)(ENTER)

Edit

Use custom sequences for specific windows:

Target Window Sequence Add

Edit Auto-Type Item

Configure Keystroke Sequence

Define a default keystroke sequence.

Target window: (Default)

Click the drop-down button on the right to see currently open windows.

☐ Use default keystroke sequence of the entry

☒ **Use custom keystroke sequence:**

(USERNAME)(TAB)(PASSWORD)(ENTER)

Insert placeholder

Standard Fields: (Title) (UserName) (Password) (URL) (Notes)

Key Modifiers: Shift +, Ctrl +, Alt +

Special Keys: (TAB) (ENTER) (UP) (DOWN) (LEFT) (RIGHT) (HOME) (END) (PGUP) (PGDN) (INSERT) (DELETE) (SPACE)

Help OK Cancel

Edit entry in KeePass

Click Auto-type tab

Click Override default sequence


Click Edit

Define a new sequence

You can type in things like {TAB}

or click the ones you want in Insert placeholder section

See also <https://keepass.info/help/base/autotype.html>



KeePass advanced features

Multi-factor authentication
key file, Windows user account, Yubikey

Duplicate passwords
Find | Duplicate Passwords...

Similar passwords
Find | Similar Passwords (Pairs)...


Password quality
Find | Password Quality...

Expiring passwords
Find | Expired / Expiring in...

TAN support
Transaction Authentication Numbers
(one-time passwords)

History
see/restore previous versions of entries

Plug-ins
(over 160)
backup
passphrase generator
import/export
...



Users helping users

Chris.Taylor@opcug.ca

30

Synchronization between devices





Multiple device synching


- KeePass for other operating systems
 - Windows, MacOS, iOS, Android, Linux, ...
- If you want to
 - use KeePass on multiple computers/devices
 - share KeePass database across all devices
- Two choices...




	<h2>Multiple device synching</h2>
	<ul style="list-style-type: none">■ Manual synching<ul style="list-style-type: none">– easiest to set up– requires manual actions each time you want databases to match on each device■ Automatic synching<ul style="list-style-type: none">– more complex to set up (once)– edit entries on any device<ul style="list-style-type: none">■ changes automatically synched to other devices



	<h2>Manual synchronization</h2>
	

	<h1>Assumptions</h1>
	<ul style="list-style-type: none">■ The instructions here assume:<ul style="list-style-type: none">– one device is a Windows 10 computer<ul style="list-style-type: none">■ KeePass already installed■ at least one entry in KeePass– other device is an Android phone
	<div><p>Note: You should be able to synchronize with other devices such as - iPhone, iPad, etc. I have not tested to see what differences there are in processes</p></div> <div></div>

	<h1>Overview</h1>
	<p>One-time actions</p> <ol style="list-style-type: none">1. install KeePassDroid on phone2. copy KeePass database to phone3. configure KeePassDroid on phone so it knows where to find database <p>Repeated actions</p> <ol style="list-style-type: none">1. update copy of database on phone according to needs (step 2 above) <div></div>

KeePassDroid

- Install KeePassDroid on the phone from
 - <https://play.google.com/store/apps/details?id=com.android.keepass>
 - *don't* create KeePass entries on the phone

Note: You should be able to synchronize with other devices such as
– iPhone, iPad, etc.
but I have not tested to see what differences there are in processes



Manual synching

- My Windows configuration
 - database is in my *Documents* folder
 - database is *Passwords-Joe-User.kdbx*
- Adjust to your configuration



Copying KeePass database to phone
(slide 1 of 3)

- Make sure
 - KeePass is closed on Windows computer
 - KeePassDroid is closed on Android phone
- Plug phone into your Windows computer
- Run File Explorer on Windows computer
- Follow the steps on the next two slides



