The Digital Sandwich Generation - adults who are the computer/network/technical "specialist" in the family and **who have a vested interest in keeping people safe**.

By definition, this generation is NOT the 4-year-old of the family. They do not have the cognitive ability to be IN the sandwich, they ARE part of the sandwich.

Best Strategies: The Digital Side
Know user IDs This usually involves email addresses or mobile phone numbers. If you (the Sandwich) knows the ID, hopefully you can reset unknown/forgotten passwords. Remember, there really is no recovery of passwords - they just need to be reset.

Know PASSWORDS. Oh, brother, if I had a quarter for everyone who didn't know a password….. I would have a lot of quarters. In this post, I am quoting heavily from Liquid Web, but when you find a good thing, there's no reason to reinvent it. Ms. Sapta Upendran does an excellent job summarizing the standards from NIST (see references at the end!).

> "The industry standards, according to Liquid Web, which is quoting from the National Institute of Standards and Technology, for passwords are as follows:

- DO Use Passwords of At Least Eight Characters Or Longer If Set By A Person: The more characters you use, the more difficult a password is to crack. Length is key. Create lengthy passwords of at least 8 characters!
- DO Use Passwords of At Least Six Characters Or Longer If Set By A System or Service: If you have a system in place that allows for new user creation, eg. an eCommerce site, a forum or basically any type of site that allows new users to sign up, the software should never allow less than a six character password.
- DO Allow Support For At Least A 64 Character Length: This setting should allow for use of passphrases when selecting a password
- DO Use a Combination of All ASCII Character Types: Use numbers, lowercase letters, uppercase letters and symbols in your password. (ex. XkeDZaJ6QG3E8!jKq3%yIOd3) This increases the overall entropy of the password and increases its chances of being compromised (Password entropy is the measure of how arbitrary or uncertain a password is. A passwords entropy is based on the type of character set used (including uppercase, lowercase, numbers, and special characters) and the length of the overall password.)
- DO Create Unique Passwords: Each password you use should be for a unique to each service you use (ex. cPanel, MySQL and, your bank account should all have different passwords).
- DO Verify Your Password Is NOT Listed In Known "Password Dictionaries": Using an online tool or software (in your program) should check against known password lists and should always be utilized

DO Use A Password Manager: Current best practice dictates that users should use a password manager to remember long, difficult passwords

- DO Randomly Generate the Password: Use one of the following sites to generate a secure password: Norton by Symantec, Random.org, or Random Password Generator
- DO Allow For At Least 10 Password Attempts Before a Lockout Is Initiated: The specified threshold is usually a balance between practicality and security depending on your companies risk level. This should be an adequate balance between allowing for possible user error and, limiting brute force attacks

- DO Use A Two-Factor Authentication System: The use of a Multifactor Authentication system as part of your security protocols will add an additional layer of protection. This includes methods like hardware key fobs, software like Google Authenticator and readable biometric data.

HAHAHAHAHAHAHA….. OK, so this is the best, what is happening in the real world? Well, most users are creating passwords that are 8 characters or more, because systems are demanding it. This is good for users. Lots of people are reusing passwords, which can be an issue, but system administrators have no real control of this.

I want to talk specifically about “password managers.” There are a bunch of digital managers online, and “but, bear in mind that a Password Manager is only as strong as its gateway passphrase which can allow access to ALL of your passwords. Although Liquidweb does not endorse any specific password manager, we can, however, provide a list of the most popular ones:

- Keeper
- Dashlane
- LastPass
- 1Password
- 1KeePass
- PWSafe. (Upendran, 2023)”

If a user forgets the main password to get into the manager, there can be many headaches! I have seen many patrons in my classes use regular analog password keepers - they are sold almost everywhere. Some are actual, dedicated alphabetical notebooks sold specifically for password management, and some are just old-fashioned address books. Regardless of what you use, keep it in a safe place - the password to the digital manager or the password book should be a part of your “in case of emergency” papers - your house deed, will, power of attorney, etc. Be careful with it! This is specifically where the Digital Sandwich comes in - many times both user IDs and PW have been set for people, older or younger. Keep this stuff safe!

A simple formula that I have suggested to many patrons that they find both useful and safe is this:

1. Create a couple of STRONG 8 character passwords (2 or 3)
2. Modify the password according to a set formula for each web site
3. Look at the settings in each web site/account. Each has a specific way to authenticate yourself if you forget a password. Many in the Sandwich put their own mobile number or email account as the backup. This can be a smart way to monitor people in your circle of responsibility.

References:

National Institute of Standards and Technology Whitepaper. (2024). Summarized by Meeba Gracy on Sprinto Web Site: https://sprinto.com/blog/nist-password-guidelines/.

Sapta Upendran. (2023). Top 10 Password Security Standards. Retrieved from Liquid Web Site: https://www.liquidweb.com/blog/password-security-standards/.