CyberSprinters Practitioner Overview

Contents

Welcome and introduction

Welcome to our educational resources toolkit for practitioners who work with children aged 7-11. We are delighted to introduce our CyberSprinters resources developed by the National Cyber Security Centre (NCSC).

This toolkit consists of:

- CyberSprinters Practitioner overview (this document)

A set of activities and practitioner notes and resources related to the key themes

Topic 1 - Passwords

- Activity 1a
  Creating Strong Passwords (session overview)
  Creating Strong Passwords (practitioner notes)
  Creating Strong Passwords (assets)

- Activity 1b
  Two Factor Authentication (session overview)
  Two Factor Authentication (practitioner notes)
  Two Factor Authentication (assets)

- Activity 1c
  Passwords and 2FA (session overview)
  Passwords and 2FA (practitioner notes
  Passwords and 2FA (assets)

- Activity 1d
  Protecting Email (session overview)
  Protecting Email (practitioner notes)
  Protecting Email (assets)

- Activity 1e
  Passwords recap (session overview)
  Passwords recap (assets)

Topic 2 - Devices

- Activity 2a
  What is Personal information (session overview)
  What is Personal Information (practitioner notes)
  What is Personal Information (assets)

- Activity 2b and 2c
  Updating devices (practitioner notes) - covers activities b and c
  Updating devices (session overview) - covers activities b and c
  Updating devices ‘bingo game (assets)
  Updating devices ‘phone game (assets)

- Activity 2d
  Pulling it all together (session overview)
  Pulling it all together (assets)

Topic 3 - Suspicious Messages

- Activity 3a
  Types of suspicious messages (session overview)
  Types of suspicious messages (practitioner notes)

- Activity 3b
  Phishing Investigations (session overview)
  Phishing Investigations (assets)

- Activity 3c
  What should an email look like (session overview)
  What should an email look like (practitioner notes)

- Activity 3d
  Phishing survival guide (session overview)
  Phishing survival guide (assets)

Additional resources

- A Certificate for children

- A Leaderboard template

- A crossword activity for children to work on at home with their parents and carers

- A wordsearch activity for children to work on at home with their parents and carers

Background

Children and young people's use of technology has grown exponentially in the last ten years and continues to grow. During the Covid 19 pandemic children were learning online as well as doing most of their socialising online.

Recent data from Ofcom highlights that:

- Half of 10 year olds now own a smartphone
- Use of smart speakers has doubled in the last year for children aged 5-15 making them more popular than radios
- More children watch video on demand than live TV broadcast
- YouTube is still very popular
- The top social media platforms are WhatsApp; Snapchat; Instagram and Facebook
- Twitch and TikTok have gained huge popularity
- Gaming amongst girls is on the increase

Ofcom 2019 – Media Use and Attitudes report

With all of this access to technology there are challenges around the protection and the level of skills that young people are able to deploy to protect themselves and their devices. With the increase in wearable technology and AI starting to infiltrate everyday life it is crucial that children and young people are able to protect themselves and know where to find support.

Children and adults can be susceptible to risk and harm in the online context and need to be educated about the risks.

Whilst many young people feel technically able, their level of understanding can be limited and parents often feel overwhelmed with the variety and pace of their children's online lives.

There has been an emphasis - especially since 2006 - on educating children and young people on broader online risks such as grooming and cyber bullying. One of the leading programmes is the NCA CEOP's ThinkUKnow programme which was launched in 2006 and whose aim is to educate children and young people about sexual exploitation online.

Cyber security is less well covered in terms of resources that are available for practitioners to help children develop their personal cyber security skills.

What is Cyber Security?

Cyber security is the means by which individuals and organisations reduce the risk of being affected by cyber crime.

Cyber security's core function is to protect the **devices** we all use (smartphones, laptops, tablets and computers), and the **services** we access online - both at home and work - from theft or damage. It's also about preventing unauthorised access to the vast amounts of **personal information** we store on these devices, and online.

Cyber security is important because smartphones, computers and the internet are now such a fundamental part of modern life, that it's difficult to imagine how we'd function without them. From online banking and shopping, to email and social media, it's more important than ever to take steps that can prevent cyber criminals getting hold of our accounts, data, and devices.

There are different types of cyber security relating to individuals and organisations, these can be categorised as follows:

- **Information security** - is the practice of protecting information by mitigating information risks. It typically involves preventing or at least reducing the probability of unauthorised/inappropriate access, use, disclosure, disruption, deletion/destruction, corruption, modification. This is generally achieved by identifying risks and ensuring that strong passwords, firewalls, encryption are in place.