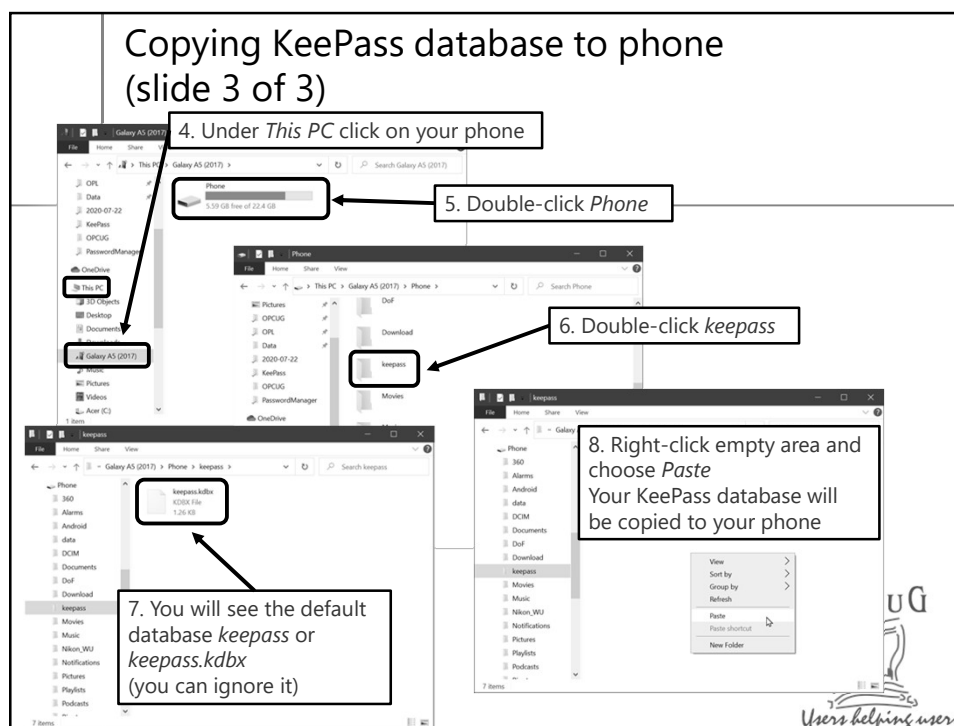
Copying KeePass database to phone
(slide 2 of 3)

1. Go to *Documents* folder
(or wherever you have database stored)

2. Right-click your KeePass database file

3. Choose *Copy*





One time only

- KeePassDroid on phone needs to know name of KeePass database file
 - The next three slides show what has to be done ONLY ONCE on your phone

Slide 1 of 3

1. Open KeePassDroid on phone

KeePassDroid

ABOUT SETTINGS

KeePass database filename:
content://com.google.android.apps.do...
☒ Use this as my default database
Enter a password and/or a key file to unlock
your database:
Password
Key file (optional)
☐ Show password ☐ Save password with biometrics
OK

2. Tap phone's
Back button

KeePassDroid

ABOUT SETTINGS

OPEN RECENT DATABASE (CLICK TO OPEN):
content://com.google.android
.apps.docs.storage/document
/acc%3D1%3Bdoc%3Dencoded
%3D163IG4KmfWlwpNK2tkN0pYC
wL21h1Z0f9vi1aUerqTU0Ba3i0V
%2Bp9K04U3p199uajb1duFg%3D
content://com.google.android
.apps.docs.storage/document
/acc%3D1%3Bdoc%3Dencoded
%3DVxNvNZ5zTG%2FulVaQY6kZyZZ
KYpCE34fXKJNP3Bk%2FC8ucFLTbS
Tgf6d6%3D%3
content://com.android.externalstorage
.documents/document/primary
%3Akeepass%2FTest%2FCTaylor.kd
ENTER DATABASE FILENAME:
/emulated/0/keepass/keepass.kdbx
OPEN CREATE

3. Tap on folder

KEEPASS

Name ^

test Vault

XSL

CTaylor ne...
57.34 KB Jul 23

CTaylor.kdbx
57.93 KB Jul 30

4. Tap on hamburger menu

Users helping users

Slide 2 of 3

OPEN FROM

Images

Audio

Recent

Downloads

Galaxy A5 (2017)
5.22 GB free

5. Tap on phone

GALAXY A5 (2017)

