Online Security & Passwords

Security must be a combination of safe computing practices and security products. No product can or ever will, provide complete security. YOU need to be careful and aware. If you are not part of the solution, you are the problem and hackers will break into your accounts. Passkeys are starting to replace passwords. The average person today has 100 accounts and passwords to manage. Most people would get a Failing grade of F for what they do today.

Why You Need A Password Manager

In the past I recommended people use a password manager, today everyone MUST use a password manager. Using other methods like a notebook, post-it notes, spreadsheet, or document does not work.

Advantages:

- You don't have to remember each password, so each one can be unique, long, and strong.
- Available on all devices like Phones, Tablets, Laptops, and Desktops. Available anywhere at any time.
- Strong passwords can be generated for you.
- Help you change passwords and track old passwords.
- Document challenge questions and notes
- Safer than storing Accounts and Passwords in a Browser or other methods

Features to consider when comparing password managers:

- **Cost -** Per device, limited free version or with ads. What devices or browsers does it support?
- **Automatic Capture** – Capture/setup username and password data as you enter it?
- **Automatic Replay** – Enter your password and login information for you?
- **Fill Web Forms** – Checkout information on a shopping site (Name, address, phone, etc.)?
- **Retains History of passwords** – In case you need an old password after making a change?
- **Support Multiple Identities** – Multiple profiles/accounts and select which one to use?
- **Strength Report** – Analyze the strength of your passwords and help you to improve them?
- **Two-Factor Authentication** – Biometric, SMS-based, Google Authenticator, or something else?
- **Application Passwords** – Does it support password storage for apps?
- **Import** – Import passwords you stored in your browser or competitors software?
- **Export Data** – Can the software export the data (for example to a .CSV file) for your backup?
- **Secure Sharing** – Sharing of passwords, messages, or documents with others?
- **Digital Legacy** – Grant access to an inheritor in the event that something happens to you?
- **Secure Online File Storage** – Save and share files/documents? Will, Passport, etc.

What I Use - Bitwarden

I recommended and used LastPass for 15 years till 2021 when they started to charge to use it on multiple devices. I now use the free version of Bitwarden https://bitwarden.com which has all the features I need. You can store an unlimited number of passwords and sync them across all your devices. Bitwarden offers native apps for Windows, macOS, Linux, Android, and iOS. Bitwarden's browser extension supports Chrome, Edge, Firefox, Opera, and Safari. You can enable multi-factor authentication via an authenticator app with the free version. It supports Passkeys.I exported my LastPass accounts and passwords and imported them into Bitwarden with no trouble in under two minutes. BitWarden has a premium version for $10 a year which provides 1 GB encrypted file storage, Two-step login (YubiKey, U2F, Duo), Vault health reports, and Emergency Access if you need these features. Show demo.

My Recommended Changes to Bitwarden defaults:

- Settings\Vault Timeout – 1 hour or Never
- Settings\Other\Clear Clipboard – 5 minutes
- Settings\Other\AutoFill\Enable Auto-fill on Page Load – Check box
- On phone or tablet app turn on fingerprint or face login

What are Passkeys and why you need them

A passkey is a new way to sign in that works without passwords. It uses biometric info like a Face ID, fingerprint, gestor, or PIN security you set up on your device. It is a standard promoted by Google, Apple, Microsoft, the World Wide Web Consortium. A passkey consists of two cryptographic keys, a public key that's registered or stored with the online service or app, and a private key that's stored on a device, such as a smartphone, tablet, or computer. When there is a data breach and a hacker gets their hands on a website's public key, the user's account is still locked because they don't have access to the private key on the user's device. Video 01:00: https://www.youtube.com/watch?v=IRafnET5S5Q

Passkeys can also help you get around the issue of having to synchronize passwords between your devices. Say you normally log in to your Google account using a smartphone, but you want to login using a laptop. That's no problem, even if the passkey isn't synchronized with the laptop, as long as the smartphone is within Bluetooth range of the laptop and the user approves the login. What's even better is that the passkey isn't transferred between the smartphone and laptop, but after confirming the login, the user instead gets the opportunity to create a passkey on the laptop if they want. No biometric information leaves your device; instead, it is used to unlock the passkey on the device.

System requirements: Windows 10+, MacOS Ventura+, ChromeOS 109+, iOS 16+, Android 9+, or a hardware security key with FIDO2 support. Also requires a current Chrome, Safari, or Edge browser.

Some well-known websites and apps that support the technology include Adobe, Amazon, Google, GitHub, PayPal, TikTok, Nintendo, WhatsApp, Shop by Shopify, X, eBay, and Uber. These are early days for passkeys, and soon we can expect across-the-board support. https://passkeys.directory/

Best way to experiment with how they work is to use the demo on: https://www.passkeys.io/ . If you're ready to take the plunge, a great place to start is by securing your Google Account with a passkey. Not only has Google made the process easy, but there's also extensive documentation available. We're a long, long way away from the death of passwords. Bitwarden, the password manager I recommend, supports passkeys. Apple users can also use the Apple Wallet or Bitwarden to sync passkeys to multiple devices.

Tips to Keep You Safe At Home

- Never, Never, Never re-use passwords between sites and accounts.
- Let the password manager generate a unique, long, and strong password.
- Change your passwords often. Especially Financial, Bank, and eMail at least once a year.
- Use two-factor authentication “2FA”, which will send a text with a code or use an Authenticator App.
- Act immediately when notified of a Data Breach and change your password.
- Use sites like “Have I been Pwned” https://haveibeenpwned.com/ to check for data breaches using your email. Over 10 billion accounts have been breached and are for sale.
- Use Credit monitoring to alert you to suspicious activity in your finances that may be due to identity theft.
- Backup your PC data, backup your PC data, and backup your PC data.
- Never download software or files from questionable sites or links.
- For your tablet or smartPhone, never install apps from outside Google Play or Apple App Store.
- Install and keep updated an AntiVirus program. For Windows 10 & 11 the Microsoft Antivirus is fine. On an Android device consider security software like "avast! Mobile Security & Antivirus", "Malwarebytes Anti-Malware", or "Bitdefender Mobile Security and Antivirus". I don’t think they are needed and they use CPU and drain your battery.
- Be wary of games, Peer-to-peer (P2P) clients, and any download claiming to be free versions of expensive software.
- Phishing tries to get you to provide confidential information (Social Security, credit card, bank, PIN, passwords, etc.). It’s estimated that 1.4 million websites are created every month to trick people.
- Be suspicious of ANY email that asks for sensitive personal information, even if the sender seems to be familiar. Call a phone number from another source (old bill etc.) to verify the message or link if there is any question.
- Password Managers will only Auto-Fill on authorized URLs/sites and not on fake sites.
- If you use a public PC, log off when you are finished and close the browser completely.
- For Account Challenge Questions enter false info for things like Birthday, Sport, Teacher, City, Street, etc. Example: First Car=Frog. Document the Q&A in your Password Manager Notes.
- When you “Friend” or “Like” on Facebook, you give permission to some personal information and messages. Enter false info or hide personal info.
- For home wireless security, see the past meeting on Home Network for settings.

Additional Links and Information

Carondelet Tech Help Resources: https://carondeletvillage.org/tech-help-resources/
Questions or comments can be sent to: TCKreuzer@gmail.com

https://www.pcmag.com/picks/the-best-password-managers
https://www.pcmag.com/picks/the-best-free-password-managers BitWarden is rated best