Passwords-Advice

Create your own ***secure passwords*** or use this random password generator:
http://passwordsgenerator.net/

Scroll down the above link page for tips on what NOT to do.

Select the length of the password. **12** is a good minimum.

Click on "Generate Secure Password" and **write this down** BEFORE entering it on a new account.
Failure to do so means that you have no record of the password!

A 12 character example, using lowercase and uppercase letters, numbers and special symbols:

Kx47*$"jt98P

Do check the strength of your various existing passwords using HowSecureIsMyPassword?:
https://howsecureismypassword.net/

If they are weak, then strengthen them by making them longer and then ***retest*** them.

IMPORTANT

To prevent your passwords from being hacked by social engineering, brute force or dictionary attack method, you should notice that:
1. Do NOT use the same password for multiple important accounts.
2. Use a password that has at least 12 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.
6. ***Do NOT use something that can be cloned (but you can't change) as your passwords, such as your fingerprints.***
7. Do NOT let your Web browsers (Firefox, Google Chrome, Safari (iPad), Opera, Internet Explorer) store your passwords, since all passwords saved in Web browsers can be revealed easily.
8. 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.

9. Do not send sensitive information online via HTTP or FTP connections, because messages in these connections can be sniffed with very little effort. You should use encrypted connections such as HTTPS and SFTP whenever possible.
10. 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.
11. Turn on 2-step authentication whenever possible.
12. Do NOT store your critical passwords in the Cloud.
13. 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.
14. Protect your computer with firewall and antivirus software, download software from reputable sites only, and verify the MD5 or SHA1 checksum of the installation package whenever possible.