Name ^

DoF

Download

keepass

Movies

Music

NIKON_WU

Notifications

6. Tap on keepass folder

KEEPASS

Name ^

keepass.kdbx
Feb 17, 2018 1.29 KB

Passwords-Joe-User.kdbx
Jul 23 89.73 KB

7. Tap on your
KeePass database

Users helping users

Slide 3 of 3

KeePassDroid

OPEN RECENT DATABASE (CLICK TO OPEN):

content://com.google.android.apps.docs.storage/document/acc%3D1%3Bdoc%3Dencoded%3D163IG4KmfWlpNK2tkN0pYCwL21h1Z0f9vi1aUerqTU0Ba3i0V%2Bp9K04U3p199uajb1duFg%3D

content://com.google.android.apps.docs.storage/document/acc%3D1%3Bdoc%3Dencoded%3DVxNvNZ5zTG%2FulVaQY6kZyZZKYPCE34fXKJNP3Bk%2FC8ucFLTbSTg%3

content://com.google.android.externalstorage.documents/document/primary%3Akeenas.%2FTest%2FC:Taylor kdhx

ENTER DATABASE FILENAME:

content://com.google.android.externalstorage.documents/document/primary%3Akeenas.%2FTest%2FC:Taylor kdhx

OPEN CREATE

KeePassDroid

KeePass database filename:

content://com.google.android.externalstorage.documents/document/primary%3Akeenas.%2FTest%2FC:Taylor kdhx

☒ Use this as my default database

Enter a password and/or a key file to unlock your database:

Password

Key file (optional)

☐ Show password ☐ Save password with biometrics


OK

9. Make sure
Use this as my default database
is checked

10. Enter the password
for your KeePass database

11. Tap OK

12. Verify KeePass shows
the same entries as on
your Windows computer



Using KeePassDroid

1. Open KeePassDroid on phone

2. Enter the password
for your KeePass database

3. Tap OK

KeePassDroid

ABOUT SETTINGS

KeePass database filename:

content://com.google.android.apps.docs.storage/document/acc%3D1%3Bdoc%3Dencoded%3D163IG4KmfWlpNK2tkN0pYCwL21h1Z0f9vi1aUerqTU0Ba3i0V%2Bp9K04U3p199uajb1duFg%3D

☒ Use this as my default database


Enter a password and/or a key file to unlock your database:

Password

Key file (optional)

☐ Show password ☐ Save password with biometrics

OK



Updating database

- When you
 - change KeePass on Windows computer
 - want to update database on phone
- Repeat previous slides
 - *Copying KeePass database to phone* (slides 1 -3)



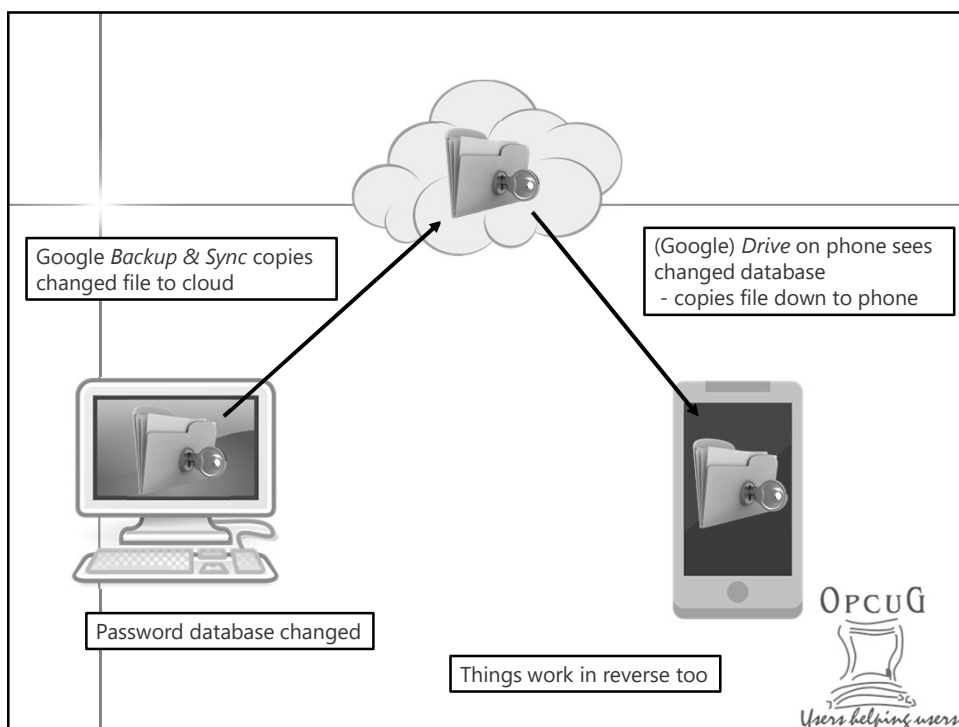
Automatic synchronization



Assumptions


■ Instructions assume:

