



Password Managers **A Quick Tour, and Why You** **Should Be Using One**

Ray Parker

PATACS / OPCUG Joint Meeting

2020 July 18

Epsilonlogix

About Today's Presentation

- You may see or hear things that give you cause for fear
- “FUD” is a tactic that has been used to sell you things for most of your life
 - IBM was famous for this decades ago; and it uses suggestive thoughts designed to encourage the feelings of:
 - Fear
 - Uncertainty
 - Doubt
- I have nothing to gain here, except your understanding of solutions which could help you navigate a world of scary people who want what you have
- The realm of Security is the one place where FUD can call you to action **BEFORE** an emergency arises

What Is A Password Manager?

- Any mechanism that allow you to track and store the many passwords you have today:
 - A leaky memory (mine and yours!)
 - A legal pad
 - A stack of Post-It notes
 - An Excel spreadsheet
 - A software tool designed expressly for this purpose
- What defines the better or worse characteristics of each of these?
 - How many passwords do you have today?
 - Which methods securely store your data?
 - Which methods allow you access from multiple locations?

Why Use A Password Manager At All?

- **We have far more accounts than we needed just a few years ago:**
 - Mortgage/Rent
 - Electric
 - Gas
 - Water
 - HOA
 - Shopping (dozens!)
 - Credit cards (dozens!)
 - Internal Revenue Service
 - Social Security Administration
 - Department of Motor Vehicles
 - Banking
 - Email

Why Use A Password Manager At All?

- **We have far more accounts than we used to have:**

- Mortgage/Rent
- Electric
- Gas
- Water
- HOA
- Shopping (dozens!)
- Credit cards (dozens!)
- Internal Revenue Service*
- Social Security Administration*
- Department of Motor Vehicles
- Banking
- Email

I currently have over **100** accounts that support my *personal* life.

If I include my *professional* life, the number today is **457**.

If I include my *customers*, the number today is **1,554**.

* If you don't have these already, you should!

Why Use A Password Manager At All? - 2

- **Security breaches happen nearly every week:**
 - <https://haveibeenpwned.com/>
 - If you don't know about this site and its author Troy Hunt, you should
 - Register your email with it, and **trust** what it tells you (many well-known companies do!)
 - 456 pwned websites
 - 9,824,438,995 pwned accounts
 - 113,658 pastes
 - 194,613,392 paste accounts
 - In my own case, **16** breached sites, including:
 - Adobe
 - Canva
 - Dropbox
 - Evite
 - Kickstarter
 - LinkedIn









Why Use A Password Manager At All? - 3

- **How many sites do you use that support (or even require) two-factor authentication (2FA)?**
 - Does your current password manager support 2FA?
 - Most can contain simple lists of pre-authorized codes
 - Some can handle 2FA calculation methods
- **Your phone is commonly used as the second authentication method, but what happens if you lose or cannot otherwise access your phone?**
 - You might lose access to your online banking!
 - In many cases, you have no choice, so fix what you can and leave the rest
- Note: **ANY** version of multi-factor authentication is superior to using only a password

Why Use A Password Manager At All? - 4

- **Do you know what a “Dictionary Attack” is?**
 - This is an attack that collects email addresses in one column and compromised passwords in another column
 - Each email address in the first column is paired with every one of the passwords in the second column, one at a time
 - The largest collections of these contain **hundreds of millions** of email addresses alone
- **Do any of your passwords get reused in more than one place?**
 - Unless your answer is **ABSOLUTELY NOT**, you are at risk
- **Does your current password management method warn you when a password you are using today has been reported as a breached password?**



Largest breaches		Recently added breaches	
	772,904,991 Collection #1 accounts		3,805,863 Quidd accounts
	763,117,241 Verifications.io accounts		582,578 Foodora accounts
	711,477,622 Onliner Spambot accounts		25,692,862 Mathway accounts
	622,161,052 Data Enrichment Exposure From PDL Customer accounts		3,589,795 Zoomcar accounts
	593,427,119 Exploit.In accounts		68,693,853 Lead Hunter accounts
	457,962,538 Anti Public Combo List accounts		9,705,172 Wishbone (2020) accounts
	393,430,309 River City Media Spam List accounts		26,372,781 LiveJournal accounts
	359,420,698 MySpace accounts		990,919 PetFlow accounts
	234,842,089 NetEase accounts		1,079,970 Artsy accounts
	172,869,660 Zynga accounts		3,670,561 Lifebear accounts

