Protect the Island

Contents

© Copyright The Tech Partnership Ltd

Protect the Island

Introduction

Protect the Island has been created in partnership with the team at Hewlett Packard Enterprise. It focuses on cyber security and its importance to individuals' everyday lives as well as to businesses and other organisations. Protect the Island sets out from the beginning to make the important distinction between e-safety – protecting yourself and your identity online – and cyber security which involves protecting information and systems from threats such as cyber terrorism, cyber warfare, and cyber espionage.

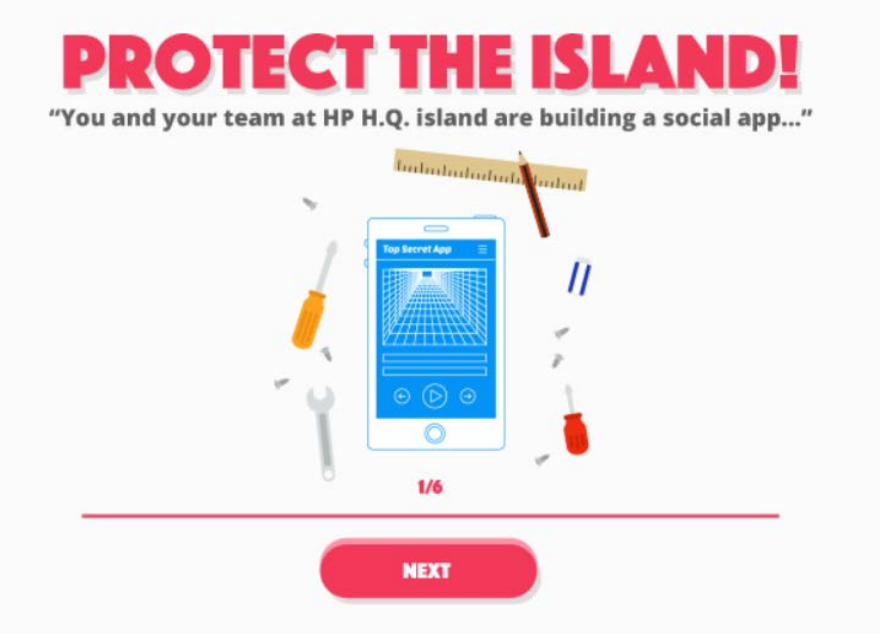
As a large part of good cyber security practice focuses on the importance of human behaviours, so the learning outcomes of this topic mainly focus on behaviours rather than technical skills.

Topic structure

The topic is made up of 4 challenges, and unlike most other TechFuture Girls learning topics, you are restricted to doing each challenge in order. This is because – uniquely for this topic – the challenges are based around a story which runs through the topic. As students start the topic, they are taken through an introduction which sets the scene and outlines the challenge:

> *"You and your team at HPE H.Q. Island are building a social app. The HPE app will be 100 times better than any competitors'. This app will change everyone's lives forever!*
>
> *But it must remain TOP SECRET until its release.*
>
> *Cyber baddies from across the globe have heard rumours of what you're up to and are keen to get their hands on your data.*
>
> *Your job is to protect the island with world-class cyber security to out-fox cyber criminals so the app can be completed."*

Once each of the challenges has been successfully completed, students are shown a message which congratulates them on securing the island and informs them that as a result, another 25% of the app has been built. Once the fourth challenge has been completed, students are invited to enter a competition to submit their ideas for the amazing app.



© Copyright The Tech Partnership Ltd

Preparing to deliver Protect the Island

Materials and technology requirements

- For researching real-life cyber crimes, students will need access to the internet
- Pencils/pens for creating a plan of a room to plot security weaknesses, and to design their app
- Printing – there are several quizzes and resources that would benefit from being printed out. Students may also wish to print out their cyber superheroes in colour.

The challenges in Protect the Island

There are four challenges in this topic, which are completed in the following order.

1. Cyber Briefing

- Introduces students to the concept of cyber security and points out the difference between e-safety and cyber security using an infographic
- Explains what is meant by the terms cyber security and encryption using two short animated films
- Asks students to reflect on what they know so far by asking them to get into pairs and quiz each other using the Cyber Security Quiz (available online or as a downloadable PDF)
- Demonstrates how people can pose a threat to cyber security threat through their behaviour and actions, consciously or unconsciously through an interactive version of the “Guess Who” game. Students can then download a Guess Who game template which they can print off to play the game offline with their friends.