- one device is a Windows 10 computer
 - KeePass is installed
 - at least one entry in KeePass
- other device is an Android phone
- you will use Google Drive to sync

Note: You should be able to synchronize with other devices such as
- iPhone, iPad, etc.
and other cloud service for synchronization
but I have not tested to see what differences there are in processes



	<h1>Overview</h1>
	<p>All one-time actions</p> <ol style="list-style-type: none">1. Create a free Google Account if you don't already have one (phone should already be using a Google Account)2. Install Google Drive <i>Backup & Sync</i> on Windows PC3. Move your KeePass database to <i>Google Drive</i> on Windows PC4. Configure <i>Google Drive</i> on phone it is just called <i>Drive</i> on Android5. Install KeePassDroid on phone6. Configure KeePassDroid on phone so it knows where to find database <div> Drive  Users helping users</div>

	<h1>Google Account required</h1>
	<ul style="list-style-type: none">■ All Google Accounts automatically have<ul style="list-style-type: none">– Google Drive■ Android uses a Google Account<ul style="list-style-type: none">– use this account throughout instructions <div> Users helping users</div>

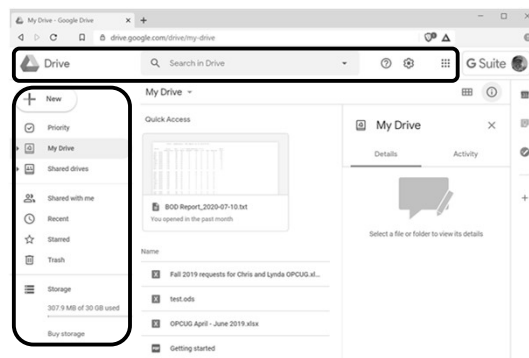
Google Drive

- Verify Google Drive working
 - browse to *https://accounts.google.com*
- If requested
 - sign in using your Google Account
- Once logged in, browse to
 - *https://drive.google.com*



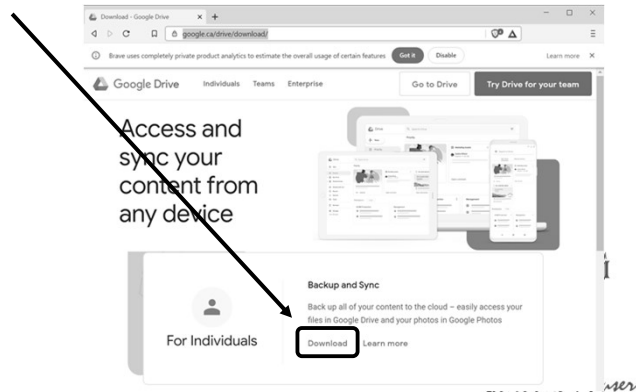
Google Drive

- Don't proceed further unless you see a screen similar to this



Backup & Sync

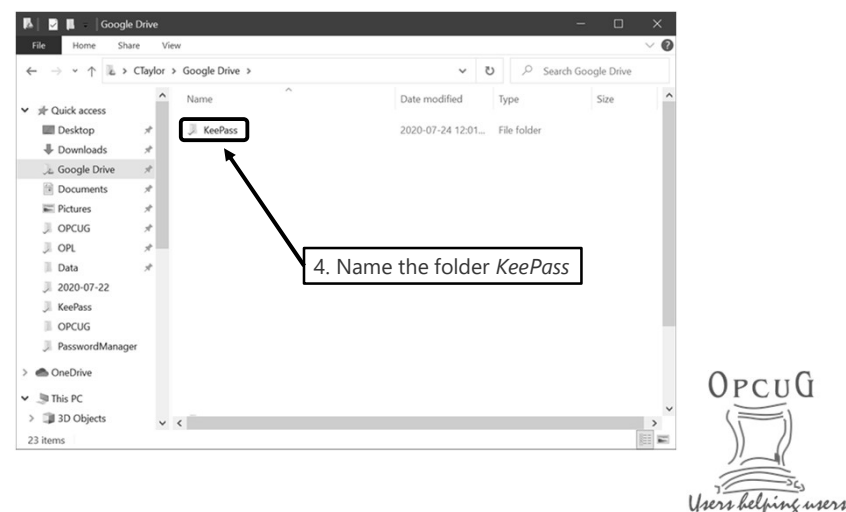
- Install Google Drive's *Backup & Sync*
 - <https://www.google.ca/drive/download/>



