# 

# The Cyber Security Learning Experience

28/11/2022

Table of Contents

[The Cyber Security Learning Experience 1](#_Toc120553612)

[iSTEM Stage 5 Specialised Topic – Cyber Security 3](#_Toc120553613)

[Duration of learning 3](#_Toc120553614)

[Outcomes Experienced 4](#_Toc120553615)

[Resources 4](#_Toc120553616)

[Learning Sequence 4](#_Toc120553617)

[Week 1, Cyber Security Fundamentals. Topics: Value of Data, Ethics, Privacy 6](#_Toc120553618)

[Week 2, Protecting Data. Topics: Goals & Framework, Access Controls, Encryption 11](#_Toc120553619)

[Week 3, Protecting Data. Topics: Authentication, Threats, Vulnerabilities & Risks 16](#_Toc120553620)

[Week 4, Networks. Topics: Targets and Hackers, Networks, Tools 20](#_Toc120553621)

[Week 5, The SMART City, Topics: The SMART City, Critical Infrastructure- The Communications Satellite 22](#_Toc120553622)

[Week 6, Communication Satellite, Topics: Flying the Satellite, Cyber Security Vulnerabilities, Analysing Information and Data 24](#_Toc120553623)

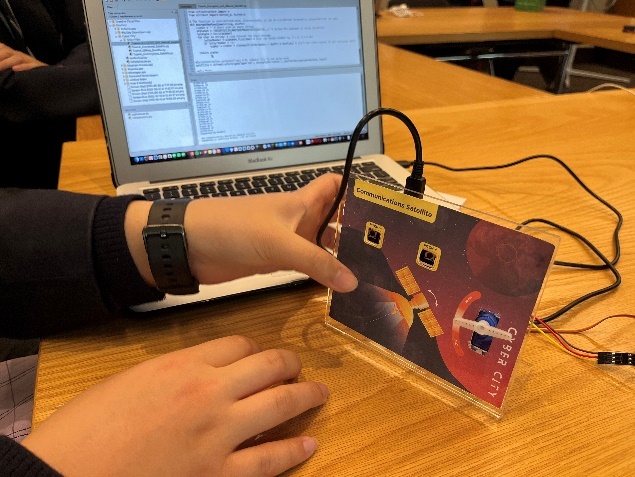
[Week 8, Assessment Preparation: SMART City Infrastructure - Innovation and Entrepreneurial Activity 31](#_Toc120553624)

[Week 9, Assesement Presentparation: Managing Cyber Risk 32](#_Toc120553625)

[Week 10, Assesement Presentation 33](#_Toc120553626)

[Evaluation of Course 34](#_Toc120553627)

# iSTEM Stage 5 Specialised Topic – Cyber Security

MCB Business Partners and Core Electronics, supported by teachers, the government, and the cyber security industry, have partnered to create a best-in-class cyber security learning experience. The Cyber City learning experience supports the new focus on cyber security and digital technologies in the new Australian curriculum. It has been specifically designed to help the new cyber security, a specialised topic in the iSTEM NSW Department of Education Approved Elective.

Cyber City is a complete, industry-aligned set of pedagogical resources and methods to support teachers introducing inquiry-led, cyber security and digital innovation concepts in the classroom. The learning program integrates diverse concepts from the hardware and networking level up to programming and the design and testing of the smart city systems while enabling students to also develop general capabilities in the Australian curriculum in areas such as systems thinking, design thinking, critical thinking and ethical understanding.

In this specialised topic, students develop skills and knowledge used in the cyber security professions by completing inquiry-based and problem-based learning tasks. Students engage with the cyber security industry and will gain insight into the nature of the profession and career pathways.

# Duration of learning

Indicative time – 25 hours

# Outcomes Experienced

* **ST5-1** designs and develops creative, innovative, and enterprising solutions to a wide range of STEM-based problems
* **ST5-2** demonstrates critical thinking, creativity, problem-solving, entrepreneurship and engineering design skills and decision-making techniques in a range of STEM contexts
* **ST5-4** works independently and collaboratively to produce practical solutions to real-world scenarios
* **ST5-5** analyses a range of contexts and applies STEM principles and processes
* **ST5-6** selects and safely uses a range of technologies in the development, evaluation, and presentation of solutions to STEM-based problems
* **ST5-8** uses a range of techniques and technologies to communicate design solutions and technical information for a range of audiences
* **ST5-10** analyses and evaluates the impact of STEM on society and describes the scope and pathways into employment.

