



Password Managers

Joel Ewing

- **These presentation slides will be added to the BVCC website (under Information → Presentations)**

BVCC

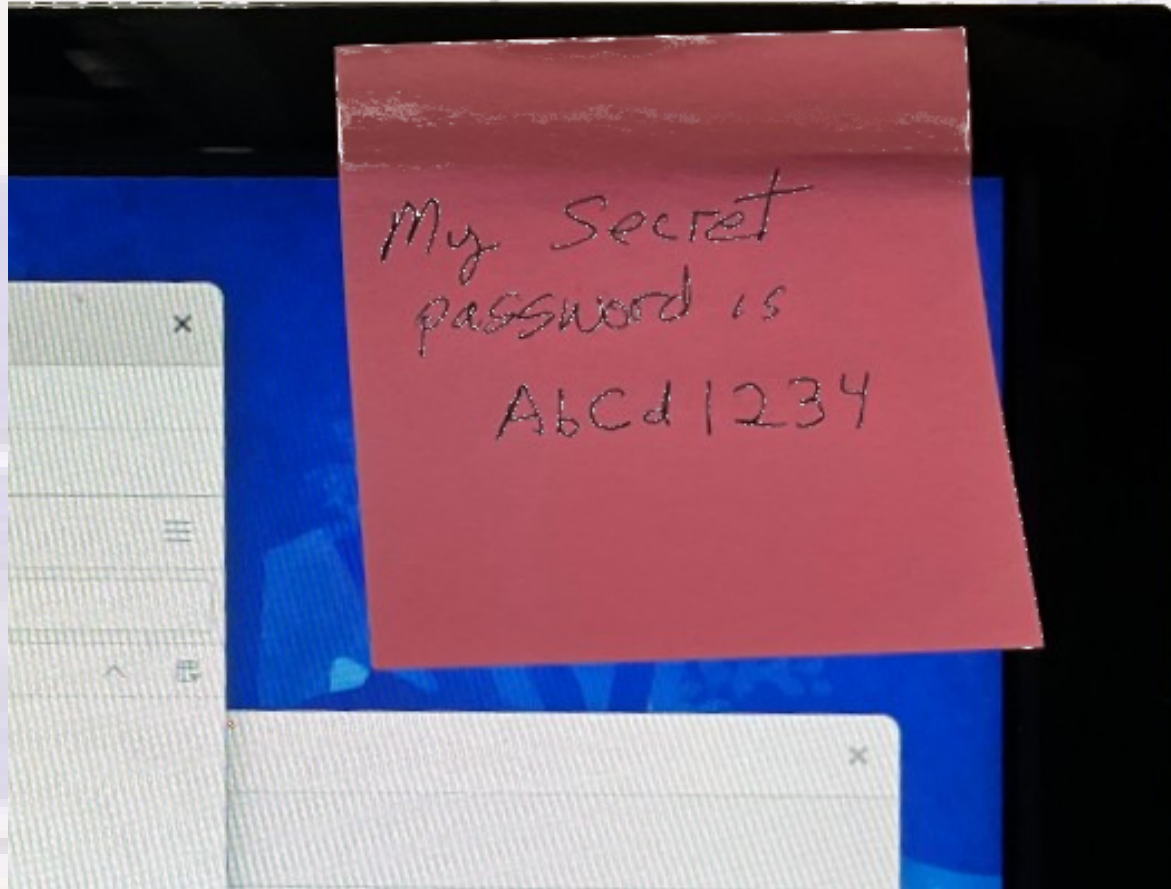
Why Password Managers?

BYCS

Early Password Management

- **Much simpler times in early days of Internet access in 1990's**
 - **Very few accounts – dial up Internet access, one email account, ?**
 - **Using same password on multiple accounts not a serious exposure**
 - **Typically no on-line financial accounts, no on-line shopping, so minimal financial value of accounts to tempt hackers**
 - **Slower Internet and slower PCs also made automated trial-and-error attacks similarly slow – could get by with shorter passwords**

Simpler Times, Simpler Password Management



On-Line Accounts Today

- **One user may need to track a large number (100's) of accounts**
 - **Some may represent financial assets of considerable value**
 - **Some may be able authorize significant expenditures**
 - **Some email accounts may be able to reset access to above accounts**
 - **All of the above need to be protected by good, unique passwords**

Password Quality

- **Single most important factor: Unique for each account**
- **Length: consider 14-17 characters; 8 no longer adequate**
- **Include upper & lower case letter, numbers**
 - **Some special characters can cause problems at different sites – avoid unless a special character is required by the site**
 - **Adding one more character to a random password without special characters is always more secure than a shorter random password that allows special characters**
- **Random is most secure, but hardest to create (without help), to remember, and type**
- **Avoid dictionary words, even with added numbers, and "worst" passwords**
- **Phrases of multiple words may be used, but need to be longer than a random password and use words that would normally not appear together in order to be equally secure**

Why Uniqueness?