Why Use A Password Manager At All? - 5

- There are more ways you could find yourself in trouble
- If the previous slides have not already convinced you, there is little point in continuing
- There are methods that plan to eliminate passwords altogether
 - **Biometrics** are simple and easy, but privacy advocates know that authorities can forcibly compel you to unlock anything that was locked with biometrics
 - **Dongles** are physical “keys” that plug into your device and are very safe, but sometimes very clumsy, and don’t necessarily plug into every device you have
 - **Automatic login without a password**: SQRL works well, but is not widely adopted
 - Many more exist, but lack of widespread support creates its own problem



A **Partial** List Of Password Managers

- 1Password
- Apple Keychain
- BitWarden
- Chrome
- Dashlane
- Firefox
- Kaspersky
- KeePass
- Keeper
- LastPass
- LogMeOnce
- McAfee
- MyKi
- Norton 360 Deluxe
- Password Boss
- RoboForm
- Safari
- Sticky Password
- True Key
- Zoho Vault

What Should A Password Manager Do?

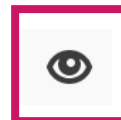
- Capture your password **automatically**
 - If you must do it manually, it significantly increases the chances of an error
- Store it somewhere
 - Secure storage is a good option, but it is an option you have to seek out
- Populate your web page or mobile app userid/password when needed
 - Why not also make filling out form fields easier?
- Provide some level of management oversight
 - Import/Export/View/Edit/Evaluate/Warn/etc.
- Allow you to access and use your data on more than one platform
 - Because you HAVE more than one platform
- **Provide all of that while only requiring you to remember a single password**

Browser: Chrome

- Not a Password Manager, but a feature built into the Chrome browser
- Synchronization provided: Yes, only to Chrome browsers on other platforms
 - Provided when “Allow Chrome sign-in” is enabled, and you are signed into Chrome
- To access:
 - Click on 3-dot menu in the upper-right corner 
 - Click **Settings**
 - Click **Autofill** in left menu
 - Click **Passwords**
 - Enable “Offer to save passwords”
 - Enable “Auto Sign-In” if you wish
 - Click the “eye” icon to view any password 

Browser & Product: Firefox Lockwise

- A feature built into the Firefox browser AND a minimal Password Manager
- Synchronization provided: Yes, to Firefox browsers on other platforms
 - Provided when “Sign-in to Sync” is enabled, and you are signed in
- Lockwise is available separately on iOS and Android
- To access in Firefox:
 - Click on “hamburger” menu in the upper-right corner
 - Click Logins and Passwords
 - Firefox Lockwise opens
 - Click the “eye” icon to view any password



Browsers: Beware!

- Browsers store their passwords **silently**, so there is little indication that anything is happening
- A desktop computer was setup as a kiosk in an office, and the browser was used to make payments by at least 40 people, including me
- When I mentioned this to the Manager, telling her how many sets of credentials were stored that, I received a completely blank look
- I deleted all of them myself
- **Browsers that manage passwords do so by default, so you must remember to disable those features you don't want.**
- Be careful, because Microsoft (and possibly others) may reset those options during the application of service

Product: 1Password

- Supports Windows, macOS, Android, iOS, and popular browsers
- Watchtower feature identifies password issues, including weak, duplicate, and known vulnerable (breached) passwords
- Tag feature allows organization of data any way you want it
- Organization supports multiple password vaults, which can be easily shared
- Supports 19 different content types, including documents
- Syncs between multiple devices (paid subscription)
- Credential filling requires a little practice, then becomes easy
- Supports Universal Second Factor (U2F) hardware keys
- No free version, but there is a 30-day free trial



Product: Dashlane

- Supports Windows, macOS, Android, iOS, and popular browsers
- Password Health feature evaluates your passwords, including weak and known vulnerable (breached) passwords
- Supports Universal Second Factor (U2F) hardware keys
- Syncs between multiple devices (paid subscription)
- Supports Authenticator-type 2FA
- Contains a built-in VPN of reasonable quality (paid subscription)
- Establish an Emergency Contact for... emergencies!



