RANSOMWARE	Be aware of so called **Ransomware**, which enters your system through emails or by downloads from infected websites. Once it's installed it encrypts nearly every file on your hard drive, save for those required to operate your PC. You then get a message (often through a pop-up window or webpage) claiming you need to pay a ransom otherwise your files would be deleted forever.
	Ransomware mostly operates using well-known exploits, for which patches usually exist. Religiously apply updates and patches to your operating systems and web browsers, and other software. This includes PCs, Macs and smart devices. Enable automatic software updates if available.
	If you are infected by Ransomware, the best way to recover is to wipe the infected machines and restore them from backups (remember, ALWAYS keep a back up of your important files).
EMAIL	Email remains as the most commonly used by cybercriminals to insert a malware or steal your valuable information. Remember to ignore emails you are unsure about without responding or clicking anything embedded. Also use spam filters and 2-factor/2-steps authentication for your personal emails.