- **Many on-line accounts now use an email address for an account "user name"**
 - **Means one user may have many accounts with same email user name**
 - **There are still people who use same password for multiple accounts**
 - **If hackers compromise a website and find a valid username-password combination for that website, they will try the same username-password combination on thousands of other popular websites and may compromise many other accounts for that user if unique passwords have not been used.**

100 Worst Passwords of 2023

- See <https://www.purevpn.com/blog/worst-password-list/>

123456

12345678

123456789

12345

1234567

password

1password

abc123

qwerty

111111

1234

iloveyou

sunshine

monkey

1234567890

123123

princess

baseball

dragon

football

shadow

soccer

unknown

000000

myspace1

purple

fuckyou

superman

Tigger

buster

pepper

ginger

qwerty123

qwerty1

peanut

summer

654321

michael1

cookie

LinkedIn

whatever

mustang

qwertyuiop

123456a

...

How Account Passwords are Hacked

- **Social engineering, phishing, tricking user into revealing account credentials**
- **Malware attacks against your PC or against website where you have an account to extract information – websites usually only store a hashed version of account passwords, not the true password**
- **Brute force attack given user name and a hashed version of the password (from a compromised website)**

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023


Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years



› Learn how we made this table at hivesystems.io/password

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years


[Learn how we made this table at hivesystems.io/password](https://hivesystems.io/password)

11

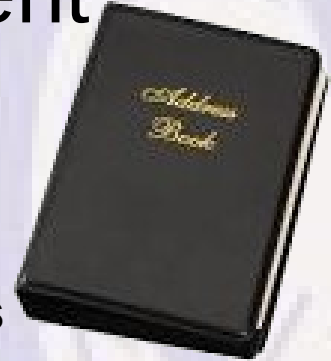
The time estimates are a minimum time scenario:
 Assumes that a hashed version of password is available, so to "try" a password involves hashing a candidate and a comparison to the known hashed password, not any interaction with a website.
 Assumes an older, still-in-use, less-compute-intensive hash technique was used
 Assumes the hacker can afford to employ a large number of graphic processor units to do many calculations in parallel, using resources currently available in the cloud and to groups doing AI development.
 For hackers with lesser resources, or sites using the most current hashing method, the times would be considerably larger.

How To Manage Passwords Reliably

- **Using longer, unique passwords for many accounts means there must be a well defined process for management to avoid chaos. The possibilities are:**
 - **More formalized handwritten manual techniques**
 - **Using digital documents using existing general purpose apps (like Word or Excel)**
 - **Using a Password Manager app expressly written to manage account credentials in a specially designed secure database.**

Manual Password Management

- **Use a notes in a small binder or address book**
 - Doesn't scale well as number of accounts increases
 - Errors in transcription when saving or using passwords
 - Making changes – readability & reliability may degrade over time
 - Readability of handwriting
 - Backups? – what if password booklet lost, stolen. Anyone with access may access all your accounts. You might lose access yourself.
 - Making information available to heirs – Do they have a way to find your account records? Can they understand your conventions and read your writing?



Using General Purpose Apps For Passwords

- **File can be saved encrypted with a "good" password**
 - **Both LibreOffice and MS Office can save documents and spreadsheets with a file password to encrypt the file**
 - **Saving without a password means anyone getting a copy of your file (on thumb drive, backup drive, via malware) reveals all your accounts – NOT A GOOD IDEA**
 - **Can use copy/paste to eliminate transcription errors when saving or using account credentials**
 - **Easy to make copies of "password" file for backup, off-site copies, or portable copies for use on other devices**

Disadvantages of General Purpose Apps

- **Once the file is opened with encryption password, all info for all accounts is visible (exposing your accounts if others can see your screen)**
- **No easy way to organize entries into categories – just a sequential list**
 - **As number of entries becomes larger, may have to scroll through multiple screens to locate needed entry**
- **Offers no support for generating "random" passwords**
 - **Passwords generated manually are invariably less random, have unconscious patterns, easier to hack**

My Web Browser Can Save Login Info

- **But,**
 - **Different browsers save login info in different places: Chrome (based on Google account), Edge (based on MS account), etc. instead of one common database**
 - **Can't save logins not associated with a website, or save other security info related to an account**
 - **Information saved in a password manager can be used with any web browser, application, and even for access codes not used on your computers or mobile devices**