Outcomes referred to in this document are from iSTEM Stage 5 course document © NSW Department of Education.

# Resources

Resources for delivering Cyber City, the Cyber Security Learning Experience, can be found on the program website: https://cybercity.education

# Learning Sequence

This sample learning sequence has been prepared by the Cyber City learning design team. It has been developed as a guide for teachers to assist in the development of a teaching and learning program contextualised to an individual school's needs.

The scope and depth of the content covered should relate to the school's context, the expertise of the teacher(s) delivering the course and the prior knowledge of the students. Teachers are invited to make adjustments to the program during its implementation in order to meet the individual needs of students and to allow for the differentiation of the iSTEM curriculum.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Teachers name: | | | Course Duration: | | |
| Quality Teaching Framework | | | Cross Curriculum Activities | | |
| **Intellectual Quality**   * Deep Knowledge * Deep Understanding * Problematic Knowledge * Higher order Thinking * Metalanguage * Substantive Communitcation | **Quality Learning Environment**   * Explicit quality Criteria * Engagement * Self Regulation * Self Direction * High Expectations | **Significance**   * Narrative * Cultural Knowledge * Background Knowledge * Inclusivity * Connectedness * Knowledge Integration | **ICT**   * Moodle * Internet * Pod Cast * Laptop/Computer * CAD * IWB   ……………………… | **Key Competencies**   * Collecting * Analysing * Organising * Communicating ideas * Planning * Working with others * Working mathematically * Problem solving | **Bloom Level/Verb examples**   * Design: Create/Propose/Predict * Evaluate: Assess/Justify/Argue * Analyse: Debate/Differentiate * Apply: Solve/Demonstrate * Understand: Discuss/Outline * Remember: Define/List/State |