Backup & Sync


- During installation
 - If prompted for a Google Account to use
 - use Google Account used on Android phone
- After installation
 - *Google Drive* folder on your computer
 - in File Explorer under *Quick Access*
 - or
 - under *C:\Users\{your account name}*

Make a KeePass folder in Google Drive (slide 2 of 2)



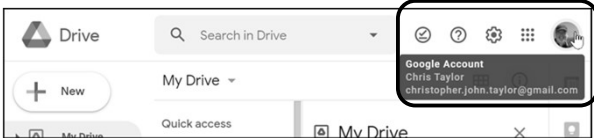
KeePass database location

- If you haven't installed KeePass, do so
 - when prompted for the location of your database, choose the folder you created within Google Drive
 - C:\users\{username}\Google Drive\KeePass
- If you have already installed KeePass
 - run KeePass and enter your Master password
 - click on File | Save As | Save to File...
 - choose the folder you created within *Google Drive*
 - C:\users\{username}\Google Drive\KeePass
 - click the Save button
 - copies database to the new location
 - updates configuration so KeePass looks for it there




Verify database sync

- Browse to <https://drive.google.com>
 - make sure you are signed in using Google Account used on phone



- Verify your database has been synced there



KeePassDroid

- Install KeePassDroid on the phone

<https://play.google.com/store/apps/details?id=com.android.keepass>

Don't create KeePass entries on the phone
- we will copy the KeePass database from Windows computer

