Passphrase Top Tips

Wildern Academy Trust

Tips for Strong & Secure Passwords

USE MORE THAN ONE PASSWORD.

Using the same password on multiple websites will increase the chances of one or all of your accounts being accessed without your permission. It's possible that someone hacking a shopping website could then gain access to your bank or mobile phone accounts....

MAKE THE PASSWORD AT LEAST **12** CHARACTERS LONG.

The longer the better. Longer passwords are harder for thieves to crack.

INCLUDE NUMBERS, CAPITAL LETTERS AND SYMBOLS.

Consider using a $ instead of an S or a 1 instead of an L, or including an & or % – but note that $1ngle is NOT a good password. Password thieves are onto this.

DON'T POST IT IN PLAIN SIGHT.

This might seem obvious but studies have found that a lot of people post their password on their monitor with a sticky note. Bad idea. If you must write it down, hide the note somewhere where no one can find it.

MAKE SURE YOUR DEVICES ARE SECURE.

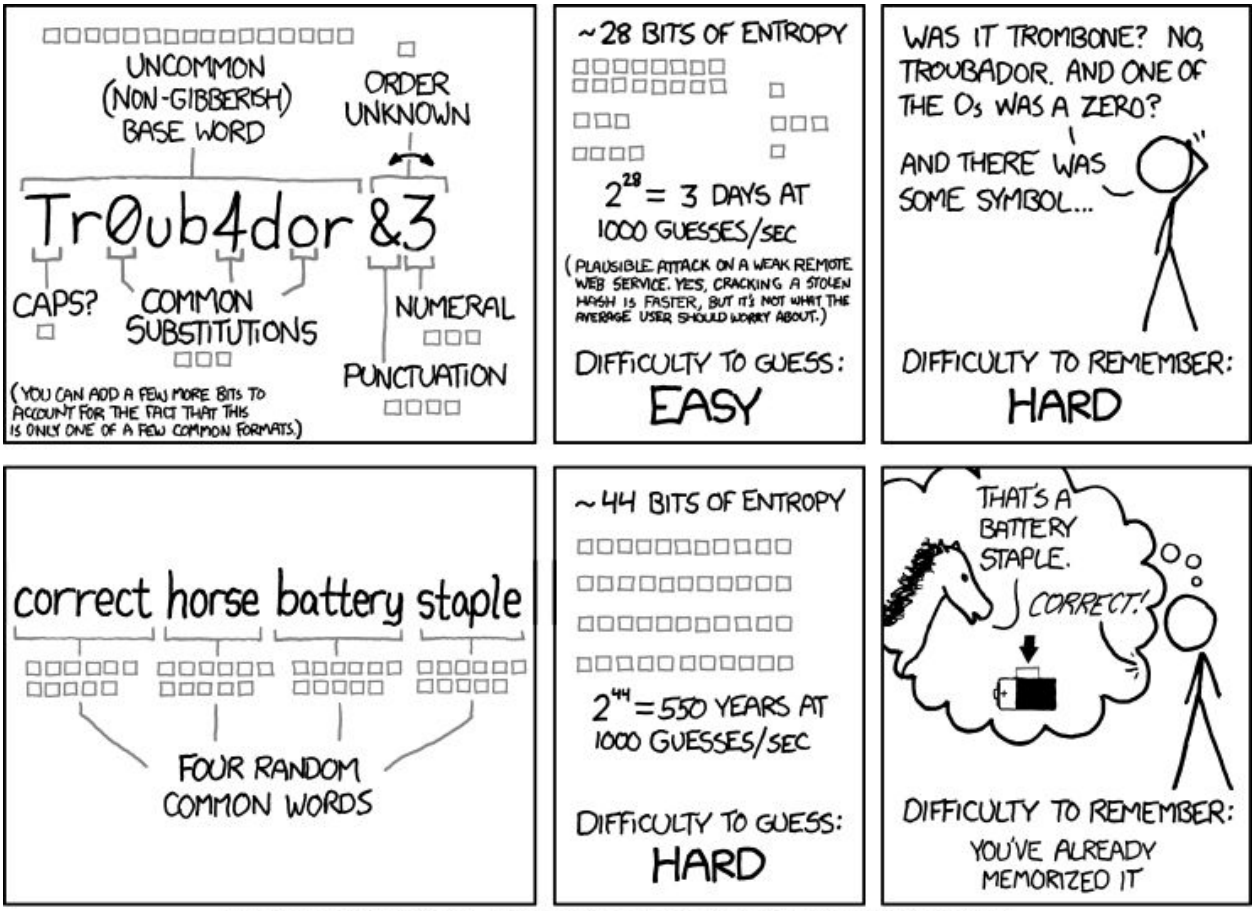
The best password in the world might not do you any good if someone is looking over your shoulder while you type or if you forget to log out on a public computer. Malicious software, including "keyboard loggers" that record all of your keystrokes, has been used to steal passwords and other information. To increase security, make sure you're using up-to-date anti-malware software and that your operating system is up-to-date. If you are unsure on how to best do this feel free to pop into the Genius Bar for support.

NEVER GIVE OUT YOUR PASSWORD TO ANYONE.

Never give it to colleagues, even if they're a trustworthy colleague. A colleague could accidentally pass your password along to others. As a school and as an individual we need to know that passwords are secure at all times once you have shared this information you cannot guarantee where and how it might be used in the future and the different access rights user accounts have on the school systems

USE A PASSPHRASE.

Security experts are now recommending a "passphrase" rather than simply a password. Such a phrase should be relatively long – we recommend between 12-20 characters or so and consist of seemingly random words strung together along with numbers, symbols and upper and lower case letters. Think of something that you can remember but others couldn't guess such as Yellow!Chocolate56Fish£ or Dover!74Sheila?



CONSIDER USING MULTI-FACTOR AUTHENTICATION.

Many services offer an option to verify your identity if someone logs on to your account from an unrecognized device. The typical method is to send a text or other type of message to a mobile device registered to you with a code you need to type in to verify it's really you. In most cases, you will not be required to use this code when logging on from a known device such as your own computer, tablet or phone.

DON'T FALL FOR "PHISHING" ATTACKS.

Be very careful before clicking on a link (even if it appears to be from a legitimate site) asking you to log in, change your password or provide any other personal information. It might be legit or it might be a "phishing" scam where the information you enter goes to a hacker. When in doubt, log on manually by typing what you know to be the site's URL into your browser window. Remember Wildern School **WILL NEVER** ask for password information.