## Week 1, Cyber Security Fundamentals. Topics: Value of Data, Ethics, Privacy

Outcomes: ST5-4, ST5-5, ST5-10

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Topic | Content | Teaching Strategies | Resources | Registration |
| Value of Data | * describe basic concepts of cyber security. * describe their online identity, profile and data, and the need to protect it, for example:   + personal data and photos, medical data, financial data, * develop an understanding of the cyber security industry. * investigate the nature of work and the pathways into the cyber security profession, for example:   + security software developer, computer forensics, penetration tester, systems administrator, cyber incident responder, cyber risk management, the cyber psychologist, security and privacy software engineer, cyber security awareness trainer, cyber intelligence officer and cyberwar analyst | Video:   * + - Introduction to cyber security     - What is Cyber Security?     - Careers in Cyber Security     - Why is it important?     - Whom does cyber security affect?     - Introducing the terms of cyber security, and information security   Work booklet:   * + - Introduction close activity of cyber security terms. Mix and match terms to definitions activity to address common terms to be learnt in the course     - What is the difference between data and information? Brainstorm on graphic layout page from whiteboard (class discussion)     - Research explicit definitions of each are formed with examples   Whole class discussion/teacher's guide:   * + - What is data, and how is it considered valuable?     - This question is explored through the three scenarios listed in the booklet. Break class into three groups to explore each scenario and scribe onto a mind map (butcher's paper/whiteboard/collab space).   Work booklet & PowerPoint Presentation:   * + - What makes data valuable?     - Value in data, Value from data, and value of data Do these three statements mean the same thing? Why/Why not?     - How does data have different values in different contexts?     - How does this change human behaviour to the items of value? | * + - Video 1.1.1     - Video 1.1.2     - Student Work booklet     - Teacher's Handbook     - Teacher's PowerPoint Aid |  |
| Ethics | * distinguish between ethical and unethical behaviour. * identify legal and ethical issues related to personal and organisational cyber security and evaluate the impact on stakeholders, including consumers, organisations and government, for example:   + safety, digital identities, cyber hygiene, embarrassment, personal data, financial loss, reputational damage, misinformation/disinformation campaigns, critical infrastructure. | Video:   * + - Introduction to Ethics     - What is ethics?     - What is the difference between ethics and morals     - What is the relationship between ethics and morals     - What is the difference between legal/illegal and ethical/non-ethical?   Work booklet:   * + - Using the knowledge from the video, scribe with a partner the behaviours that would be considered ethical and non-ethical in the scenarios listed     - Students are to identify the different parties in the scenario and justify their point on what they considered as ethical and unethical behaviour in one of the scenarios.     - Were any illegal actions/behaviours present in scenarios? If not, what factors could make these scenarios illegal?   Think pair share:   * + - Students in pairs evaluate the value of ethics in cyber security in the context of individuals, organisations and government, pairs share their view with the class with reasoning   Whole class discussion:  How does ethical behaviour influenced by ownership or value of the data? Brainstorm on whiteboard topic questions of   * + - "If something has value how do we respond differently?"     - "If something does not have value how do we behave?"   Work booklet:  A real-life scenario regarding a person who is an employee of a company and has taken a photo advertising the company on their personal social media, and the company has asked for the employee to take it down following questions of   * + - Who owns the data?     - Who has the ethical responsibility to protect it?     - Is the behaviour of each party fair and ethical? | * + - Video 1.2.1     - Student Work booklet     - Teacher's Handbook     - Teacher's PowerPoint Aid |  |
| Privacy | * describe the interrelationship between confidentiality, integrity and availability (CIA triad) and how it underpins privacy. | Video: Mindreader video  Work booklet:  Using the knowledge from the video,   * + - What data should be private?     - After watching the video, do you still think your previous data types should remain private, more? Less?   What are the meanings of these terms (Worksheet with matching term to definition activity)   * + - privacy     - confidentiality     - disclosure     - anonymity     - security     - private information     - public information     - personally identifiable information (PII)     - persona (optional)     - identity theft.   Work-booklet:  Small Group Work:   * + - What is the relationship between Privacy and Confidentiality?     - Privacy and Anonymity?     - PII and social identity?   Each group brainstorms concepts on butcher's paper and will rotate the three brainstorms between the three groups. Class discussion is suggested to consolidate efforts. Scribe in booklet  Individual Work:   * + - What are the issues with publishing private information?     - Modelled as a template of a social media page. Students fill the page out, selecting their personal interpretation of what is suitable to post.   Think Pair Share:   * + - Students used their mock social media pages to evaluate each other's,     - Students discuss the choices they have made and their reasoning eg. Passing round booklets)     - What are issues related to privacy presented in the scenarios (Same as ethical scenarios, but in terms of privacy)?     - Is there a violation of privacy?   Extension - Think Pair Share:   * + - Pairs decide from the scenario who is responsible for maintaining privacy in each scenario and provide solutions to protecting privacy and confidentiality in a future potential occurrence.     - Pairs present their idea and reasoning to the class | * + - Video 1.3.1     - Student Work booklet     - Teacher's Handbook     - Teacher's PowerPoint Aid |  |