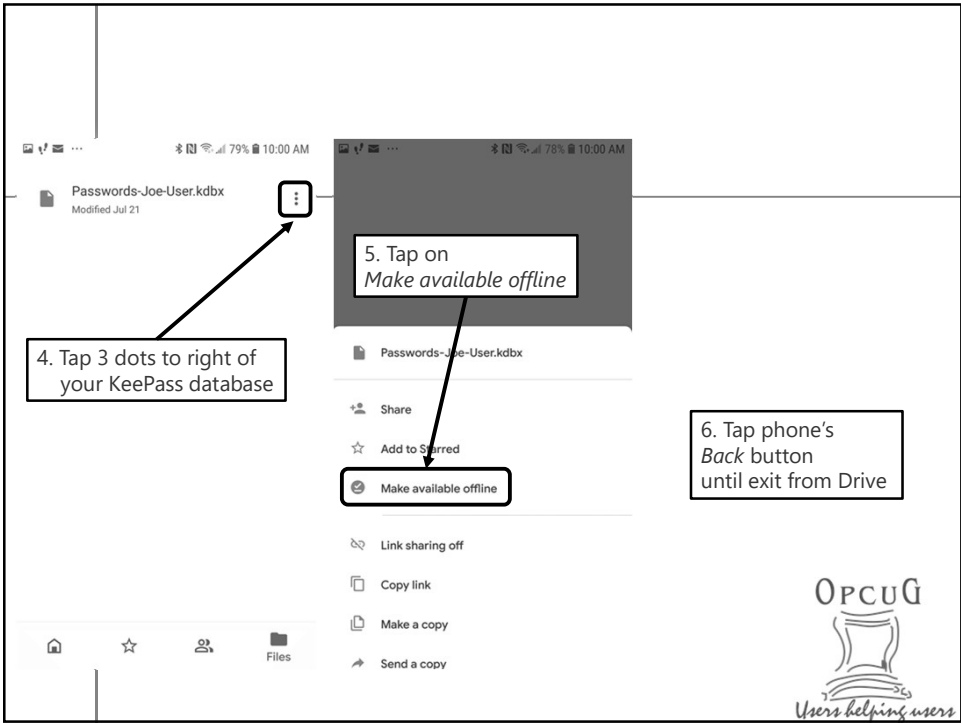
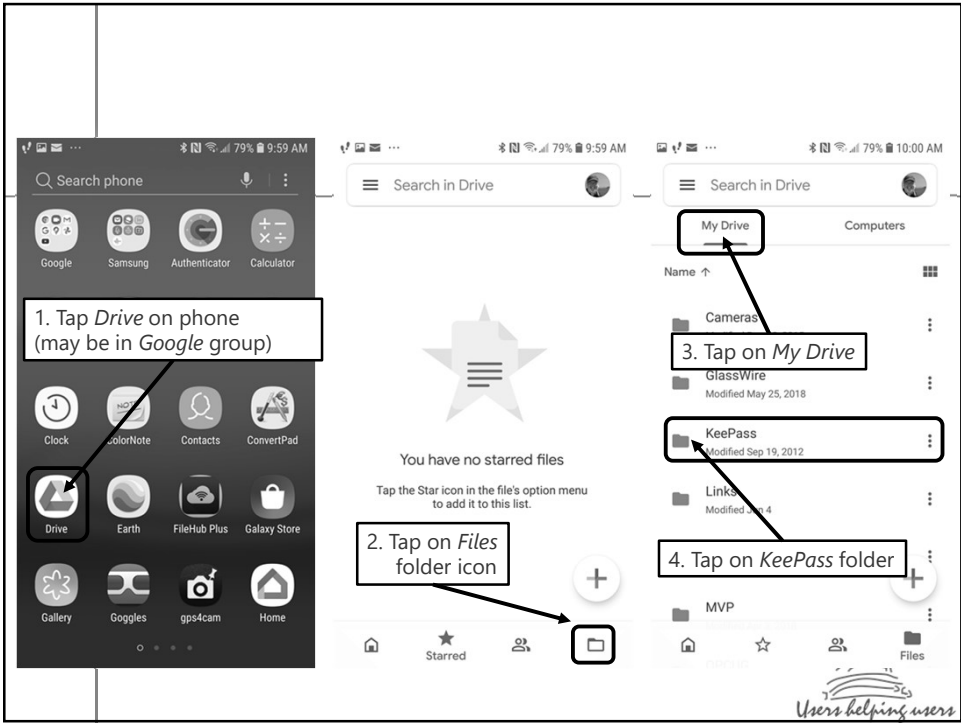
Note: You should be able to synchronize with other devices such as
- iPhone, iPad, etc.
but I have not tested to see what differences there are in processes



Configure Google Drive

- Configure Google Drive on Android phone
 - set KeePass database to be available offline
- Next two slides only need to be done ONCE





