IT Security – Password Management Recommendations

Passwords – how to keep & store passwords securely

Keep my passwords private – and unique

Don't reuse the same password on multiple sites. "Normal" passwords create a big security problem
Why? 1.2 Billion email & password combinations are available for sale on the dark web in free-text form
These exposed combinations can be used on any bank or credit card (or other) site in the world
Exposures didn't typically result from insecure behavior – but from hacks of sites you trusted
If you have used a "normal" password in the past, change the password on all sites – today would be good…

Password Management Principles

Enable two-factor authentication for all web accounts that offer it – especially important for email
Don't use work email address for personal accounts & don't use same passwords on home & work accounts
Never store written passwords anywhere around your desk or keyboard
Find out if your passwords have been compromised – PBSI can do a darkweb search - free on request

Use a Password Manager

Password Managers are secure – All mass-market Password Mangers are encrypted at high levels
Password Managers dramatically reduce issues with human memory, portability and security
Password adds/changes/updates are auto-shared among all your devices: PCs/Macs/tablets/phones
Never store your "master password" on your PC, Mac or phone when using a password manager

Don't Store Important Passwords on your Web Browser (Chrome, Edge, Firefox, Safari, etc.)

Web browsers are wide open & exposed if a device is hacked – every browser pw is available to a hacker
You may choose to store *some* passwords on web browsers for convenience, but know they are ***NOT*** secure

Idea to Create & Remember Unique Passwords

Choose a "normal" pw – but NEVER use it – just remember it - Include text portion and number portion
Example: "normal9" or "n9" = <mytext1234> - Of course, pick your own… don't use this example
Make notes to yourself (text & number portion) that don't expose the password, but make it knowable
For text portion, change or capitalize portions of the text: Ex: **n9 Cap 3rd** would = my**T**ext1234
For number portion: Replace numbers, so **n9 4433** would = mytext**4433**
Put it together: **n9 Cap 2nd 6543** = **mYtext6543**
Store your notes in a secure location

Alternatives to a Password Manager – Use tools you already use

OneNote – use an **Encrypted** OneNote tab – Benefit: OneNote can be protected by MFA
Word or Excel – **Encrypted** Word or Excel doc stored on your OneDrive/Google Drive for portability
Outlook Contact notes – no way to encrypt – Choose an obscure contact **not** in your family
None of these ideas is as secure as a Password Manager

No Passwords on Public Wi-Fi

Public Wi-Fi is not secure. Unless using a secure app or VPN, do not enter passwords on public Wi-Fi
Cellular is safe – When in a public place, cellular is always safe. Cellular traffic is always encrypted.