Do it yourself Structured User IDs and Passwords

Internet websites that provide a unique account for you which includes a password presents a new issue for you in an insecure world.

Recent breaches of security at well known websites suggest that you cannot rely on your password being protected. While these businesses may take action to protect you and provide compensation and services to limit the damage, this does not carry over to other websites that you maybe using the same password on.

Current advice from security experts maintain that you must have a unique password for each website. And are now saying that *keeping a written list* is the answer. This reversal of wisdom that cautioned you from keeping your passwords written down (paper memory) is new. Additionally, many websites are improving their security by making you create insane passwords.

Installing and using a Password Manger is one solution!

This presentation is for a do-it-yourself write it down on paper approach. Using Excel is even better. Because you can search for that website (if you have many).

Fashion a list as follows:

Website	User ID	Password	Notes
Optimium Online	John 0 - - -	1001 - - - - - -	
www.e-zpassny.com	johna	1002 - - - - - -	
www.samsung.com	john's gmail	1003 - - - - - -	
www.roku.com	john's gmail	1004 - - - - - -	pin 0 - - -
www.americanexpress.com	johna	7000 - - - - - -	My credit card account ending in 1002
www.youtube.com	john's gmail	use google gmail	
www.ebay.com	john's gmail	1010@ - - - - - -	
https://play.google.com/store	maria's gmail	use google gmail	android apps
www.protectmyid.com	john's gmail	3000J - - - - - -	experian id protection paid by Adobe
www.amazon.com	maria's gmail	1011 - - - - - -	
www.pseg.com	ajohn	2107 - - - - - -	

Why this works

- you cannot remember many unique passwords and/or user ids (websites might not allow your usual ID)

- you must be able to accommodate website password rules

- the - - - - - - is your secret password kept in your head (never changing and not from your ID)

- denote a pin number likewise 0 - - - or 22 - - - with - - - being your secret number

- many sites accept your email address as user id (so indicate which address you use)

- some sites are related to a parent like Google and consolidate login – so you do use the same password

- some require special characters like @ or uppercase letter

- the list is useless to other people - encourages you to get rid of real written passwords (which are useful)

- if a website is breached you only have to change that website's password

Your secret word must not be from your ID information. Sites are starting to block usage of anything that appears in the rest of your registration ID information. 6 Characters - - - - - - makes hacking the stolen list nearly impossible.

Have several devices – store the list in the cloud !