Product: LastPass

- Supports Windows, macOS, Android, iOS, and popular browsers
- Free version has capabilities of many paid versions
 - Unlikely to need the premium version
- Actionable password strength report
- Organization supports nested folders only
- Establish Emergency Contacts for... emergencies!
- Better (but not perfect) form filling capability

LastPass... |

Product: RoboForm

- Supports Windows, macOS, Linux, Android, iOS, and popular browsers
- Oldest product, has the most robust form filling capability
- Can also provide passwords for Windows applications
- Security Center identifies weak and duplicate passwords
- Syncs between multiple devices (paid subscription)
- Establish Emergency Contacts for... emergencies!
- Limited 2FA support

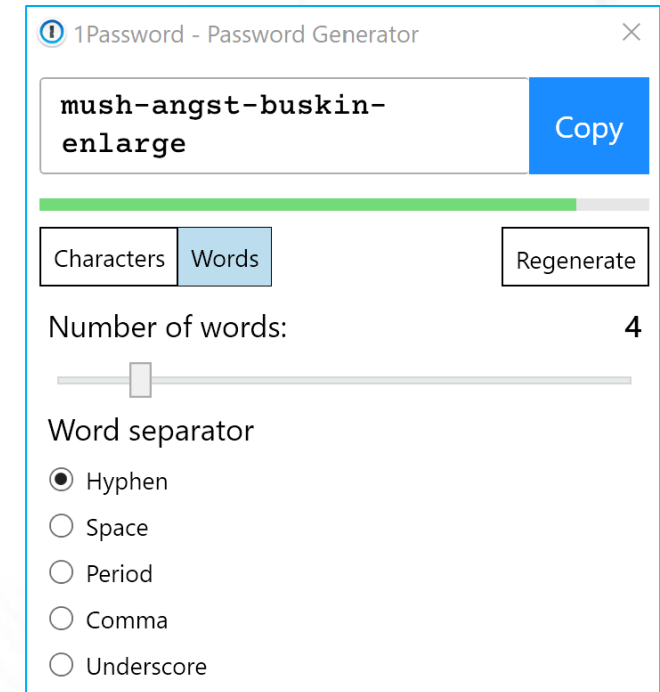


You Have A Tool, Now What?

- Learn how to use it:
 - They all behave differently
 - Some autofill everything, some don't autofill anything
 - Check ALL the product options to see if any need to be changed
 - **Always disable auto-login; it is a security risk (as well as an occasional pain)**
 - Test your synchronization
 - I dropped one subscription product after 2 years because sync kept failing
- Desktop/Laptop/Mobile browsers:
 - You may need to install a browser extension to use it efficiently
 - One product requires you to use their own browser (I don't care for their browser)
- Mobile devices:
 - Android and iOS platforms require a one-time setup step to allow your new tool to interact with your phone's applications
 - On my phone, the very first time I sign in with a new app, I must designate the correct stored password for this app, because there is no URL to parse

What Else Do You Need?

- Passwords!
- Password Generator
 - Very nice feature to have, as it easily resolves most (but not all) of the issues with creating new passwords
 - It's common for one product running on different platforms to have different defaults for the passwords they generate
- A few Password Managers which support this feature:
 - 1Password
 - Dashlane
 - LastPass
 - RoboForm