## Week 2, Protecting Data. Topics: Goals & Framework, Access Controls, Encryption

Outcomes: ST5-4, ST5-5, ST5-10

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Topic | Content | Teaching Strategies | Resourses | Registration |
| Goals & Framework | * describe the interrelationship between confidentiality, integrity and availability (CIA triad) and how it underpins privacy. * identify cyber security approaches, for example:   + risk assessment, people, physical access, policies and technology. | Video:   * + - Introduction to the CIA triad     - Outlining the information security model security professionals and organisations use to develop policies and procedures to protect information and systems     - examples of how each component is important to the model and its relationship with other models   PowerPoint Presentation Prompt & Work booklet:   * + - What are the goals of information security?     - What is the importance of maintaining these goals, such as Protecting data/information and managing risk.     - Consolidating CIA with close activity, where students are to define the components   Whole class discussion/Workbooklet/Teacher's guide:   * + - Whole class contributes to mind map taking in turns with whiteboard markers to write answers to the question of 'How data can be protected?'     - Three coloured markers to be used to distinguish which answer is answering how data is protected in a virtual space? Physical space? Or both?   Video:   * + - Introduction to security controls     - Addressing what security controls are used to enhance confidentiality, why they are important     - What they are (Access controls and Encryption)?     - What is the relationship between the security controls and the NIST Cybersecurity and the five areas, where does the security controls fit in the five steps. | * + - Video 2.1.1     - Student Work booklet     - Teacher's Handbook     - Teacher's PowerPoint Aid |  |
| Access Controls | * identify tools, controls and technologies commonly used to protect people and organisations from a cyber-attack, for example:   + training, cyber incident response plans and practice, firewalls, antivirus software, wireless security, browser security, automatic updates, email security, sandboxing, multi-factor authentication, Essential Eight Maturity Model. | Video:   * + - Introduction to Access Controls     - What are access controls?     - What types of access controls are there?     - What are the implementations of each access control type?     - What are the advantages and disadvantages of access controls?     - What are some examples of why they may be used?   PowerPoint Presentation Prompt & Work booklet:   * + - What is Identification?     - What is Authentication?     - What is Authorisation?     - Address how each of these access controls can be used in an organisation, provide modern examples (through individual research) of organisations and/or their products that have incorporated these techniques.     - the advantages and disadvantages of restricting access to others regarding viewing of data.   Whole class discussion/Workbooklet/Teacher's guide:   * + - Small Group Work:     - What is the most appropriate access control type?     - With reasoning for each of the scenarios listed.     - Students will scribe their access control type and why, their reasoning of how staff numbers or different facilities may affect access controls and potential customisation solutions to staff/faculties they think is appropriate to possess x data (choose one data type, to allow other groups to have different contributions).     - Each group brainstorms concepts on butcher's paper and will rotate the three brainstorms between the three groups. | * + - Video 2.2.1     - Student Work booklet     - Teacher's Handbook     - Teacher's PowerPoint Aid |  |
| Encryption |  | PowerPoint Presentation Prompt & Work booklet:   * + - What is encryption? What is its roles within cyber security for:     - providing confidentiality     - guarding stored data on devices     - protecting transactions     - securing network communications     - Is there any other roles encryption possesses in relation to cyber security?   Whole class discussion/Workbooklet/Teacher's guide:  Discuss the use of encryption for scenarios listed,   * + - how does encryption keep the data safe?     - What data is being protected?     - Why is the data valuable to other parties that aren't the owners?     - Are other parties involved?   Video:   * + - Introduction to Encryption     - What is encryption     - The difference between asymmetric and symmetric encryption     - Why is data encryption necessary to organisations?     - Types of encryption methods     - Why different types are most appropriate for organisations   Workbooklet:   * + - Research activity: Students use technology to research an organisation and the type of data they store, with reasoning they must write notes what type of encryption would be most appropriate for the organisation's data. Teacher may ask students to present their examples.     - List the advantages and disadvantages table of different encryption methods, e.g., VPN. Brainstorm on whiteboard |  |  |

