DIGITAL TECHNOLOGIES HUB

Australian Curriculum V9.0

Privacy and security

The protection of data when it is stored or transmitted through digital systems.

ACARA, 2022

Years 7–8

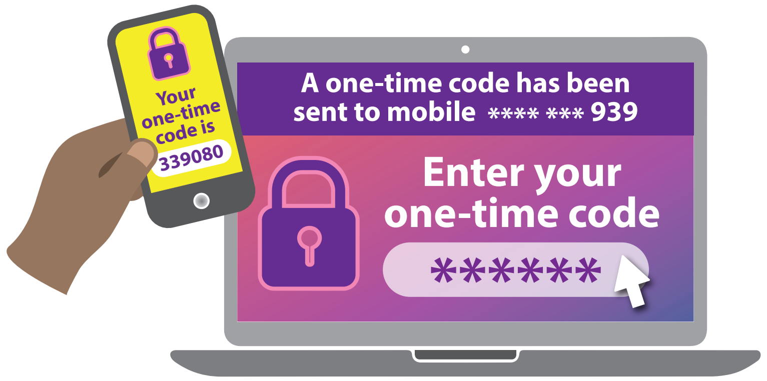
I can explain how multi-factor authentication prevents unauthorised access to online accounts. I can identify common techniques used in phishing scams to exploit susceptible users and I can also review and manage my digital footprint.

Multi-factor authentication prevents unauthorised access to online accounts by requiring additional verification steps beyond just entering a password, such as providing a one-time password or token.

Phishing scams often employ various techniques to identify and exploit susceptible users. One common tactic is the use of email addresses from unofficial domains, creating the illusion of legitimacy, such as pretending to be a well-known online retailer.

A person's online activity contributes to their digital footprint. To manage one's digital footprint, a person should always consider privacy implications and only selectively share content online, and adjust privacy settings on social media to control who sees their content.

Create a poster or infographic that explains various levels of security. Include multi-factor authentication, and describe how it works and its benefits above some other forms of authentication. Include statistics about data protection, such as frequency of password breaches and data leaks, and show the types and levels of security a person can put in place.


Your one-time code is 339080
A one-time code has been sent to mobile **** *** 939
Enter your one-time code
******

Research and create a presentation focusing on strategies for reviewing and managing your digital footprint across online tools. Include examples of media services that track user habits, such as music streaming platforms that curate personalised playlists based on listening habits.

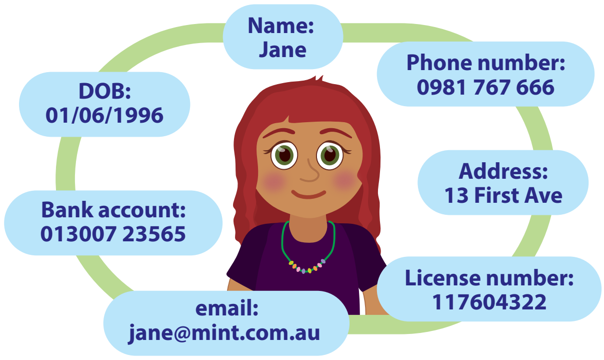
Achievement standard	Students manage their digital footprint.
Content descriptions	Explain how multi-factor authentication protects an account when the password is compromised and identify phishing and other cyber security threats | Digital Technologies AC9TDI8P13 Investigate and manage the digital footprint existing systems and student solutions collect and assess if the data is essential to their purpose | Digital Technologies AC9TDI8P14

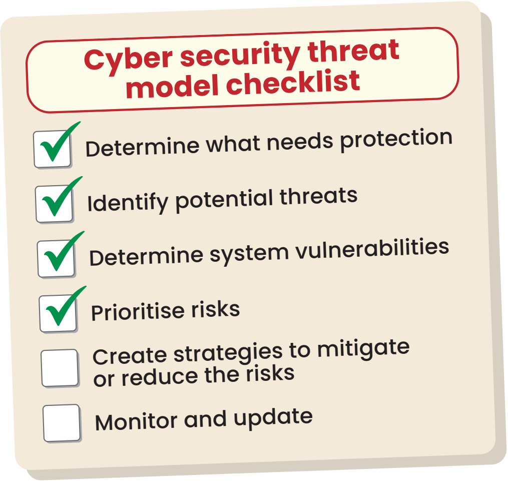
Years 9–10

I can explain how private information moves through a system and identify when it's most vulnerable to a cyber attack. I can use the Australian Privacy Principles to evaluate how well user information is protected in online systems.

