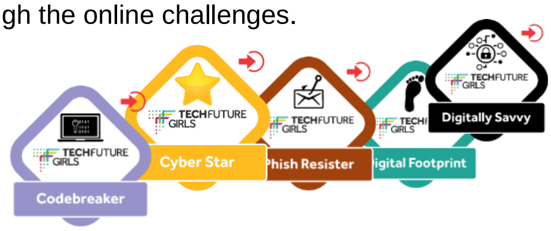
Facilitator support guide

Guide to the Cyber Safety topic

Club members learn about how to recognise phishing attacks, and what a digital footprint is and how their online behaviour contributes to it. They try their hand at codebreaking whilst learning about encryption as a way of securing information, and become digitally savvy by thinking about passwords, ethical behaviour online, privacy and online safety more broadly.

Five Digital Badges for members to gain by working through the online challenges.

- Phish Resister
- Digital Footprint
- Codebreaker
- Digitally Savvy
- Cyber Star – automatically awarded to all students who gain all four Cyber Safety badges.



How a TechFuture Girls topic works

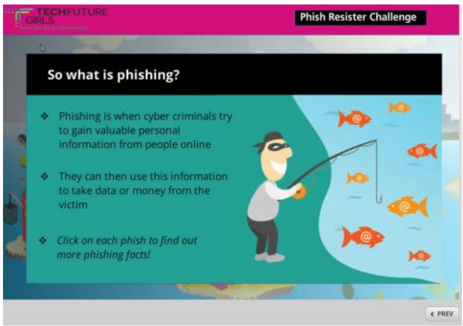
Within each topic – chosen to be particularly interesting to girls – there are three or more challenges for members to complete. Each challenge has an online e-learning module, which explores key concepts within a topic, with embedded quiz questions to assess understanding along the way. Members who score 80 percent or more automatically receive a Digital Badge, which appears in their profile once earned.

Alongside the online challenge, an offline challenge document is provided which asks members to go further with the topic. This is supported with sets of how2 documents that help build skills as the offline challenge is completed.

Online challenges can take between 30 and 45 minutes. Offline challenges can typically take longer, usually over several sessions. The offline challenges also lend themselves to team work and collaboration.

The online challenge format

The online challenges are built as e-learning. They are a series of screens that often include hotspots, where clicking on images or markers bring up more information. In most cases, all the hotspots have to be checked before the 'next' button appears. So if one of your members/students can't see the next button, it is because there is an unchecked hotspot!


Phish Resister Challenge

So what is phishing?

- Phishing is when cyber criminals try to gain valuable personal information from people online
- They can then use this information to take data or money from the victim
- *Click on each phish to find out more phishing facts!*

In the screenshot on the right, each fish is a hotspot. Only after exploring each of these will be next button appear so the learner can move on.

The challenges in the Cyber Safety topic

There are four challenges in Cyber Safety, with a Cyber Star badge for girls who achieve all four of the online challenge badges.

Challenge 1: Phish Resister

In this challenge, members are introduced to phishing, the techniques used by cyber criminals to entice people to download malware to their computer, or to reveal personal information by clicking on infected links in emails and other messages. They are shown how to recognise phishing, and what to do if they suspect someone is trying to fool them into revealing information, or clicking on infected links. The e-learning includes video animations to support this topic.

The offline challenge is to create an interactive poster in MS PowerPoint that explains to others – friends and family – how to recognise and avoid phishing attacks. This forms a pattern in this topic – we want girls to become empowered to share their knowledge of secure practices online with others. So other challenges ask them to explain the digital footprint and to creatively show others how to select secure passwords.

Additional resources provided for girls include How2 make an interactive poster in MS PowerPoint, How2 turn PowerPoint slides into JPEGs, and How2 use MS Publisher to create the poster.

Challenge 2: Your Digital Footprint

This topic introduces members to what a digital footprint is and how all online activity, starting with childhood, can contribute to a permanent record of online activity.

Girls learn about the different activities that can contribute to the footprint, including social media. The important message of the age restrictions on social media accounts is made very explicitly, whilst recognising girls will have heard about the various types of social media that are out there.

The offline challenge is to use multimedia to explain the digital footprint to others. This could be a video, animation, news bulletin or an animated presentation. It could be carried out as part of the BBC School Report.

Resources supplied for this challenge include How2 be inspired to create a multimedia presentation and a folder of copyright-free images to use in the presentation, featuring many of the images girls will have seen in the online challenge.

Challenge 3: Codebreaking

The third challenge introduces cryptography, encryption and codebreaking to girls, with two main ciphers covered in the online challenge – the pigpen and codeword ciphers. They also hear about how encryption of information is important when transferring data across the Internet, and how asymmetrical encryption works.

The offline challenge is to encrypt a message using either pigpen, codeword or a cryptograph wheel. They are provided with How2s that explain each of these ciphers and how to use them.

