OPTIMUM PASSWORD PROTECTION - https://howsecureismypassword.net/

To prevent your passwords from being hacked by social engineering, brute force or dictionary attack method, and keep your online accounts safe, you should notice that:

1. Do not use the same password, security question and answer for multiple important accounts.

2. Use a password that has at least 16 characters, use at least one number, one uppercase letter, one lowercase letter and one special symbol.

3. Do not use the names of your families, friends or pets in your passwords.

4. Do not use postcodes, house numbers, phone numbers, birthdates, ID card numbers, social security numbers, and so on in your passwords.

5. Do not use any dictionary word in your passwords. Examples of strong passwords: ePYHc~dS*)8$+V-' , qzRtC{6rXN3N\RgL , zbfUMZPE6`FC%)sZ. Examples of weak passwords: qwert12345, Gbt3fC79ZmMEFUFJ, 1234567890, 987654321, nortonpassword.

6. Do not use two or more similar passwords which most of their characters are same, for example, ilovefreshflowersMac, ilovefreshflowersDropBox, since if one of these passwords is stolen, then it means that all these passwords are stolen.

7. Do not use something that can be cloned (but you can't change) as your passwords, such as your fingerprints.

8. Do not let your Web browsers (Firefox, Chrome, Safari, Opera, IE) to store your passwords, since all passwords saved in Web browsers can be revealed easily.

9. Do not log in to important accounts on the computers of others, or when connected to a public Wi-Fi hotspot, Tor, free VPN or web proxy.

10. Do not send sensitive information online via unencrypted (e.g. HTTP or FTP) connections, because messages in these connections can be sniffed with very little effort. You should use encrypted connections such as HTTPS, SFTP, FTPS, SMTPS, IPSec whenever possible.

11. When travelling, you can encrypt your Internet connections before they leave your laptop, tablet, mobile phone or router. For example, you can set up a private VPN (with MS-CHAP v2 or stronger protocols) on your own server (home computer, dedicated server or VPS) and connect to it. Alternatively, you can set up an encrypted SSH tunnel between your router and your home computer (or a remote server of your own) with PuTTY and connect your programs (e.g. Firefox) to PuTTY. Then even if somebody captures your data as it is transmitted between your device (e.g. laptop, iPhone, iPad) and your server with a packet sniffer, they'll won't be able to steal your data and passwords from the encrypted streaming data.

12. How secure is my password? Perhaps you believe that your passwords are very strong, difficult to hack. But if a hacker has stolen your username and the MD5 hash value of your password from a company's server, and the rainbow table of the hacker contains this MD5 hash, then your password will be cracked quickly.

To check the strength of your passwords and know whether they're inside the popular rainbow tables, you can convert your passwords to MD5 hashes on a MD5 hash generator, then decrypt your passwords by submitting these hashes to an online MD5 decryption service. For instance, your password is "0123456789A", using the brute-force method, it may take a computer almost one year to crack your password, but if you decrypt it by submitting its MD5 hash (C8E7279CD035B23BB9C0F1F954DFF5B3) to a MD5 decryption website, how long will it take to crack it? You can perform the test yourself.

13. It's recommended to change your passwords every 10 weeks.

14. It's recommended that you remember a few master passwords, store other passwords in a plain text file and encrypt this file with 7-Zip, GPG or a disk encryption software such as BitLocker, or manage your passwords with a password management software.

15. Encrypt and backup your passwords to different locations, then if you lost access to your computer or account, you can retrieve your passwords back quickly.

16. Turn on 2-step authentication whenever possible.

17. Do not store your critical passwords in the cloud.

18. Access important websites (e.g. PayPal) from bookmarks directly, otherwise please check its domain name carefully, it's a good idea to check the popularity of a website with Alexa toolbar to ensure that it's not a phishing site before entering your password.