© Copyright The Tech Partnership Ltd

2. Protect the Island

- Students are welcomed into the offices of HPE and play a game where they move around the virtual office spotting potential cyber security threats
- There are 4 quick, offline games which students can play;
    - they can draw a plan of a room (the school ICT suite for instance) and mark on it the points where there might be a cyber security risk
    - they can print off and cut out “Security Risk” badges and stick them on places around the room, or school, where a cyber security threat might occur
    - they can create and act out a story about how a cyber villain might trick their way into a building, like the HPE H.Q., and commit a cyber crime
    - they can investigate real high-profile cyber crimes including the Stuxnet story.

© Copyright The Tech Partnership Ltd

3. Meet Your Dream Team

- In the first part of this challenge, students meet 3 real-life members of HPE's cyber security team. They are shown a video wall with short clips of interviews with each of the cyber people – Yolanta, Kate and Christy. They talk about what they do in their jobs, how they got there, what they enjoy about their jobs and offer some careers advice. Students have to watch a minimum of 3 short clips before they can move on
- Next, they have to create a new member of the cyber "dream team". Using the interactive "Create-O-Matic", students flick through qualities and personalities until they have created their own cyber superhero. They can then print this off to take home, or you could start a TechFuture Girls "Cyber Dream Team" display in your classroom
- Students are asked to compare their cyber superheroes with those created by their friends and talk about what their different skills and attributes are, the purpose being that students realise that a great team is made up of people with a good mix of different skills and personalities
- Students then get into pairs and find out from each other what their own superpowers might be – are they good at maths, or really creative, or are they brilliant organisers…? They could feed back to the group on what their partners' superpowers are.

© Copyright The Tech Partnership Ltd

4. Use the Cyber Force

- In the final challenge, students must use all the tools they've picked up in the rest of the topic to fend off a final cyber threat. They are told that "global cyber baddies have heard that the HPE app is almost finished" and that they "must use all the skills you have learnt to boost the cyber force field around HPE Island".
- The game is a simple "Space Invaders" type concept – students use the arrow keys on their keyboard, or their mouse to move a boat around HPE Island and collect the "boosters" which include a cyber forensics team, antivirus updates, firewall encryption and software updates, whilst dodging the threats – malware, suspicious people, phishing emails and code bugs. As they get more points, the cyber force field around the island gets visibly stronger – or weaker if they lose points. Once the force field is at 100%, they have completed the game.
- The app competition: Students are invited to enter the 2015/16 super app competition between TechFuture Girls clubs. They need to think about the app's name, what it does, the audience it's for and what it looks like. They can download and print off a template to illustrate the 4 requirements, and once their entry is complete, they are asked to get their teacher to tweet their entry using the hashtag **#HPEcybersleuths**.

Suggested delivery schedule

This topic can be completed within four 45 minute sessions. A recommended breakdown of the challenge by session is shown below, although for shorter clubs each of the suggested sessions could be delivered across two sessions.

Session 1

- The introduction to Protect the Island and challenge 1 – Cyber Briefing – is all about explaining what cyber security is and how it is different from what students know as e-safety.

  Students will begin by clicking through the introduction and will then move on to looking at the "What is cyber security" infographic, which you could display on a whiteboard, and two short animations which you could watch as a group to initiate a discussion about students' understanding of cyber security, what the risks are and why a company such as HPE, or an organisation like their school might need to be aware of the risks and take measures to protect against cyber attacks.

© Copyright The Tech Partnership Ltd

- After the animations, the students can quiz each other using the suggested questions on the screen (you can also download and print off the quiz questions). Again, this could be done either in pairs, small groups or as a whole group.
- The third phase of challenge 1 is an interactive “guess who” game. Students could do this individually or could pair up on a computer to play the game together.

  To play Guess Who, students click on a character to find out more about them and then decide whether that character poses a cyber threat or not by dragging and dropping them into the “Yes” or “No” pile. They can check their score for feedback throughout the game and will be told at the end of the game what their final score is, and why the characters pose a threat or not.
- The last phase of challenge 1 is an offline version of Guess Who. Students can try out either or both games. The first is “Guess Who Cyber Island” which asks students to get into pairs, print out cards featuring the 8 characters from the online Guess Who games, pick a card each and then try and guess which character your partner is by asking questions with yes or no answers.

  The second game is “Guess Who You Know”. Again, students get into pairs and print off 6 cards – this time with 6 mystery characters. Students then have to create 6 characters based on people they know, or fictitious people who might knowingly or unknowingly pose a cyber security threat. This encourages students to think about the behaviours people might commonly display that might make them a cyber threat, e.g. forgetful people who write down passwords for their computer, network or websites.

Session 2

- Whereas challenge 1 was all about introducing the concept of cyber security, challenge 2 – Protect the Island – starts to show how the cyber security practices and behaviours seen in challenge 1 can be put into practice. Challenge 2 begins by welcoming students to the offices of HPE. Students are told that there have been reports of security weaknesses in the office and they need to search the virtual office for anything that could be a threat to HPE’s cyber security.

