



AUSCERT

CYBER SECURITY FUNDAMENTALS PARTICIPANT CHECKLIST



UQSchoolsNet

Action to Take in the Next Week

Enable 2FA or MFA for your personal email account and any social media. [2fa.directory](#) provides instructions for many sites.

Enable auto updating for all the devices you own. If auto updates are not an option, create a monthly reminder at a time you know you can action it to check for manual updates and apply them.

If you use Chrome, enable [Google Safe Browsing](#). On Firefox, it is part of the inbuilt [phishing and malware protection](#). On Safari, it is part of [privacy and security in Settings](#).

Subscribe to the [SANS OUCH!](#) and the [IDCARE newsletter](#).

Subscribe to the [AUSCERT ADIR](#) (AUSCERT Daily Intelligence Report) - a daily summary of curated infosec news.

Action to Take in the Next Month

Visit the web sites of [ScamWatch](#), the [NCSC](#) and the [eSafety Commissioner](#) to see if they have information of value to you and if so, bookmark them.

Talk to your family members and loved ones, especially young people and older people, about cyber security threats and the differences between online and offline trust. Use the DANCE mnemonic to explain how attackers use social engineering to trick people:

- **D**istracti**D**on - Attackers pull your focus in one direction so you don't notice or think about the thing they want you to miss
- **A**pp**A**pearance - Attackers 'blend in' and appear to be normal and trustworthy - and scam emails look legitimate
- **N**eed - The attack will make you want something and then provide the solution from a position of power or authority

- Context - Attackers prefer places/situations/times of day when you are busy or stressed, and your guard is down
- Emotion - Attackers rely on creating an emotional state such as panic or gratitude in their victim because emotions override rational thinking

Visit the [IDCARE Facebook page](#) and if you find it useful, Like it to receive updates.

Start using a password manager and migrate your accounts into it, changing your password into a random password each time. Start with the most important accounts first.

If you use Chrome's password manager, check the [Google account settings to warn about unsafe \(publicly disclosed\) passwords](#) and for [non-Google accounts](#).

If you use the Keychain password manager, check the [Keychain breach notification settings](#).

Action to Take in the Next 6 Months

If you are interested in behavioural science, check out the Hidden Brain, Making Positive Psychology Work and Choiceology podcasts.

If you are interested in cyber security true crime stories, check out the Darknet Diaries podcast.

Review all the apps installed in mobile devices and uninstall any you don't definitely need.

Resources to get Help in a Cyber Security Emergency

If you think you might be the victim of identify theft or a cyber security attack as an individual: [IDCARE's Cyber First Aid Kit](#).

If you think your organisation has been the victim of a cyber security attack, contact AusCERT:

07 3365 4417

AUSCERT.ORG.AU