## Week 3, Protecting Data. Topics: Authentication, Threats, Vulnerabilities & Risks

Outcomes: ST5-4, ST5-5, ST5-10

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Topic | Content | Teaching Strategies | Resources | Registration |
| Authentication |  | Video:   * + - Introduction to Authentification     - What is authentication?     - What are some examples of authentication?     - What is two-factor authentication?     - What are the advantages and disadvantages of each type of authentication?   Work booklet:  Research activity:   * + - Students use technology to research modern examples of an authentication type and write notes on     - how it works?     - What is the method?     - Examples of who may use it?     - Modern examples of it being used.     - Students may be asked to present the authentication process they investigated.   Whole class discussion/Workbooklet/Teacher's guide:   * + - Demonstration:     - Teacher may download an authenticator app and provide a walk-through demo, detailing each step of using the app and asking students what steps allow this app to be two-factor authentication rather than just authentication   Whole class discussion:   * + - Advantages and disadvantages of organisations using the two-factor authentication apps in the workplace. Brainstorm on a whiteboard. | * + - Video 3.1.1     - Student Work booklet     - Teacher's Handbook     - Teacher's PowerPoint Aid |  |
| Threats | * analyse types of cyber security threats and how they are used to attack organisations, individuals, computer systems and networks, for example:   + phishing, social engineering, malware, ransomware, denial-of-service (DoS) attacks, person in the middle, business email compromise (BEC), password harvesting, and software vulnerabilities. | Video:   * + - Introduction to Threats     - What is a threat in relation to cyber security?     - How does cyber security affect the event of a threat?   Whole class discussion/Workbooklet/Teacher's guide:   * + - Whole class discussion:     - Demonstrate the similarities between security and physical security in the metaphor of a physical house and protecting your contents with locked doors and windows, alarms etc.     - Students are given a worksheet with a house with doors, windows, and alarms and must label each household factor with a cyber security factor to eliminate the event of threat.   Work booklet & PowerPoint prompt:   * + - How do protection levels affect the vulnerability of losing security?     - Pair the correct threat with its meaning with match-up activity     - Are threats always visible?     - Can they be avoided or controlled? | * + - Video 3.2.1     - Student Work booklet     - Teacher's Handbook     - Teacher's PowerPoint Aid |  |
| Vulnerabilities & Risks | * develop and demonstrate an understanding of the importance of secure coding approaches, for example:   + shift left, baked-in security, testing, and version control. * explain how hardware technologies are targeted and exploited in a cyber-attack, for example:   + servers, laptops, desktop computers, tablets and smartphones, routers, networks, the cloud, and Internet of Things (IoT) devices. * explain how software applications are targeted and exploited in a cyber-attack, for example:   + websites, email, operating systems, browsers, embedded software. | * + - Video:     - Introduction Vulnerabilities & Risks     - What is a Vulnerability in a cyber security context?     - What is a Risk in a cyber security context?     - What types of vulnerabilities are there?     - What vulnerabilities may be tried to be exploited?     - What can happen when a threat successfully exploits a vulnerability?     - What is vulnerability's effect on inflicting higher risk     - What is the potential impact cyber security vulnerability presents in an organisation   Work booklet:   * + - Research activity: Students use technology to research modern examples of breaches, including but not limited to:     - Linked in breach     - Yahoo breach     - Facebook breach     - Evaluate the impact of the cyber security breach     - Why was the organisation a target?     - How could the company minimise vulnerabilities?     - Can vulnerabilities be controlled?     - Are third parties affected by a breach and discuss the impacts for the organisation and third parties. | * + - Video 3.3.1     - Student Work booklet     - Teacher's Handbook     - Teacher's PowerPoint Aid |  |

## Week 4, Networks. Topics: Targets and Hackers, Networks, Tools

Outcomes: ST5-4, ST5-5, ST5-10

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Topic | Content | Teaching Strategies | Resources | Registration |
| Targets & Hackers | * explain the motives of different types of hackers, for example:   + white, grey and black hats, organised cyber criminals, cyber espionage, hacktivists, terrorists, and state sponsored actors. * explain how critical infrastructure is targeted and exploited in a cyber-attack. | Video:   * + - Introduction to Targets and Hackers     - What is a target?     - What is a hacker?   What types of hackers are there?  Whole class Discussion & Work booklet:   * + - Whole class discussion:     - Demonstrate the differences between black and white hat hackers     - How does ethics play a role in these types?   Work Booklet:   * + - What is the purpose of hacking data?     - Why is data valuable in different contexts?     - Why may vulnerabilities affect an individual group from becoming a target? | * + - Video 4.1.1     - Student Work booklet     - Teacher's Handbook     - Teacher's PowerPoint Aid |  |
| Networks | * describe how software and hardware communicate across a network, for example:   + protocols, devices, applications and OSI model. | Video:   * + - Introduction to Networks     - What is a network?     - Why are networks important?     - What are real-life examples of networks at work?   Whole class Discussion & Work booklet:   * + - What are network topologies?     - What are the types of topologies     - What are the designs of each topology     - What are the benefits and disadvantages of each topology   Work Booklet:   * + - What are network operating systems, and what is their importance in establishing cyber security?     - The advantages and disadvantages of establishing a network | * + - Video 4.2.1     - Student Work booklet     - Teacher's Handbook     - Teacher's PowerPoint Aid |  |
| Tools |  | Video   * + - Introduction to Cyber Security tools     - What is the use of security mechanisms and tools to protect systems?     - What is cryptography?     - What are the advantages and disadvantages of these tools?   Work Booklet   * + - What is an algorithm?     - What are the essential elements required for these types of encryption | * + - Video 4.3.1     - Student Work booklet     - Teacher's Handbook     - Teacher's PowerPoint Aid |  |