  When students enter the game they are shown instructions which explain that they can use their mouse or laptop trackpad to hover over potential threats in the office. If a situation or object is a potential threat it will glow green and students can then click to find out more and then answer “Yes” or “No” as to whether they believe it is a threat. They can use the arrows in the corners of the game to navigate around the office. Once all the threats have been correctly identified, students can review why each was a threat and then move on to phase 2 of challenge 2.

  There are also some potential threats that are not part of the game and you could set students the extra challenge of spotting these and award credits for each one they identify. The other potential threats are:

  - There is a laptop open on the desk below the security camera with no screen saver/locked screen
  - There are print-outs on the printer and in the “in/out” trays that nobody has picked up
  - There’s a mobile phone left unattended on a desk near the box of USBs.

© Copyright The Tech Partnership Ltd

- In the next phase of challenge 2, there are 4 quick offline games in which students can:
    - draw a plan of a room (the school ICT suite for instance) and mark on it the points where there might be a cyber security risk
    - print off and cut out “Security Risk” badges and stick them on places around the room, or school, where a cyber security threat might occur
    - create and act out a story about how a cyber villain might trick their way into a building, like the HPE H.Q. and commit a cyber crime
    - investigate real high-profile cyber crimes including the Stuxnet story.

  With each of the four games, students can download and print a PDF showing the instructions for the game. To save on printing, you could print out a couple of each of the PDFs before your club so that students can share a copy and work together on each of the games.

Session 3

- Challenge 3 – “Meet the Dream Team” – focuses on the human side of cyber security and how companies like HPE are fighting cyber attacks by assembling teams of people with the right mix of skills.
- In the first phase of the challenge, students meet Kate, Yolanta and Christy – all real-life cyber professionals working out of the HPE Labs in Bristol. Clicking on a tile on the video wall will bring up short snippets of film showing each of the cyber mentors talking about their careers so it would be useful for students to have headphones for this.

  All three women have fascinating jobs in a fast-growing, innovative and exciting area of technology which offers great future career opportunities, so the hope is that meeting the cyber mentors will inspire the girls to consider a future career route that they might not have previously known about. Once students have watched at least 3 clips, they can move on to the next phase of the challenge.
- Having met three “cyber superheroes”, students move on to building their own using the “Create-O-Matic” – a fruit machine style game where students select skills, personality traits and a style to create someone that could represent themselves, or could just be someone they think would make a great cyber superhero. Once they’ve made their cyber superhero, students can print them out and compare them with their friends’ creations.
- In the final part of challenge 3, students consider how their own skills might make them potential cyber superheroes. They are asked to get into pairs or small groups and identify valuable skills or personality traits in each other. There is a downloadable PDF with some suggestions, such as creative thinking, problem solver etc. which you could print prior to your club starting so that students can share a copy between them.

  You could ask students to present back in their pairs or groups at the end of the session to tell the rest of the club which qualities they’ve found in each other.

Session 4

The fourth and final challenge in this topic brings the story to a close. The cyber baddies have found out about amazing HPE app that is in development and are planning a cyber attack on the island to try and get their hands on the app.

© Copyright The Tech Partnership Ltd

Students will need a computer each to play the Use the Cyber Force game – a kind of space invaders style game where students navigate a boat around HPE Island and collect the "boosters" which include a cyber forensics team, antivirus updates, firewall encryption and software updates, whilst dodging the threats – malware, suspicious people, phishing emails and code bugs. As they get more points, the cyber force field around the island gets visibly stronger – or weaker if they lose points. Once the force field is at 100%, they have completed the game.

Once they have completed the game, HPE Island is now a secure place to develop the super app and students are invited to enter the 2015/16 super app competition between TechFuture Girls clubs. They need to think about the app's name, what it does, the audience it's for and what it looks like. They can download and print off a template to illustrate the 4 requirements, and once their entry is complete, they are asked to get their teacher to tweet their entry using the hashtag **#HPEcybersleuths**.

If neither you nor your school has a Twitter account, please email your entries to the TechFuture Helpdesk – helpdesk@techfuture.com - and we can tweet your entries from the @TechFutureGirls Twitter account.

Links to the National Curriculum in England

Although TechFuture Girls is designed to be used as an extra-curricular activity, this topic does have links to the Computing National Curriculum in England as follows:

Programmes of study aims	Key Stage 2	Key Stage 3
The National Curriculum for Computing aims to ensure that all pupils… …are responsible, competent, confident and creative users of information and communication technology.	Pupils should be taught to… …use technology safely, respectfully and responsibly; recognise acceptable/ unacceptable behaviour; identify a range of ways to report concerns about content and contact.	Pupils should be taught to… …understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy; recognise inappropriate content, contact and conduct, and know how to report concerns.