- **Organisational cyber security** – this is about protecting the information held within a certain organisation and ensuring that it is safe.

- **Personal cyber security** – is about protecting your own data and devices this includes ensuring that software is up to date, using strong passwords and ensuring that your data is backed up.

These resources specifically support children in developing their own personal cyber security skills, to ensure that they are educated and supported in doing so and signposting them to support when things go wrong.

The Cost of Cybercrime

A recent report put the cost of worldwide cybercrime at $600 billion per year or 0.8% of global GDP. Common types of cybercrime in the UK involve hacking of personal information or malware and viruses on devices. Many organisations, including the NHS have been victims of cybercrime and many schools have put robust systems in place to protect their data.

In a recent report by City of London Police – Assessment of the threat posed to the UK from Cyber Dependent Crime highlighted:

The top three cyber threats as:

1. Hacking social media and email
2. Computer virus/malware/spyware
3. Personal hacking

It equated to **£5.4 million in losses**

Some of the key ways in which people were scammed were phishing emails, weak passwords which enabled access to accounts and general weak security.

With many children and young people using social media, and high numbers of cyber security offences relating to the hacking of social media accounts, it is important that children and young people develop the skills and understanding to help keep themselves and their accounts secure.

‘Offences of hacking of social media or email accounts totalled nearly 50% of all reports and accounted for the highest collective loss to victims’

Individuals are more likely to report Cybercrime (88%)

The victims of cybercrime are not just adults, children can also be victims. Internet enabled devices like smart watches and speakers can be hacked and used for surveillance or children can be victims of online shopping scams. There is some evidence to suggest that children are less likely to realise that they are the victim of a cybercrime.

Children need to be encouraged to recognise the signs and be supported in helping to protect themselves and to report incidents.

About the National Cyber Security Centre

NCSC stands for the National Cyber Security Centre. Our mission is to help protect the United Kingdom from cyber threats and to make sure the United Kingdom is a safe place to live and work online.

The NCSC develop a range of resources and provide advice for organisations and individuals to help them stay secure online.

Key messages

All of the resources and the CyberSprinters game focus around conveying key messages to children and will help them to develop their knowledge, skills and understanding in crucial areas.

Using and managing passwords	Protecting your devices	Suspicious emails
I can describe simple strategies for creating and keeping passwords private. I can explain what a strong password is and demonstrate how to create one. I can explain why I need a strong, separate password on my email account. I can explain why I need to reset my password if it is shared, lost, or stolen.	I can describe what personal information is and why it's important to me. I can explain what backing up a device means and why it's important. I can explain why it's important to update the software and apps on my device. I can explain why it's helpful to turn on automatic updates on my device.	I can describe ways to spot a suspicious email. I can describe what to do if I receive a suspicious email. I can explain what a phishing email is and why criminals send them. I can explain where to report a suspicious email if I receive one.

The intention is that children will be supported on their cyber security journey to develop the necessary skills to enhance their own personal cyber security at every stage.

About the new resources

After reviewing the available resources for children and young people the NCSC found that:

- There were limited resources to support children and young people in developing their personal cyber security skills
- Most of the resources focused on issues like developing effective passwords
- There was a need for a suite of resources that could be used in a range of educational settings which highlighted the evidence based messages

The NCSC wanted to ensure that children were being given credible advice and support to develop their skills, something that was interactive and fun which would be relevant to them.

How to use the resources

There is no right or wrong way to use the resources and as a practitioner you will want to think about what suits your children and your setting.

During the course of reviewing of the materials several practitioners made suggestions about how they would use the materials and the game.

NCSC would recommend using the resources in order – e.g. the passwords resources first, then moving onto updating devices and suspicious contact. This will help the children to learn the concepts. The resources have been created for the 7-11 age groups but you may decide to only use some of them for specific age ranges.

Example 1 (school setting)

The teacher shows the game on the whiteboard and has the activities ready to play. The game is played on the whiteboard and is stopped at the key points (e.g. where there are questions that need to be answered) and the children are invited to the front of the class to contribute their answers. At the end of the session the key points are summarised and the children are asked if they have found anything surprising. After the game has been played the children work through the resources on a week by week basis.

Example 2 (non-formal educational setting)

All of the children worked through the activities – passwords; updating devices and suspicious contact. This was done in bite size chunks over a period of weeks. At the end of each week the children played the game and tested their knowledge and we shared our scores on the leaderboard which we kept in the classroom. When the activities were completed the children took home the crossword and wordsearch to show their parents/carers.

Activities Overview:

There are three sets of activities for practitioners to use with children aged between 7-11, one which focuses on passwords, one which focuses on updating devices and the final one which focuses on suspicious contact. The purpose of all of the resources is to help children develop their own personal cyber security skills.