Private information is stored and transmitted in a digital system, and its vulnerabilities to cyber attacks can be identified by understanding the flow of this information.

The Australian Privacy Principles are a set of principles that regulate how Australian government agencies and some private sector organisations handle, use and manage personal data. They are designed to protect individuals' privacy rights by setting standards for the collection, use and disclosure of personal data.


Name: Jane
Phone number: 0981 767 666
DOB: 01/06/1996
Address: 13 First Ave
Bank account: 013007 23565
License number: 117604322
email: jane@mint.com.au

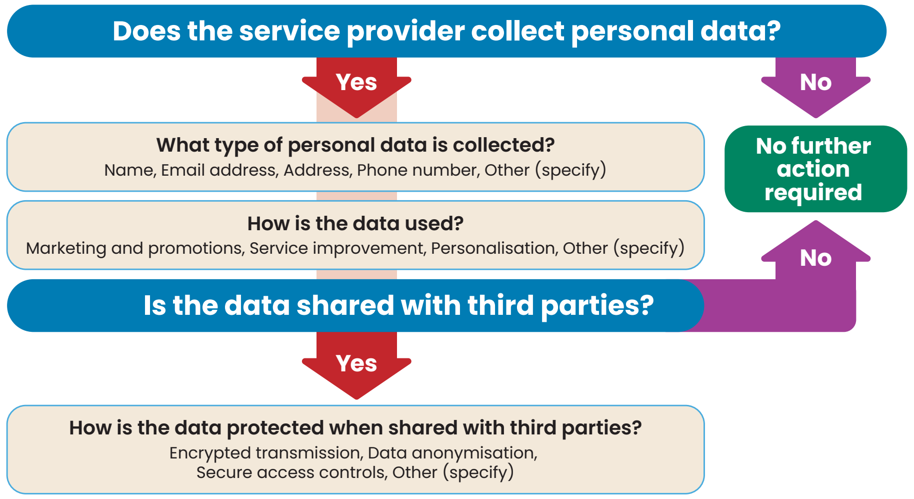


Cyber security threat model checklist

- ☑ Determine what needs protection
- ☑ Identify potential threats
- ☑ Determine system vulnerabilities
- ☑ Prioritise risks
- □ Create strategies to mitigate or reduce the risks
- □ Monitor and update

Analyse scenarios to identify assets (such as personal information), threats (such as phishing) and vulnerabilities (such as weak passwords) using the cyber security threat model. Propose mitigation strategies (for example, multi-factor authentication) to protect against these threats.

Create a privacy audit toolkit for apps and websites, inspired by the Australian Privacy Principles. Design interactive elements like quizzes or decision trees to help users understand how their data is handled and suggest improvements.



Does the service provider collect personal data?

Yes

What type of personal data is collected?
Name, Email address, Address, Phone number, Other (specify)

How is the data used?
Marketing and promotions, Service improvement, Personalisation, Other (specify)

Is the data shared with third parties?

Yes

How is the data protected when shared with third parties?
Encrypted transmission, Data anonymisation, Secure access controls, Other (specify)

No

No further action required

Achievement standard	Students apply privacy principles to manage digital footprints.
Content descriptions	Develop cyber security threat models, and explore a software, user or software supply chain vulnerability | Digital Technologies AC9TDI6P09 Apply the Australian Privacy Principles to critique and manage the digital footprint that existing systems and student solutions collect | Digital Technologies AC9TDI6P10

Find more resources at www.dthub.edu.au