19. Protect your computer with firewall and antivirus software, block all incoming connections and all unnecessary outgoing connections with the firewall. Download software from reputable sites only and verify the MD5 / SHA1 / SHA256 checksum or GPG signature of the installation package whenever possible.

20. Keep the operating systems (e.g. Windows 7, Windows 10, Mac OS X, iOS, Linux) and Web browsers (e.g. Firefox, Chrome, IE, Microsoft Edge) of your devices (e.g. Windows PC, Mac PC, iPhone, iPad, Android tablet) up-to-date by installing the latest security update.

21. If there are important files on your computer, and it can be accessed by others, check if there are hardware keyloggers (e.g. wireless keyboard sniffer), software keyloggers and hidden cameras when you feel it's necessary.

22. If there are WIFI routers in your home, then it's possible to know the passwords you typed (in your neighbor's house) by detecting the gestures of your fingers and hands, since the WIFI signal they received will change when you move your fingers and hands. You can use an on-screen keyboard to type your passwords in such cases, it would be more secure if this virtual keyboard (or soft keyboard) changes layouts every time.

23. Lock your computer and mobile phone when you leave them.

24. Encrypt the entire hard drive with LUKS or similar tools before putting important files on it and destroy the hard drive of your old devices physically if it's necessary.

25. Access important websites in private or incognito mode, or use one Web browser to access important websites, use another one to access other sites. Or access unimportant websites and install new software inside a virtual machine created with VMware, VirtualBox or Parallels.

26. Use at least 3 different email addresses, use the first one to receive emails from important sites and Apps, such as PayPal and Amazon, use the second one to receive emails from unimportant sites and Apps, use the third one(from a different email provider, such as Outlook and Gmail) to receive your password-reset email when the first one(e.g. Yahoo Mail) is hacked.

27. Use at least 2 different phone numbers, do NOT tell others the phone number which you use to receive text messages of the verification codes.

28. Do not click the link in an email or SMS message, do not reset your passwords by clicking them, except that you know these messages are not fake.

29. Do not tell your passwords to anybody in the email.

30. It's possible that one of the software or App you downloaded or updated has been modified by hackers, you can avoid this problem by not installing this software or App at the first time, except that it's published to fix security holes. You can use Web based apps instead, which are more secure and portable.

31. Be careful when using online paste tools and screen capture tools, do not let them to upload your passwords to the cloud.

32. If you're a webmaster, do not store the user’s passwords, security questions and answers as plain text in the database, you should store the salted (SHA1, SHA256 or SHA512) hash values of these strings instead. It's recommended to generate a unique random salt string for each user. In addition, it's a good idea to log the user's device information(e.g. OS version, screen resolution, etc.) and save the salted hash values of them, then when he/she try to login with the correct password but his/her device information does NOT match the previous saved one, let this user to verify his/her identity by entering another verification code sent via SMS or email.

33. If you are a software developer, you should publish the update package signed with a private key using GnuPG and verify the signature of it with the public key published previously.

34. To keep your online business safe, you should register a domain name of your own, and set up an email account with this domain name, then you'll not lose your email account and all your contacts, since you can host your mail server anywhere, your email account can't be disabled by the email provider.

35. If an online shopping site only allows to make payment with credit cards, then you should use a virtual credit card instead.

36. Close your web browser when you leave your computer, otherwise the cookies can be intercepted with a small USB device easily, making it possible to bypass two-step verification and log into your account with stolen cookies on other computers.

37. Distrust and remove bad SSL certificates from your Web browser, otherwise you will NOT be able to ensure the confidentiality and integrity of the HTTPS connections which use these certificates.

38. Below recommended password generator sites with ratings!

☺☺☺☺

https://www.lastpass.com/password-generator

☺☺

https://passwordsgenerator.net/

☺

http://www.freepasswordgenerator.com/

☺

https://www.random.org/passwords/

☺☺☺

https://www.securesafepro.com/pasgen.html

☺☺☺☺☺

https://my.norton.com/extspa/idsafe?path=pwd-gen