IRON RULES PROTECT ALL OF YOUR DEVICES AND DATA

SOFTWARE DOWNLOADS	**Software downloads** may appear legitimate, but be wary. Take some time and do your research first, and if you no longer need a piece of software, uninstall it. Don't download random plugins or video viewers unless you know the source is legitimate. Use mainstream download sites rather than some forums or sources off the track. Don't try to find free copies of commercial programs – malware could be planted in free software, especially gambling software and simple games. Consider creating an account with limited privileges instead of 'administrator' level account for everyday tasks (many vulnerability exploits are executed with higher access privileges) - you normally only need admin level access for installing new software, changing system configuration etc.
WEB BROWSING	**Browser attacks** use deceptive web pages or links to redirect you to undesired locations, to hijack browsing sessions, to trick your browser into doing things it shouldn't e.g. download (malicious) software, changing your browser settings, divulging your log-in credentials; or, to exploit security flaws in your browser or its plug-ins (such as Flash, Java, Quick Time) to compromise your computer. Ensure your web browsers and plug-ins are up to date. You are encouraged to configure your browser to block plug-ins (particularly adobe flash), scripts, or adware. Or, for flash you could use 'click to play'. Be cautious of any pop-up clicks. Switch on the built-in firewall within your operating system.