## Week 5, The SMART City, Topics: The SMART City, Critical Infrastructure- The Communications Satellite

Outcomes: ST5-4, ST5-5, ST5-10

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Topic | Content | Teaching Strategies | Resources | Registration |
| The SMART City |  | Video   * + - Welcome to Cyber City     - The Future Cities and Places - The Smart City / Place     - How does a Smart City connect - What is its network?     - Who designs a Smart City or Place     - How do we make a SMART City work (IoT)     - What are the cyber security threats?   Video: Demonstration   * + - Demonstrate the code to be entered by students     - Describe the code's relationship with each micro:bit sensor/output     - Discuss the code's purpose of the hardware   Individual task / Work booklet   * + - Follow the steps from the video in screenshot form to create a visual method for students to follow the exercise | * + - Video 5.1.1     - Video 5.1.2     - Student Work booklet     - Teacher's Handbook     - Teacher's PowerPoint Aid     - Smart City Kit     - Computers |  |
| Critical Infrastructure – The Communications Satellite | * complete practical exercises solving cyber security problems. * describe the contributions that cyber security professionals make to society. * engage in industry career development opportunities to gain a deeper knowledge of cyber security professions, develop skills, knowledge and understanding of authentic, real-world problem-solving, for example: * ambassador programs, mentors, work experience, micro-credentialing courses, excursions, industry groups, site visits, exhibitions, and competitions. | Video:   * + - Presents industry experts that explain     - Their company     - Their role     - Why is their role important?     - Why is their role crucial to infrastructure?     - What is a satellite?     - What is the cost of a satellite?     - How does a satellite work?   Why is maintenance essential?  Whole class brainstorm:   * + - Creating hypothesis of control outcomes and proposing control strategies   PowerPoint presentation:   * + - Outlining the rules and roles of the game     - Demonstrate with screenshots of, the appropriate code needed to control the infrastructure and control mechanisms relevant to completing the set task   Worksheet:   * + - Code with errors, to be identified by students, to be fixed and maintain the infrastructure | * + - Video 5.2.1     - Video 5.2.2     - Student Work booklet     - Teacher's Handbook     - Teacher's PowerPoint Aid     - Smart City Kit     - Computers |  |

## Week 6, Communication Satellite, Topics: Flying the Satellite, Cyber Security Vulnerabilities, Analysing Information and Data