Examples of Password Managers

- **A search for password managers finds many lists. Look for ones on several lists. Many choices. Examples:**
 - **Bitwarden (Forbes: best free option),**
 - **Dashlane,**
 - **Keeper,**
 - **NordPass,**
 - **1Password,**
 - **Norton Password Manager,**
 - **LastPass,**
 - **RoboForm,**
 - **KeePassXC**

Things to Look For

- **Availability of free version – what restrictions?**
- **Auto Sync across all devices is a feature most want**
 - **Implies a copy of your encrypted database on cloud server**
 - You will set up an associated account
 - Look for managers claiming ZK (Zero Knowledge): your actual encryption password is not stored in any form on the cloud service or known to the service provider. Even a court order or someone with total access to and knowledge about the cloud server cannot access your encrypted data, provided...
 - You need to err on the side of longer and more secure master password for the password manager database.
 - LastPass has reported an incident where encrypted user password databases have been accessed and potentially downloaded. Other auto-sync password managers are potentially vulnerable as well. SO, use a secure master password that cannot be hacked for thousands of years and it won't matter if bad people see your encrypted password database.

Things to Look For

- **A way to backup or export your data**
 - In a format that would preserve your essential data should support for the password manager cease
 - That would allow copies off-site, like in a bank box, for disaster recovery
- **Auto-fill support for the browsers you use**
 - Most password managers have plug-ins for common web browsers
 - Some techniques websites use to defeat automated login hacking may also interfere with this auto-fill support, but copy/paste always works
- **Support for all platforms you use: Linux, Windows, macOS, iOS, Android**

Things to Look For

- **Some managers provide a way to share credentials or folder of credentials to another user (e.g., other family members with family subscription to LastPass)**
 - **Seems like this feature might be mutually exclusive with Zero Knowledge of encryption passwords**
- **The design of password managers that auto-sync implicitly assumes you have a single common account with one password database. Can't support multiple databases on the same device.**

Paranoid? Don't Need Real Time Auto-Sync?

- **Consider the KeePassXC Password Manager**
 - **Open source, completely free on Windows, Linux, macOS. There is a chargeable app for iPhone/iPad that is compatible with the KeePassXC database format.**
 - **Database is a single file and by default stored only on local machine**
 - **Copies of database may be placed on external media, ported to your other devices via personal cloud storage or external media, which may also be used as disaster recovery backups. You have complete control over where the database is stored, when copies are made, and with whom you share copies.**
 - **Since databases aren't associated with a logged-in account, multiple databases are easily supported and multiple databases can be open at the same time when copy/paste are used for username & password. Extremely useful when you have to track independent personal and organizational (BVCC) sets of passwords.**

bvcc-mainc.kdbx - KeePassXC

Database Entries Groups Tools View Help

Search (Ctrl+F)...

homepwc.kdbx [Locked] × bvcc-mainc.kdbx ×

- W7
 - MobileBeacon(obs)
 - TrueNAS
 - Treas
 - Internet
 - eMail
 - Financial
 - Other
 - obsolete
 - wm
 - WebMgmt
 - eMail
 - Old
 - Backup
 - Recycle Bin
 - VP

Searches and Tags

- Clear Search
- All Entries
- Expired
- Weak Passwords

Title	Username	URL	Notes
dis-notes		http://bvcompclu...
dis-notes		https://bvcomput...
mxtoolbox.com	https://mxtoolbo...
R4L-Board22-files	https://bvcomput...
R4L-Board22-files	https://bvcomput...
r4l-DB_user		
R4L-FTPS		ftps://ftpes.bvco...
r4l-test		
R4L.com-Ad		https://www.r4l.c...
R4L.com-Alt		https://www.r4l.c...

Root / wm / WebMgmt

General Advanced

Username [Masked]

Password [Masked]

Tags

Notes [Masked]

- Copy Username Ctrl+B
- Copy Password Ctrl+C
- Copy URL Ctrl+U
- Copy Attribute
- TOTP
- Tags
- Perform Auto-Type
- Edit Entry... Ctrl+E
- Clone Entry... Ctrl+K
- Delete Entry... Del
- New Entry... Ctrl+N
- Open URL Ctrl+Shift+U
- Download Favicon Ctrl+Shift+D

https://bvcomputerclub.org/board

Never

13 Entries

KeePassXC (Linux) accessing two databases, with right-click on one entry in one sub-folder of BVCC database.

Display of username, password, & notes suppressed by default, but can be temporarily overridden for selected entry.

Questions?

BYSS