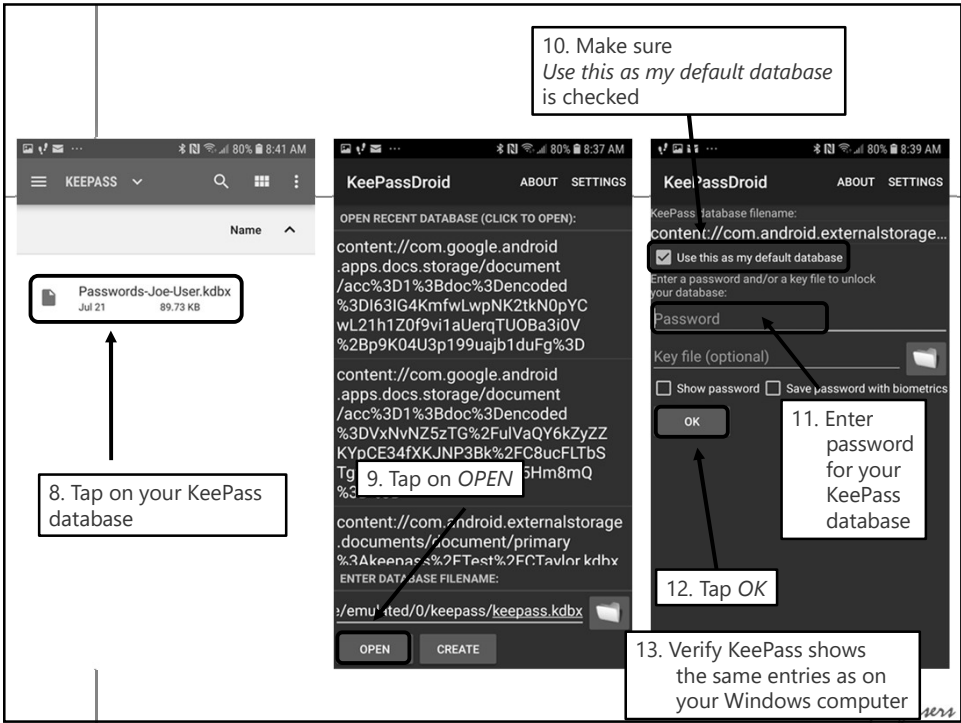
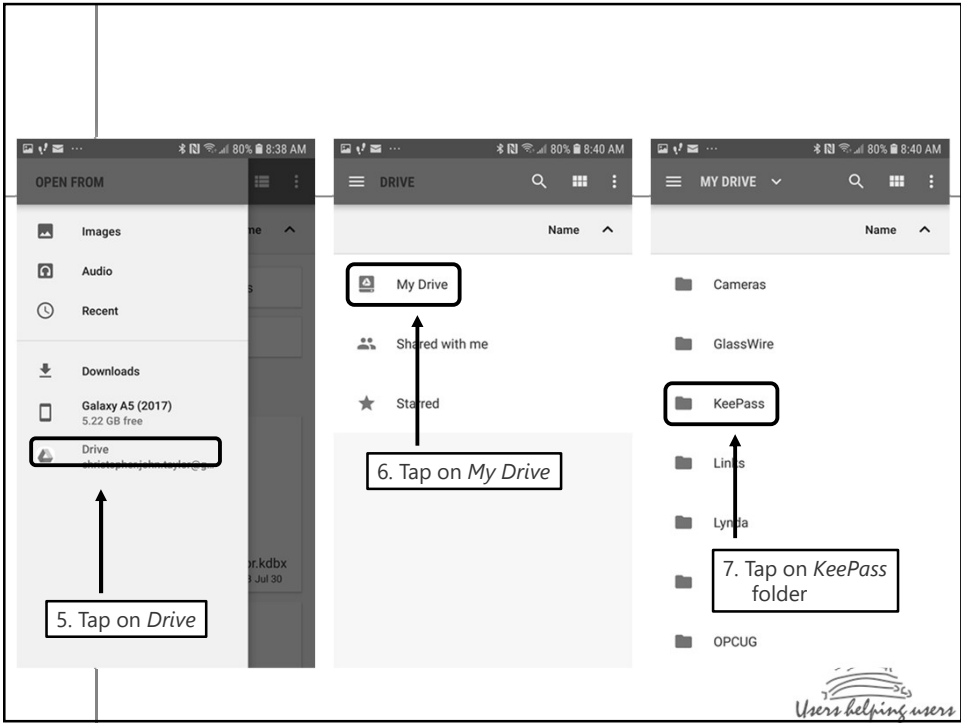
One time only

- KeePassDroid on your phone needs to know the name and location of your KeePass database file
 - The next three slides show what has to be done ONLY ONCE on your phone



1. Open KeePassDroid on phone



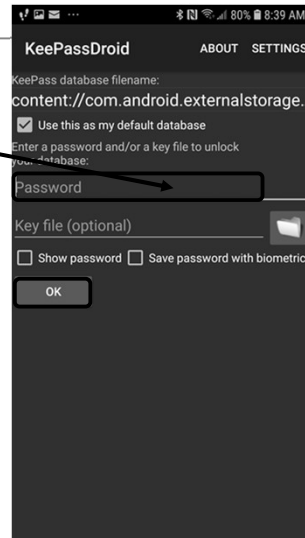


Using KeePassDroid

1. Open KeePassDroid on phone

2. Enter the password for your KeePass database


3. Tap OK





Automatic synching


- You can make changes to
 - KeePass in Windows
 - KeePassDroid on phone
- Changes will be automatically synched
- *Don't*
 - *make changes to both at the same time*




