TECHFUTURE CLASSROOM

Guide to the Cyber Security Badge Academy

Introduction

Within the Tech Partnership Badge Academy, we have a dedicated academy for Cyber Security for Key Stage 4 and above students. This has been supported by a range of employers including TCS, CGI, Fujitsu, Samsung and Cisco and recognises the importance of these skills in young people, and the need for future talent who are inspired to enter the cyber security industry.

All badges within the Cyber Security Badge Academy are automatically awarded to students through the platform for completion of associated e-learning. Students have to pass the assessment built into the e-learning with a score of 80 percent. The badge is then automatically awarded to them, and they receive an email notification. This eliminates the need for you as a teacher to verify their work to gain the badge. Details of each badge and the learning outcomes for each are shown below.

Table 1: The Cyber Security Badges and their learning outcomes

Badge Name	Learning outcomes
Social Engineering	Understand proactive and reactive cyber security Understand the techniques used in phishing emails and how to spot them Understand that social engineering uses psychological techniques to fool victims Understand techniques such as pretexting, *Quid Pro Quo* and how to recognize suspicious emails Understand why victims are vulnerable and why they respond to social engineering
Encryption	Understand the difference between encryption and cryptography Understand different types of cipher, including substitution and transposition Understand what asymmetric and symmetric algorithms are, and how public key cryptography works Understand and use a range of simple ciphers including code word, pigpen and paragraph-word-letter Understand how to identify that a website is using encryption through the HTTPS in the URL
Hacking	Understand some of the main motivations for cyber-crime including political ideology, hacktivism and identity theft Understand that the main driver for cyber-crime is theft or corruption of information that is shared and exchanged across the internet

Brought to you by

TECH PARTNERSHIP

Badge Name	Learning outcomes
	Understand what a Distributed Denial of Service attack is and how they are perpetrated Understand how cyber security professionals are in an arms race with cyber criminals and what types of strategies both use in the race including patching and phishing Understand how typical viruses work and how new ways of committing cyber-crime include ransomware Understand the differences between white hat, black hat and grey hat hackers Understand how to make judgements about the actions of others in terms of their ethical or unethical use of computers
Threats	Understand what malware is and how it is used to commit cyber crime Understand the difference between virus, worms and Trojans, ransomware and adware Understand how firewalls can be implemented to reduce the threat of malware attack Understand the mode of action of viruses, that they require the user to run an infected program, and can allow a hacker to record a user's key strokes Understand the mode of action of worms, which are standalone malware that can easily transmit across networks Understand the mode of action of Trojans and how they can vary in their mode of action including through rootkits, backdoor and botnets
Digital Footprint	Understand the challenge of social media for cyber security Understand the permanent nature of the digital footprint and how it can impact on college and university applications, and recruitment into work Understand the potential of Facebook, posting and image tagging for spreading information that may not be positive Understand and apply good practice in controlling the use of social media Understand how to use Twitter in a safe manner by controlling followers and protecting tweets Understand how LinkedIn is different from Facebook and how, when used safely, it can benefit future career prospects
Online safety	Understand the importance of e-safety for school, including the requirements of Ofsted Understand how e-safety includes content, contact and conduct and what this means Understand the implications of cyber bullying, and how to help those who are known to be victims Understand how to deal with negative social media activity, using best practice to address any examples

Badge Name	Learning outcomes
	Understand why password security is important and how to choose secure passwords that cannot be guessed by others Understand good and safe practice on social media and what should and should not be shared Understand how to ensure websites are secure before entering personal information
Network Security	Understand how the Internet works, including the importance of TCP/IP in movement of data across the network Understands how TCP establishes a connection with other computers, and then breaks down information to be sent into packets before sending Understand how IP addresses work and how text and numerical addresses are matched using a Domain Name Server Understand how computers can do multiple tasks using the internet through the use of TCP ports Understand HTTPS and how it provides a secure way of sending information across the Internet Understand that HTML is the language of the web, which relies upon tags Understand what packet sniffing is and how it can be used ethically and unethically Understand how networks are protected by levels of access and identity management Understand the importance of protecting home networks with a security key to prevent others accessing it Understand what WPA-2 is and why it is important in protecting a home network Understand why it is important to not allow mobile devices to connect to Wi-Fi networks outside the home

The Cisco Cyber Detective badge

There is another badge in the Cyber Security Badge Academy which is associated with completion of the Countdown to Chaos cyber-attack simulation. This badge is suitable for 11-16 year olds who can use the resource. However, the open badge can only be gained by students aged 13 or over as they can only open the Mozilla Open Backpack at the age of 13 years. Under-13s can gain the digital (rather than open) badge and see it under their My Badge profile on the platform, but cannot share it until old enough to open the Mozilla Backpack account.

There are two versions of this badge:

- **Badge with the red icon** is automatically awarded when students individually work through the four acts within the Countdown to Chaos project. Once they have worked through and completed the four acts, the system will recognise this and award the badge.
- **Badge without the red icon** has the same criteria, but this is available to students who have not individually worked through the resource. This would be suitable for students who have worked as a large group with the contents being projected, as in a whole- or part-class activity

or in an after-school club. In this case, we will supply a code for students to input to gain the badge. The code is changed monthly to ensure students do not share the code.

- In both cases students will need to login to claim their badge.

If you have any further questions about using the Cyber Security Badge Academy, or the Tech Partnership Learning Hub, email sue@thetechpartnership.com and we will respond as quickly as we can.