Topic 1 - Passwords

- Activity 1a
  Creating Strong Passwords (session overview)
  Creating Strong Passwords (practitioner notes)
  Creating Strong Passwords (assets)

- Activity 1b
  Two Factor Authentication (session overview)
  Two Factor Authentication (practitioner notes)
  Two Factor Authentication (assets)

- Activity 1c
  Passwords and 2FA (session overview)
  Passwords and 2FA (practitioner notes
  Passwords and 2FA (assets)

- Activity 1d
  Protecting Email (session overview)
  Protecting Email (practitioner notes)
  Protecting Email (assets)

- Activity 1e
  Passwords recap (session overview)
  Passwords recap (assets)

Topic 2 - Devices

- Activity 2a
  What is Personal information (session overview)
  What is Personal Information (practitioner notes)
  What is Personal Information (assets)

- Activity 2b and 2c
  Updating devices (practitioner notes) - covers activities b and c
  Updating devices (session overview) - covers activities b and c
  Updating devices ‘bingo game (assets)
  Updating devices ‘phone game (assets)

- Activity 2d
  Pulling it all together (session overview)
  Pulling it all together (assets)

Topic 3 - Suspicious Messages

- Activity 3a
  Types of suspicious messages (session overview)
  Types of suspicious messages (practitioner notes)

- Activity 3b
  Phishing Investigations (session overview)
  Phishing Investigations (assets)

- Activity 3c
  What should an email look like? (session overview)
  What should an email look like? (practitioner notes)

- Activity 3d
  Phishing survival guide (session overview)
  Phishing survival guide (assets)

  Additional resources:

- A Certificate for children

- A Leaderboard template

- A crossword activity for children to work on at home with their parents and carers

- A wordsearch activity for children to work on at home with their parents and carers

In addition to the activities for practitioners there are two additional resources developed for children to do at home with their parents/carers. A crossword and a wordsearch focusing on the key themes and definitions.

Certificates

After completion of the activities and the game you can download a certificate to give to children.

Leaderboard

There is a leaderboard that can be used in your setting so that you can record scores and see who is able to answer the most questions!

Secret code
Within the game there is an additional character, Nano, which children need a secret code for to unlock. The secret codes are hidden in the following activities:

- Activity 2b & 2c: Updating devices (practitioners notes)
- The crossword
- The wordsearch

Each of the codes are different, the code in the updating devices activity is morse code so children need to enter the following:

-. .- -. --- (this is Nano in morse code)

This code should be given to children who win the Updating your phone game.
Morse code was invented by Samuel Morse in the 19th century as a way of sending signal messages via telegraph. It is a code where each letter is made up of a specific sequence of dots and dashes. It is a type of international communication. All sorts of codes are used to write the computer programmes and apps you use every day, they are like types of languages.

In the crossword **Enigma** is the secret code you can find to access the Nano character.

The Enigma machine was used in WWII by German intelligence services to send encrypted messages to the front line and the chain of command. During WWII, mathematicians based at Bletchley Park, working for the predecessor of GCHQ, were able to find a way of decrypting these highly sensitive messages and relaying useful intelligence to the British Armed Forces.

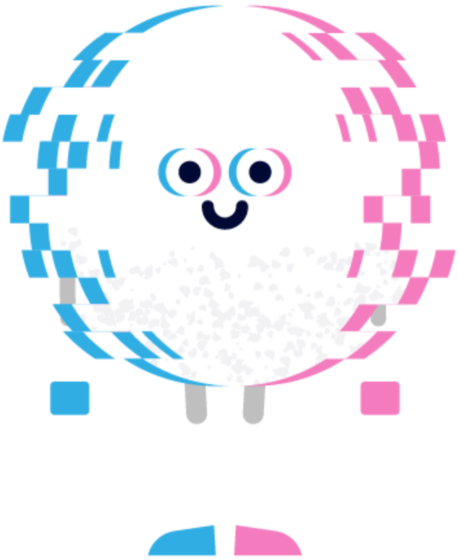
In the wordsearch the children can find another code to unlock the Nano character. Starting with the number of words to find (12) x 100 – 50 = **1150**

The CyberSprinters game

CyberSprinters is an online game which can be found here: www.ncsc.gov.uk/cybersprinters
It can be played on phones, tablets and desktop, or it can be played on a whiteboard.

As a CyberSprinter, children race against their depleting battery to collect cyberspheres and score points. They boost power by collecting padlocks and correctly answering a question on staying cyber secure. If they bump into battery-sucking cybervillains, they face a mini game with a different internet lesson to win back their power.

