DIGITAL TECHNOLOGIES HUB

Australian Curriculum V9.0

Digital systems

Processing data in binary, made up of hardware, controlled by software, and connected to form networks.

ACARA, 2022

Years 7–8

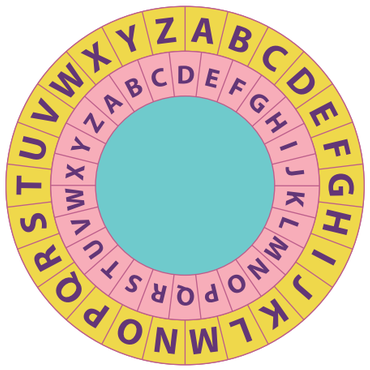
I can select appropriate hardware for particular tasks, explain how data is transmitted and secured in networks, and identify cyber security threats.

Just as computer hardware components have pros and cons depending on requirements, the performance of physical networks (wired and wireless) can also be compared. Network protocols are used to ensure data is transmitted correctly from one device to another.

Digital systems are vulnerable to various cyber threats, such as phishing and ransomware. Threats can be mitigated through techniques such as email filtering and multi-factor authentication (which enhances the security of passwords).

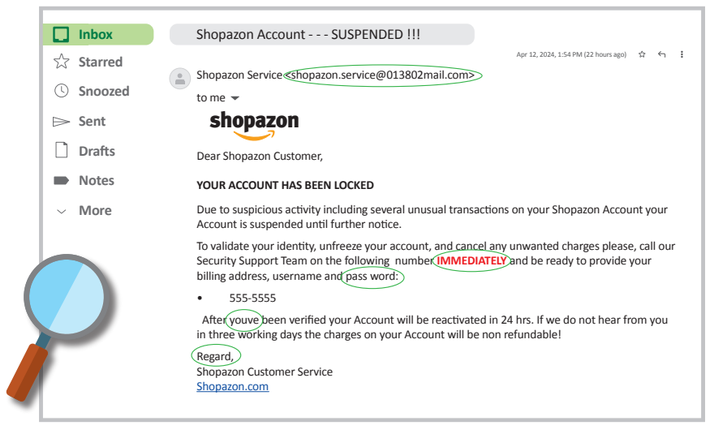
Compare physical networks (wired and wireless) to the ancient networks related to First Nations Peoples' trading practices throughout history, including trade routes.

Computer network	Ancient trade routes
Cables and connections	Paths or trails that connected different trading locations
Routers	Key points along trade routes where decisions were made about which path to take
Protocols (for example, TCP/IP)	Rules and customs that governed trade along the routes



Use interactives and other online resources to practise performing encryption and decryption using custom online tools.

Analyse common phishing scams, gaining a deeper understanding of the techniques used by scammers. Develop rules for AI algorithms to detect these scams, promoting critical thinking about cybersecurity and online safety.



Achievement standard	Students select appropriate hardware for particular tasks, explain how data is transmitted and secured in networks, and identify cyber security threats.
Content descriptions	Explain how hardware specifications affect performance and select appropriate hardware for particular tasks and workloads | Digital Technologies AC9TDI8K01 Investigate how data is transmitted and secured in wired and wireless networks including the internet | Digital Technologies AC9TDI8K02

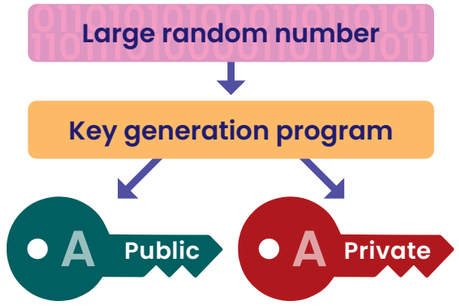
Years 9–10

I can explain how various protocols and systems are used to manage, control and secure access to data. I can model cyber security threats and explore a vulnerability.

Internet hardware and software use various protocols and systems to ensure data is correctly delivered from one digital system to another across local networks and across the world.

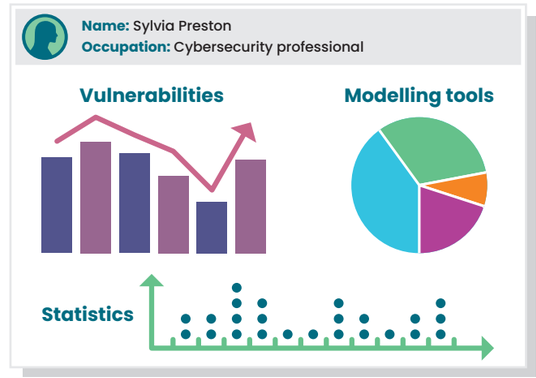
Encryption techniques make data less readable – and therefore less accessible – so that it can be transmitted more securely across a network and decrypted at its destination.

Create an interactive workshop where students role-play different user roles, demonstrating access control elements like authentication and permissions. For example, demonstrate role-based access to illustrate the necessity of restricting software installation access to administrators only.



Investigate cryptography and modern encryption methods for transmitting digital data securely. Encryption of data is a means of protecting data, one example being the use of secret and public keys. Students encode and decode a message creating a public key, an encryption key and a private key.

Create an infographic about the role of a cybersecurity professional. Include statistics on cybersecurity importance, threat frequency, impact, and the growing demand for professionals. Illustrate the use of modelling tools such as threat modelling software to identify and assess risks. Include network vulnerabilities like brute force attacks and malware.



Achievement standard	Students explain how digital systems manage, control and secure access to data; and model cyber security threats and explore a vulnerability.
Content descriptions	Investigate how hardware and software manage, control and secure access to data in networked digital systems | Digital Technologies AC9TDI10K01