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 acquire your email and password and own your accounts. Solutions to replace accounts and passwords are being used for some services, but today we all need to manage our accounts and passwords. The average person has almost 100 accounts and passwords to manage. Most people would get an Failing grade for what they do today.

Today we need to be protected from:

- Cyber criminals who target large numbers of people in hopes of stealing information from a small percentage who are easily tricked or have not adequately protected their PC. This is a huge multi billion dollar business.
- Data Breaches exposing accounts and passwords to hackers.
- Companies capturing information about you that they can use or sell to other companies.
- Hackers who create problems for the fun of it.

Why You Need A Password Manager

Passwords are terrible, but we don't have a better solution today, so we have to make the best of it. For security, you must use a different non-guessable strong password for every site we use so a data breach on one site does not expose dozens of your other accounts. The only way we can accomplish that feat is by relying on a password manager.

You Don't Trust A Password Manager - There is a perceived vulnerability with password managers that all your eggs/data are in one basket and that a hacker could get all your accounts and passwords easily. This is FALSE, your data is encrypted with the unlock key only available to you. An employee of the password manager service or a hacker of the service site can not decrypt your data, so it is of no value to them even with a data breach. You do need to use a unique, long, and strong password as your master password and change it. Setup a recovery phone, email, or store in a safe place for if you forget the master password.

Advantages:

- You don't have to remember each password, so each one can be unique, long, and strong.
- Available on multiple devices Phone, Tablet, Laptop, and Desktop. Available anywhere at anytime.
- Strong passwords can be generated for you.
- Make it easy to change passwords.
- Cloud backup and track old passwords.
- 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 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 . The open-source software's free tier has few limitations and 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 also enable multi-factor authentication via an authenticator app with the free version. 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 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.
CNet review: https://www.cnet.com/tech/services-and-software/bitwarden-review-the-best-free-password-manager-for-2021

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 turn on fingerprint or face login

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.
- Only use secure sites "https://" when connected to public WiFi. A virtual private network (VPN) can also help.
- 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.
- Chrome Browser extension - Password Checkup helps you identify accounts that were affected by data breaches. Wherever you sign-in, if you enter a username and password that is no longer safe due to appearing in a data breach known to Google, you'll receive an alert. https://bgr.com/2019/02/05/google-password-checkup-chrome-plugin-will-identify-hacked-passwords/
- Backup your PC data, backup your PC data, and backup your PC data.
- Never download software or files from questionable sites, links, or download programs.
- For your tablet or smartPhone, never download apps from outside Google Play or iTunes who do the work of screening apps.
- 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.
- Never open unexpected e-mail attachments or links; be very careful what you click on.
- Phishing try's 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.
- Internet of Things "IoT" devices can have serious security problems - Your household is full of internet-aware devices, and most of them are woefully insecure, to the point where a hacker could take over the entire network by reaching in through your baby cam.
- For Account Challenge Question 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

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

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