Meet the Characters



This is Glitch

I move left and right faster than Encryptor….But I use more battery power!

This is Encryptor

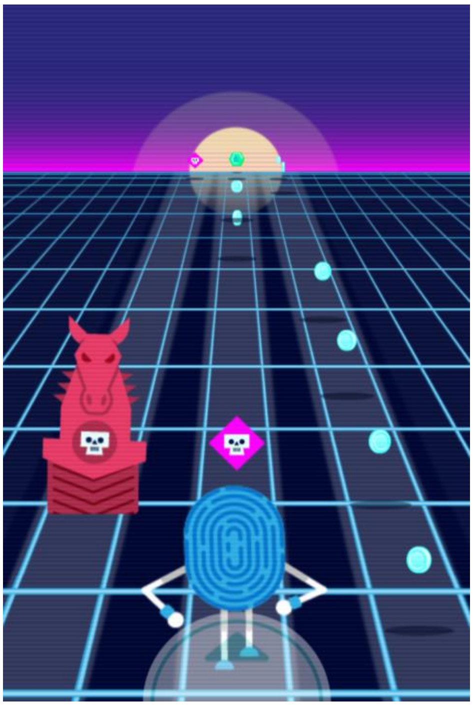
I can run for ages and my battery power lasts a long time!

This is Nano

I'm the quickest, coolest and best! But to be me you need a secret code! Psst….you can't play as me yet until we release the secret code

There are several ways in which children can access the code to play Nano highlighted in the section above. They feature in the unlock your phone game, the wordsearch and the crossword.

As you run through cyberspace with your selected character you try to get the best possible score that you can and avoid the baddies!



The baddies – Hacker; Clone and Trojan will try and steal your battery power as you run through, so you are presented with a series of mini games to protect it if you hit them – Randomiser; Tap Out; Lock the Gate and The Cloud. These games challenge children to a series of questions or tasks that relate to the main themes of passwords, updating devices and suspicious contact.

The game gets faster and children aim to score as high as possible! There is a template leaderboard provided so that you can record the children's scores.

FAQ's

Below is a series of FAQ's to help you understand the issues related to cyber security.

- ***Why is it so important that devices are kept up to date?***
  Cyber criminals use weaknesses in software and apps to attack your devices and steal your identity. Software and app updates are designed to fix weaknesses whenever they are found and installing them as soon as possible will keep your devices more secure.

- ***Why has the password advice changed?***
  Passwords are a gateway to all of your accounts and devices so it is crucial that they are kept secure and up to date. It is essential that passwords are made less predictable so that data can be protected. NCSC promote the use of three random words as a way to create strong and memorable passwords. This ensures that there is novelty and that it isn't too short, making it harder to guess or crack using hacking methods such as dictionary attacks, while at the same time it is much easier for the user to remember than a sequence of letters, numbers and symbols.

- ***Why are children at this age being taught about email security when they only have a school email?***
  Many children are given a school email account or use an email account that has been set up by their parent/carer. However as children get older they are required to use an email account to set up gaming accounts and social media accounts, perhaps begin online shopping. This is about preparing them, and helping them understand that email security is a priority, because these accounts are a gateway and cyber criminals can hack into email accounts and find out lots of personal information, and gain access to other associated accounts.

- ***Why have the NCSC developed these resources?***
  NCSC conducted a review of the available resources to support children in developing their personal cyber security skills. Whilst there were some resources available there was nothing that focused on developing children's personal cyber security skills and the NCSC wanted to support children in developing their skills and understanding to help keep them cyber secure in the future.

- ***What do if I do if the children don't have access?***
  The activities have been designed to be used offline and don't require any access. They cover a lot of the same information. If children do not have access in the setting that you are in they can play the game on a variety of devices or they could always ask their teacher to show them at school.

- ***Can I deliver the sessions without a whiteboard and or wifi access?***
  Yes as mentioned above the offline activities still cover the key learning points so the children can still learn the key messages.

- ***Will the NCSC be developing resources for older children?***
  The NCSC plan to develop another set of resources for 11-14 year olds. The intent is for these to be launched in the autumn.

- ***How will the programme be evaluated?***
  If you are happy to participate in some evaluation via a feedback form, we plan to run this in a few months' time and would really appreciate your input. You can register interest via the link at the bottom of the CyberSprinters webpage

(www.ncsc.gov.uk/cybersprinters), and of course opt out in the future should you change your mind.

- ***Is the NCSC collecting any data from children?***
  NCSC is committed to protecting privacy and will not collect any personal data or use cookies to collect personally identifiable information about users of the game.