Cyber security: A quick guide

Why is cyber security so important?

The internet is revolutionising our society by driving economic growth and giving people new ways to connect and co-operate with one another. Falling costs mean accessing the internet will become cheaper and easier, allowing more people in the UK and around the world to use it, 'democratising' the use of technology and feeding the flow of innovation and productivity. This will drive the expansion of cyberspace further and as it grows, so will the value of using it.

As with most change, increasing our reliance on cyberspace brings new opportunities but also new threats. While cyberspace fosters open markets and open societies, this very openness can also make us more vulnerable to those – criminals, hackers, foreign intelligence services – who want to harm us by compromising or damaging our critical data and systems.

© Copyright The Tech Partnership Ltd

The impacts are already being felt and will grow as our reliance on cyberspace grows. The networks on which we now rely for our daily lives transcend organisational and national boundaries. Events in cyberspace can happen at immense speed, outstripping traditional responses (for example, the exploitation of cyberspace can mean crimes such as fraud can be committed remotely, and on an industrial scale).

(ref. The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, 2011; www.Gov.uk)

What is cyber security?

Cyber security is a way of fighting against and preventing cyber crime. It is a field that is growing rapidly as the techniques to create cyber attacks become more and more sophisticated. Attacks can take many forms and so cyber security professionals are constantly learning and improving their skills to keep up with the cyber criminals.

Cyber Security Glossary

Some common terms used in cyber security:

Active Attack

A deliberate assault that intends to alter a system, its resources, its data or its operations.

Blacklist

A list of entities that are blocked or denied privileges or access.

Black Hat Hacker

Someone with extensive computer knowledge whose purpose is to breach or bypass internet security. Black hat hackers are also known as crackers or dark-side hackers. The general view is that, while hackers build things, crackers break things, and whilst White Hat Hackers hackers hack for ethical reasons, Black Hats are hacking with malicious intent.

Bot

A computer connected to the Internet that has been secretly compromised with malicious logic to perform activities under the remote command and control of a remote administrator.

Cryptography

The use of mathematical techniques to provide security services, such as confidentiality, data integrity, entity authentication and data origin authentication.

Cyber Space

The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems and embedded processors and controllers.

Data Breach

The unlawful movement or disclosure of sensitive information to a party, usually outside the organisation, that is not approved to have or see the information.

Digital Forensics

The processes and specialised techniques for gathering, retaining and analysing system-related data (digital evidence) for investigative purposes.

© Copyright The Tech Partnership Ltd

Enterprise Risk Management

A comprehensive approach to risk management that engages people, processes and systems across an organisation to improve the quality of decision making for managing risks that may hinder an organisation's ability to achieve its objectives. Companies such as Hewlett Packard Enterprise offer specialist enterprise risk management services to both private and public clients.

Encryption

The transformation of data into a secret code. Encryption is the most effective way to ensure data passing from one source to another stays secure. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

Firewall

A firewall is a network security system that checks information coming from the Internet or a network, and then either blocks it or allows it to pass through to your computer, depending on predetermined security rules.

Intrusion Detection

The process and methods for analysing information from networks and information systems to determine if a security breach or security violation has occurred.

Key

An encryption key is a security measure that turns data into an unreadable cipher through complex algorithms to ensure data passing through networks is kept confidential.

Malware

'Malware' is a term which denotes a variety of hostile or invasive software, including adware, computer viruses, trojan horses, ransomware, spyware, scareware, worms and other malicious programs.

Passive Attack

An attack which is committed by someone who intends to make use of information from a system but does not attempt to alter the system, its resources, its data or its operations.

Penetration Testing

An evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.

Phishing

A digital form of social engineering to deceive individuals into providing sensitive information.

Root

A set of software tools with administrator-level access privileges installed on an information system and designed to hide the presence of the tools, maintain the access privileges and conceal the activities conducted by the tools.

Virus

A computer program that can replicate itself, infect a computer without permission or knowledge of the user and then spread or propagate to another computer.

© Copyright The Tech Partnership Ltd

Whitelist

A list of entities that are considered trustworthy and are granted access or privileges.

White Hat Hacker

A White Hat Hacker is someone who breaks into systems or networks to test their security for ethical reasons. They might be employed to uncover vulnerabilities so that security measures can be put in place before Black Hat Hackers are able to exploit the weaknesses for malicious reasons.

End of document

© Copyright The Tech Partnership Ltd