POLICE DIGITAL SECURITY CENTRE ADVICE GUIDE

How to secure web browsing

The popularity of web browsing has proven an attractive resource for criminals to spread malware or steal information. Although many reputable web browsers have safeguarding measures in place, businesses should seek to minimise the risk where possible with these tips:

Best Practice

- Make web browsing an activity for only those who need it for their job role
- Do not allow personal web browsing from work devices
- Never allow web browsing from the administrator account
- Do not connect to public Wi-Fi, as sensitive information can be captured by criminals
- Bookmark trusted websites to be confident you are submitting information to a genuine source
- Educate staff to look out for HTTPS (the locked padlock to the left of the search bar)

Technical measures

- Use a web browser that is regularly maintained with updates
- Automatically update the browser, Operating System and plugins/extensions
- Use updated AntiVirus that can scan downloads
- Block popups to avoid clicking on ads that contain malware
- Enable “do not track” to prevent websites from tracking your browsing activity
- Manage Third-Party Cookies where possible to prevent your browsing activity from being tracked by unknown companies
- Use a VPN (Virtual Private Network) to encrypt the information travelling across the network, especially if your staff need to connect to public Wi-Fi
- Use a Password Manager that will automatically fill-in login details for legitimate websites
- Use “Safe Web Search” to block known malicious sites – some web browsers have this integrated, just make sure it is enabled. Many AntiVirus providers offer a plugin
- Use Quad9 to block known malicious sites https://www.policedsc.com/images/PDSC_HOW_TO_SET_UP_QUAD_9.pdf
- Create a Whitelist policy for websites, applications and plugins/extensions to restrict online activity