Outcomes: ST5-1, ST5-2, ST5-6, ST5-8

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Topic | Content | Teaching Strategies | Resources | Registration |
| Flying the Satellite |  | Video   * + - Introduction to Satellites     - What is a satellite?     - What services does a satellite provide to the community, business, and government?     - What do Future satellite services look like?     - What may happen if a satellite is under cyber security breach?   Video- Outlining.   * + - Teacher/Industry Expert motivates the need for encryption     - Commands + state data are plaintext and so extremely vulnerable to interception/injection     - The issues of becoming vulnerable in cyber security     - Can we minimise vulnerabilities? If so, how?     - What is a cipher? Introduce cipher concepts and perform encryption/decryption with cipher exercises.     - Workbook cont. (Ciphers)     - Link to Cipher:     - Encrypt + decrypt messages using a Caesar cipher     - Caesar cipher blurb information for context     - Exercises that will allow students to solve and create their own ciphers     - Answer questions regarding Caesar cipher's vulnerabilities     - Encrypt + decrypt messages using a cipher wheel     - Identify the (plaintext) vulnerability and consequences e.g. Data interception – espionage, command injection – infrastructure disabled. | * + - Video 6.1.1     - Video 6.1.2     - Video 5.2.1     - Video 5.3.1     - Video 5.3.2     - Video 5.3.3     - Student Work booklet     - Teacher's Handbook     - Teacher's PowerPoint Aid     - Smart City Kit   Computers |  |
| Cyber Security Vulnerabilities | * apply encryption to secure data, for example:   + TLS, SSL, secure VPN, secure messaging, hash-based checksums. | Video:   * + - Why test for vulnerabilities in our networks and infrastructure     - How do we use this information to protect our networks and infrastructure?   Content   * + - Introduce subversion techniques eg. Social engineering, password reuse, and phishing.     - Introduce strategies to minimise risk (password management, https, certificates)   Exercises   * + - Research examples of subversion techniques and create a glossary of terms with their purpose     - Research strategies to minimise risk and create a glossary of terms with their purpose   Video – Demonstration   * + - Facilitate deploying the cipher in MicroPython.     - Demonstrate to students the micro python needed to fulfil the action of     - Deploy the Caesar cipher on the micro:bit (abstracted)     - Decrypt with a 'stolen' key eg. Obtained by social engineering, key reuse. Discuss these vulnerabilities   Workbook cont. (Ciphers)   * + - Students use the resource in the workbook and follow the method sheet to allow students to, step by step, Decrypt with a 'stolen' key e.g. Obtained by social engineering, key reuse.     - After students complete the reflection question 'Discuss these vulnerabilities' below | * + - Video 6.2.1     - Video 6.2.2     - Student Work booklet     - Teacher's Handbook     - Teacher's PowerPoint Aid     - Smart City Kit     - Computers |  |
| Analysing Information and Data |  | Video   * + - What role do analysts and communication specialists play in cyber security?     - How do you look at and interpret data?   Content   * + - Introduce codebreaking techniques eg. Brute-force and dictionary attack. Facilitate codebreaking by outlining a brute-force attack strategy   Exercises   * + - Research examples of codebreaking techniques and create a glossary of terms with their purpose   Video: Demonstration   * + - Demonstration of an Interception and perform a brute-force attack on encrypted data (26 possible keys, look through decrypted messages for human-readable messages.)     - Use this obtained key to decrypt all further messages and subvert infrastructure by eg. disabling it.     - Students use this demonstration to answer the workbooks questions   Workbook cont.   * + - What is a brute-force attack strategy?     - Facilitate codebreaking by outlining a brute-force attack strategy: try a key, show the result, and repeat for all 26 keys.     - What is a naïve attack?     - How is this relevant to a brute-force attack strategy?     - Discuss the weakness of this cipher? | * + - Video 6.3.1     - Video 6.3.2     - Student Work booklet     - Teacher's Handbook     - Teacher's PowerPoint Aid     - Smart City Kit     - Computers |  |

Week 7,Cyber Security Mitigation Strategies**,** Topics:Cyber City Satellite Communication

Outcomes: ST5-1, ST5-2, ST5-6, ST5-8, ST5-10

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Topic | Content | Teaching Strategies | Resources | Registration |
| Cyber Security Mitigation Strategies | * use security mechanisms and tools to protect systems, for example:   + end points, antivirus software, backups, firewalls, password safes, multi-factor authentication, patching and applying security updates. | Video   * + - Introduction to Mitigation     - What is mitigation?     - What security mechanisms and tools can protect systems?     - What is a cipher?   Video   * + - Outlining What is the concept of 'rotating key' encryption     - What is the Shifting Caesar Cipher?     - What is the Substitution Cipher?     - How to calculate the number of keys that are possible     - What is the difference between these ciphers?   Workbook (Ciphers)   * + - Encrypt/decrypt with the substitution cipher     - Substitution cipher blurb information for context     - Exercises that will allow students to solve and create their own ciphers     - Describe the advantages of both ciphers.     - Describe their weaknesses     - Calculate the number of possible keys with either. | * + - Video 7.1.1     - Video 7.1.2     - Student Work booklet     - Teacher's Handbook     - Teacher's PowerPoint Aid     - Smart City Kit     - Computers |  |
| Cyber City Satellite Communication | * apply encryption to secure data, for example:   + TLS, SSL, secure VPN, secure messaging, hash-based checksums | Workbook cont.   * + - Introduce modern encryption concepts - more sophisticated attacks eg. Dictionary attacks, Probabilistic approaches / 2-, 3-, 4-letter n-grams.   Exercises   * + - Research examples of modern encryption concepts and create a glossary of terms with their purpose     - Students identify how naïve brute force becomes less viable     - Students must identify which cipher is the best solution for implementation for strongest encryption (shifting Caesar or substitution) on infrastructure and observe how breaking is far more difficult/intractable with simple techniques.   Extension: Implement another encryption technique | * + - Video 7.2.1     - Student Work booklet     - Teacher's Handbook     - Teacher's PowerPoint Aid     - Smart City Kit     - Computers |  |
| Cyber City Satellite Communication | * work individually and collaboratively to apply an engineering design process to complete real-world problems and challenges to cyber security-related scenarios, for example:   + using either physical or virtual platforms. | * + - Video     - What is automation?     - What types of infrastructure are there?     - How may each type benefit cyber security?     - What are the consequences/issues related to each infrastructure? (Feasibility)   Workbook cont. (research task) Research task   * + - Research a chosen SNART City infrastructure.     - Explore the purpose of the infrastructure, the benefits for society, commerce and other human factors.     - Students will have a scaffold for the research task, broken into sub-categories eg. Name, purpose etc for students to fill in Students create an overall statement summarising their research with their research, students assess the impact of a cyber-attack, and what they would do if they were cyber security specialists to safeguard operations, regarding their chosen infrastructure | * + - Video 7.3.1     - Student Work booklet     - Teacher's Handbook     - Teacher's PowerPoint Aid     - Smart City Kit     - Computers |  |