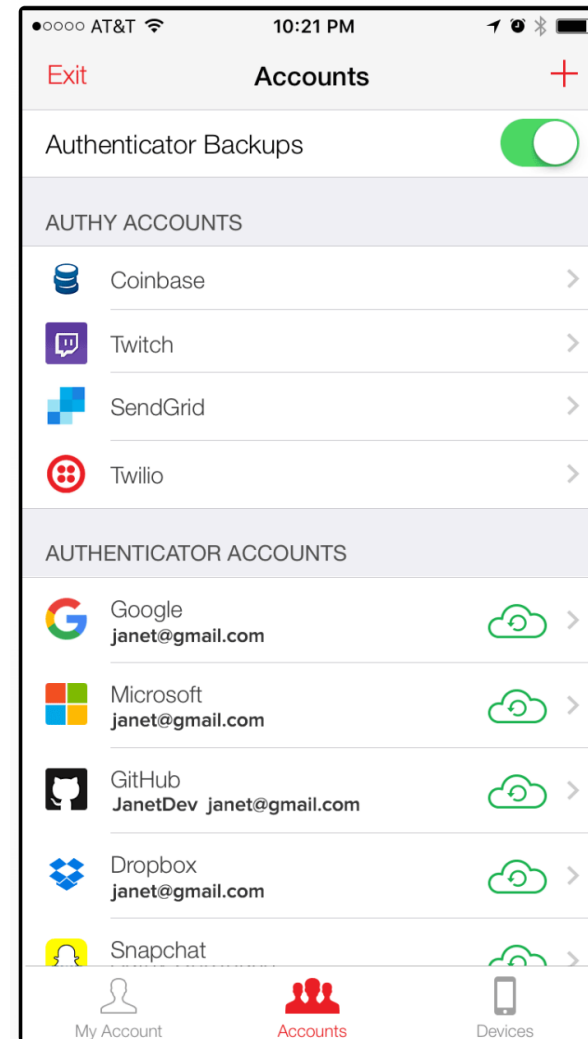
Password Policies & Tips

- In the beginning, there was no standard password policy
- A few years ago, an expert suggested the use of mixed-character passwords
 - They are very hard to remember, hard to type, and not really very good
 - The expert who suggested this policy now regrets it
- What is the one factor that best determines the strength of a password?
 - **Length**. Not complexity, use of mixed characters, etc.
- **Tip:** Passphrases
 - Long strings of random words connected by a standard character of your choice
- **Tip:** Password stuffing
 - Using a character (or string) of your choice to make a password longer

mush-angst-buskin- enlarge

What Else Do You Need?

- Two-factor authentication (2FA)
 - Your phone
 - Common, but not always the best choice
 - **Authy (free)**
 - iOS, Android, MacOS, Win32, Win64, Linux
 - Syncs across multiple devices
 - Supplies 2FA guides for use with many sites
 - Supports backup/restore
 - Google Authenticator (free)
 - iOS and Android
 - Microsoft Authenticator (free)
 - iOS and Android
 - Many, many more



What Else Do You Need?

- Patience
 - Many web sites do not clearly delineate their password policies:
 - “At least 8 characters”
 - Surprisingly, they frequently limit the length
 - “At least 1 special character”
 - Yes, but which ones are allowed?
 - “At least 1 lower-case and 1 upper-case letter”
 - When they do display a password policy, it may well be wrong
 - The people who are coding these pages are not senior people, and frequently make mistakes in the implementation
 - Many pages were coded more than a few years ago, and won’t be changed
 - You are trying to push them into the 21st century, so you will see this often

Really, Why Use A Password Manager?

- It automates much of what you do anyway
- It allows you to create, store, and manage many passwords
- It allows you to create, store, and manage **data other than passwords**
 - Credit cards, passports, documents, notes, license keys, and more
- Secure storage means you can retrieve YOUR data when you need it
- What does secure mean?
 - If I lose the master password, they can't recover the data
 - This is the correct answer!
 - I can store data without concern for sensitivity

Can I Get All Those Features For Free?

- A number of products are available with a free version
 - Sync capability is the usually the first feature to be discarded for free accounts
- The best products have the best features, but also charge a premium
 - Yearly subscription costs range from \$11-\$90
 - \$35 will get you an excellent product that you can depend on
 - Some products have “Family” options, so you can manage all the passwords everyone needs, and decide who gets to use them
- Take the time to check the reviews on the next slide
 - Once you have an idea of the features you want, they are easier to work through
- This is the best use case I know for actually having a subscription

Password Manager Reviews

- Consumer Reports – March 2020
 - <https://www.consumerreports.org/password-managers/best-password-managers-review-digital-security-privacy-ease-of-use/>
- PC Magazine – July 1, 2020
 - <https://www.pcmag.com/picks/the-best-password-managers>
- CNET – June 29, 2020
 - <https://www.cnet.com/how-to/best-password-manager-to-use-for-2020-1password-last-password-more-compared/>
- PC World – May 28, 2020
 - <https://www.pcworld.com/article/3207185/best-password-managers-reviews-and-buying-advice.html>

Questions?