	<h2>Extras</h2>
	<ul style="list-style-type: none">■ Periodically backup your KeePass database<ul style="list-style-type: none">– if database ever corrupted, recover backup■ Explore menus or see help<ul style="list-style-type: none">– clipboard auto-clear time– lock workspace after KeePass inactivity<ul style="list-style-type: none">■ KeePass won't lock if an entry is open– Esc in main window locks workspace– <i>View Always on Top</i>– auto-fill web logon credentials– <i>Find Duplicate Passwords</i><ul style="list-style-type: none">■ change passwords on such sites 

	<h2>Other password-related issues</h2> 

	<h2>Security questions</h2>
	<ul style="list-style-type: none">■ Some sites allow password resets<ul style="list-style-type: none">– if you know answers to security questions<ul style="list-style-type: none">■ what city were you married in?■ what's your favourite food?■ what is your mother's maiden name?■ Could anyone find the answers with a little online research? 

	<h2>Security questions</h2>
	<ul style="list-style-type: none">■ Solution one<ul style="list-style-type: none">– give nonsense answers– record answers in KeePass's <i>Notes</i> field<ul style="list-style-type: none">■ Q. What is your favourite author?■ A. sleep■ Q. What high school did you go to?■ A. plastic 

	<h2>Security questions</h2>
	<ul style="list-style-type: none">■ Solution two<ul style="list-style-type: none">– answer correctly (easy to remember)– always add same “secret” word (eg. tap)<ul style="list-style-type: none">■ Q. What is your favourite food?■ A. tappizza■ Q. Where were you born?■ A. tapottawa– record in Notes field in KeePass as well 

	<h2>Data breaches</h2>
	<ul style="list-style-type: none">■ Register your email addresses<ul style="list-style-type: none">– https://haveibeenpwned.com/■ They will email you<ul style="list-style-type: none">– if your address shows up in a data breach■ At breached sites<ul style="list-style-type: none">– change password– change answers to security questions 

Digital inheritance

- Don't let online accounts die with you
- For others to get access to your online accounts
 - may be impossible
 - always will be difficult
 - may be costly



Digital inheritance

- You can provide access
 - it is all in your KeePass database
- Minimum information
 - you have a *KeePass* database
 - name & location of .kdbx (database) file
 - password to open password database
 - sign in username & password for computer



Digital inheritance

Print Emergency Sheet

File Group Entry Find View Tools Help

New... Ctrl+N

Open Ctrl+O

Open Recent

Close Ctrl+W

Save Ctrl+S

Save As

Database Settings...

Change Master Key...

Print Ctrl+P

Print Emergency Sheet

Import...

Export...

Synchronize

Lock Workspace Ctrl+L

Exit Ctrl+Q

oo-User.kdbx

User Name	Password	URL
o paste... 123456789	*****	
ook JoeUser@example.com	*****	
ay Inn JoeUser@example.com	*****	https://
erCard	*****	
ort	*****	https://

Group: Passwords-Joe-User, Title: VirusTotal, User Name: ctaylor.ca@outlook.com, Password: *****, URL: https://www.virustotal.com/gui/sign-in, Creation Time: 2020-07-21 11:22:06 AM, Last Modification Time: 2020-07-21 11:23:01 AM

1 of 6 selected Ready.

KeePass Emergency Sheet

Database

Database file: C:\Users\CTaylor\Documents\Passwords-Joe-User.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

Master password: Username/password to sign into your computer

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 have access to it.

If you lose the database file or any of the entries (composition), all data stored in the database is lost. There is no 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/>.

Users helping users

Digital inheritance

■ Very helpful

- links to KeePass help info
 - show the person how it works
- what you want done with online accounts
- KeePass entry detailing what entries are most important & what you would like done
 - name it !Read Me so it is sorted at top

OPCUG

Users helping users

Digital inheritance

- Don't forget!
 - they will need
 - username/password to sign in to your computer



Digital inheritance

- Leave info with
 - Power of attorney
 - Executor
 - someone you trust
 - safe deposit box
 - if someone else knows to access in emergency



Digital inheritance

- Are you executor / power of attorney for someone else?
- Ask what they want done with online accounts
- Ask if they want to give you access
 - in the event of incapacitation or death



This deck available at:
<https://opcug.ca/presentations/keeping-passwords-safe.pdf>