## Week 8, Assessment Preparation: SMART City Infrastructure - Innovation and Entrepreneurial Activity

Outcomes: ST5-1, ST5-2, ST5-6, ST5-8

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Topic | Content | Teaching Strategies | Resources | Registration |
| Assessment Preparatio | * demonstrate innovation and entrepreneurial activity, and communicate solutions to problems involving cyber security. | * + - Assessment Booklet (Over the 3 lessons)     - Individual work/ RES     - Students to create a new smart city infrastructure similar to their satellite in their cyber city task.     - Students are to define their infrastructure     - Students are to explain a value proposition either economically, socially or environmentally     - Students are to complete a feasibility study on their infrastructure | * + - Student Work booklet     - Student Assessment Booklet     - Teacher's Handbook     - Smart City Kit     - Computers |  |

## Week 9, Assesement Presentparation: Managing Cyber Risk

Outcomes: ST5-1, ST5-2, ST5-6, ST5-8

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Topic | Content | Teaching Strategies | Resources | Registration |
| Assessment Preperation | Assessment Booklet   * demonstrate innovation and entrepreneurial activity, and communicate solutions to problems involving cyber security. * complete a cyber risk assessment of an organisation and at home, for example:   + gap analysis and report on findings to evaluate the level of cyber hygiene. | * + - Assessment Booklet (Over the 3 lessons)     - Individual work/ RES     - Students are to complete a risk assessment of their infrastructure with the template within their booklets     - Students are to complete the close mitigation activity on their infrastructure to declare the risk minimisation ideas.     - Students are to suggest how their infrastructure can be implemented into the cyber city program     - Students are to design their infrastructure design, on their micro bit tile template within their booklets and complete a poster/video on their product | * + - Student Work booklet     - Student Assessment Booklet     - Teacher's Handbook     - Smart City Kit     - Computers     - Canva     - Cameras |  |

## Week 10, Assesement Presentation

Outcomes: ST5-1, ST5-2, ST5-6, ST5-8

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Topic | Content | Teaching Strategies | Resources | Registration |
| Assessment Presentation | Assessment Booklet   * demonstrate innovation and entrepreneurial activity, and communicate solutions to cyber security problems. * explain the effects of emerging technologies on current and future cyber security challenges and on professional skills and careers in the industry, for example:   + deep fakes, artificial intelligence-enabled cybercrime. | Assessment Booklet (Over the 3 lessons)  Individual work/ RES   * + - Students will declare the dependent and independent variables of their infrastructure and how they will measure the success e.g. Pitch like the satellite etc.     - Students will address emerging technologies within the field and provide examples of careers and companies that may use this product.   Extension:   * + - Students may present their video or poster of their infrastructure | * + - Student Work booklet     - Student Assessment Booklet     - Teacher's Handbook     - Smart City Kit     - Computers |  |

# Evaluation of Course

|  |  |
| --- | --- |
| Evaluation of Course Module | Completion Date .................................. |
| Suitability of Activities | |
| Progress | |
| Timing | |
| Suitability to student needs | |
| Adequacy of Resources | |
| Assessment | |
| Evaluation of Assessment: | |

Signature:................................................................................ Date:.......................................................