Challenge 4: Digitally Savvy

The fourth challenge explores more about online safety including addressing the ‘three Cs’ – content, conduct and contact. It also looks at good password security, ethical online behaviour and understanding privacy.

The offline challenge is to creatively share with others how to construct a secure password from a familiar word that is then adjusted to include upper and lowercase letters, numbers and characters. Ideas include role play, music or poetry (including a rap) or a presentation. Girls are encouraged to let us know at helpdesk@techfuture.com if they come up with a particularly creative way to do this!

The Cyber Star badge

For girls who are collect all four badges for completed online challenges, the Cyber Star badge will automatically award. So girls can achieve five badges for this topic.

Going further

Members and facilitator/teachers of TechFuture Girls now have access to additional content on TechFuture Classroom. At the bottom of each topic page, there are links to do more. For this topic, a link is provided to the very popular Countdown to Chaos project on TechFuture Classroom. This is a real time simulation across four acts of a cyber attack on the power grid. Girls have to identify the perpetrator of the cyber attack before the lights go out.

We have also provided a link to our Cyber Security Roles game, where girls have to choose the correct cyber security professional for five different scenarios. This gives them an insight into the careers available in the cyber security industry.

A third link takes them to the Bletchley Park website to find out more about the cracking of the Enigma Code.

How2s included in this topic

Each challenge has a set of how2s – guides on skills and concepts – to help members complete the offline challenges and build on knowledge acquired in the online challenges. The table below shows all the how2s in the Cyber Safety topic.

Table 1: The How2 documents provided in this topic

Challenge	How2
Phish Resister	How2 make an interactive poster in MS PowerPoint
	How2 turn PowerPoint slides into JPEGs
	How2 use MS Publisher to create your poster
Digital Footprint	How2 be inspired to create a multimedia presentation
Codebreaker	How2 use the pigpen cipher to encrypt a message
	How2 use a cryptograph wheel to encrypt a message
	How2 use a codeword cipher to encrypt a message

Learning Outcomes and curriculum mapping for the Cyber Safety topic

The table below displays the learning outcomes for each topic and their relevance to the Programmes of Study for Computing (Key Stages 2 and 3).

Table 2: Learning outcomes and Computing PoS mapping

Challenge	Learning Outcomes	Programmes of Study for Computing
Phish Resister	Understand what phishing is and how it is used by cybercriminals	**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 *(Key Stage 2)* Select, use and combine a variety of software on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including …. presenting data and information *(Key Stage 2)* 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 *(Key Stage 3)* Undertake creative projects that involve selecting, using and combining multiple applications, preferably across a range of devices, to achieve challenging goals, including collecting ... data and meeting the needs of known users *(Key Stage 3)*
	Understand how cybercriminals use psychological characteristics in phishing attacks	
	Understand how to recognise phishing attempts in emails and other messages	
	Understand how phishing can lead to malware infection	
	Understand how phishing can lead people to surrender personal and confidential information	
	Understand how to resist phishing attempts	
Digital Footprint	Understand what a digital footprint is and how it can last forever	**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 *(Key Stage 2)* Select, use and combine a variety of software on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including …. presenting data and information *(Key Stage 2)* 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 *(Key Stage 3)* Undertake creative projects that involve selecting, using and combining multiple applications, preferably across a range of devices, to achieve challenging goals, including collecting ... data and meeting the needs of known users *(Key Stage 3)*
	Understand how all online activity can contribute to the digital footprint	
	Understand how cookies can track activity on websites which can then feature in the digital footprint	
	Understand how social media activity can contribute to the digital footprint	
	Understand how and why social media is age restricted	
	Understand how to find out about your own digital footprint	

Challenge	Learning Outcomes	Programmes of Study for Computing
Codebreaker	Understand what cryptography, encryption and codebreaking are	**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 *(Key Stage 2)* 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 *(Key Stage 3)*
	Understand how to use different ciphers to encrypt a message	
	Understand how to decrypt a message when you know a codeword	
	Understand how important encryption is when sending data through the Internet	
	Understand how public and private keys work in asymmetric cryptography	
Digitally Savvy	Understand how to use good password security including choosing passwords that cannot be guessed or hacked	Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact *(Key Stage 2)* Select, use and combine a variety of software on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including …. presenting data and information *(Key Stage 2)* 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 *(Key Stage 3)* Undertake creative projects that involve selecting, using and combining multiple applications, preferably across a range of devices, to achieve challenging goals, including collecting ... data and meeting the needs of known users *(Key Stage 3)*
	Understand how to work ethically, including not making use of others' work or ideas	
	Understand how to act ethically online in communication with others	
	Understand the importance of privacy settings in online accounts and different applications	
	Understand how to work online safely	
	Understand how to ensure online conduct, content viewed and contacts are sensible and safe	

If you require any help setting up your TechFuture Girls club, wish to use the resources, and TechFuture Classroom, in school, or have any questions about our platform, email us at helpdesk@techfuture.com and we will respond to your request within 48 hours.