**References:**

**2 - Incident Management**

* Protective Security Principles Framework​
* Information Security Manual​
* Australian Cyber Security Centre – Cyber Incident Response Plan​
* NIST SP800-61 - Computer Security Incident Handling Guide

**3 - Laptop and PC Hardening**

* [Hardening Microsoft Windows 10 version 21H1 Workstations | Cyber.gov.au](https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-windows-10-version-21h1-workstations)
* [Securing Microsoft Accounts | Cyber.gov.au](https://www.cyber.gov.au/acsc/view-all-content/guidance/securing-microsoft-accounts)

**4 - Mobile Phone Hardening**

* [Securing Instagram | Cyber.gov.au](https://www.cyber.gov.au/acsc/view-all-content/guidance/securing-instagram)
* [Securing Facebook and Facebook Messenger | Cyber.gov.au](https://www.cyber.gov.au/acsc/view-all-content/guidance/securing-facebook-and-facebook-messenger)
* [Securing Signal | Cyber.gov.au](https://www.cyber.gov.au/acsc/view-all-content/guidance/securing-signal)
* [Securing WhatsApp | Cyber.gov.au](https://www.cyber.gov.au/acsc/view-all-content/guidance/securing-whatsapp)
* <https://www.cyber.gov.au/acsc/view-all-content/advice/multi-factor-authentication>
* https://securityintelligence.com/new-mobile-security-threats-malware/
* https://tosdr.org/

**5 - Browser Hardening**

* [ipfingerprints.com](https://www.ipfingerprints.com/)
* [whatsmyua.info/](https://www.whatsmyua.info/)
* [coveryourtracks.eff.org](https://coveryourtracks.eff.org/)
* [clickclickclick.click](https://clickclickclick.click/)
* [amiunque.org](https://www.amiunique.org)

**6 - Social media handling**

* <https://sofrep.com/news/did-a-fitness-app-expose-the-identities-of-sas-operators/>​
* ​[Fugitive John McAfee’s location revealed by photo meta-data screw-up – Naked Security (sophos.com)](https://nakedsecurity.sophos.com/2012/12/03/john-mcafee-location-exif/)

**7 - Cell Tracking**

* [Russian military phone calls hacked after 3G goes offline (yahoo.com)](https://au.news.yahoo.com/russian-military-being-hacked-after-its-own-soldiers-destroy-3-g-internet-towers-104303881.html)​
* [Iran’s Secret Manual for Controlling Protesters’ Mobile Phones (theintercept.com)](https://theintercept.com/2022/10/28/iran-protests-phone-surveillance/)​
* [Police Can’t Keep Records of Electronic Surveillance Secret Indefinitely, EFF Argues to California Supreme Court | Electronic Frontier Foundation](https://www.eff.org/press/releases/police-cant-keep-records-electronic-surveillance-secret-indefinitely-eff-argues)

**9 - Bluetooth Characteristics**

* [Guidelines for Enterprise Mobility - Information Security Manual (https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-enterprise-mobility)](https://www.cyber.gov.au/sites/default/files/2021-12/11.%20ISM%20-%20Guidelines%20for%20Enterprise%20Mobility%20%28December%202021%29.pdf)​
* [NCC Group uncovers Bluetooth Low Energy (BLE) vulnerability that puts millions of cars, mobile devices and locking systems at risk](https://www.mynewsdesk.com/nccgroup/news/ncc-group-uncovers-bluetooth-low-energy-ble-vulnerability-that-puts-millions-of-cars-mobile-devices-and-locking-systems-at-risk-447952)​
* [NIST SP 800-121, Guide to Bluetooth Security](https://www.nist.gov/privacy-framework/nist-sp-800-121)​
* [Bluetooth Basics](https://www.hackers-arise.com/hacking-bluetooth)​
* [BLE Series Part 1: A Brief Overview of Bluetooth Low Energy](https://www.hackers-arise.com/hacking-bluetooth)​
* [Deep Dive into Bluetooth LE Security](https://www.hackers-arise.com/hacking-bluetooth)
* [wired.com/story/tesla-model-x-hack-bluetooth/](www.wired.com/story/tesla-model-x-hack-bluetooth/)