- ***Can this be used in all of the 4 nations?***
  The activities and the game have been developed to apply across all of the four nations. Each of the administrations have provided curriculum links detailed below.

For more general information about cyber security please visit
https://www.ncsc.gov.uk/cyberaware
https://www.ncsc.gov.uk/section/information-for/individuals-families

Curriculum mapping

All of the resources have been developed to be flexible and to support delivery of learning objectives within the respective curricula across the four nations. Specifically the resources support teaching in ICT, Computing and PSHE.

As well as the specific areas of the curriculum this resource also maps to the UK Council for Internet Safety (UKCIS) Education for a Connected World framework https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896323/UKCIS_Education_for_a_Connected_World_.pdf

As the respective curricula differs across the four nations each of the education authorities has highlighted the key links in their respective curricula.

Northern Ireland

Key age ranges:

Key Stage 1: 6-8 year olds;
Key Stage 2: 9-11 year olds

Supports aspects of the Cross-Curricular Skill of **Using ICT** and the Area of Learning of **PD&MU** (Personal Development & Mutual Understanding)

How does CyberSprinters support learning outcomes:

Online Communication is one aspect of the learning that happens within **Using ICT**. Online Communication is where children work together online using digital tools to communicate, collect and share ideas to complete a task or create something new. Underpinning this is the need for children to be aware of e-safety practices, including cyber-security such as:

- understanding the need to keep personal information and passwords private;
- recognising the need for a secure password;
- knowing that if they share information online it leaves a digital footprint or trail;

In **PD&MU**, online safety and cyber security awareness is reflected in the following Curriculum requirements:
At KS1, teachers will enable children to develop knowledge, understanding and skills in Personal Understanding and Health, including developing strategies for keeping themselves safe. In KS2 this expands to develop knowledge, understanding and skills in sustaining wellbeing and coping safely and efficiently with their environment.

Scotland

Key age ranges
These resources support the year groups P3 – P7

How does CyberSprinters support learning outcomes:

The Cyber Sprinters aligns to the Scottish curriculum through Digital Literacy under the curriculum organiser of Cyber Resilience and Internet safety at Second level and third level

Second level experience and outcomes

can explore online communities demonstrating an understanding of responsible digital behaviour and I'm aware of how to keep myself safe and secure.
TCH 2-03a

Third level experience and outcomes
can keep myself safe and secure in online environments and I am aware of the importance and consequences of doing this for myself and others.
TCH 3-03a

Whether the learners are playing the game or practitioners are delivering the learning actives that accompany the game these will help leaners gain the knowledge to keep themselves safe and secure in an online environment.

England

Key age ranges:

The materials are intended to be used with pupils in year groups 4 to 6, or the age ranges of 7 to 11.

How does CyberSprinters support learning outcomes:

This links specifically to the computing programme of study (PoS) learning aims for pupils in Key Stage 2 regarding information technology and digital literacy, namely pupils' use of technology safely, respectfully and responsibility.

As outlined in the PoS, pupils should be able to recognise acceptable/unacceptable behaviour and identify a range of ways to report concerns about content and contact.

The materials also have strong links with the Education For A Connected World framework, specifically copyright and ownership, self-image and identity, managing online information, online relationships and reputation.

Wales

Key ages ranges:
7-11 year olds (Key Stage 2)

In addition to the Digital Competency Framework, these resources support schools in embedding digital competence across all areas of learning. These resources can also be introduced as part of the Health and Well-being Area of Learning and Experience.

How does CyberSprinters support learning outcomes:

Digital competence is the set of skills, knowledge and attitudes that enable the confident, creative and critical use of technologies and systems. It is essential for learners if they are to be informed, capable and have the potential to be successful in today's society. The foundations of digital competence are built on learners safety and security which includes online security practices for example:

- understanding the differences between private and personal information

- identifying strategies for protecting personal data and hardware, *e.g.* using secure passwords
- understanding how to protect themselves from online identity theft and scams, *e.g. identifying secure sites, phishing*

Health and Well-being
Safe behaviour in the digital and online world can also be introduced as part of the Health and Wellbeing Area of Learning and Experience (AoLE). Prior to the new curriculum requirements coming into effect, delivery could also be through Personal and Social Education (PSE) lessons.

Information for parents and carers

Below is a set of information that you might want to share with parents/carers and also a link to the activities that children can do at home you can find more information at https://www.ncsc.gov.uk/section/information-for/individuals-families

NCSC have developed a range of resources that you might find useful to share with parents and carers based on a range of topics including:

- Protecting devices from viruses and malware
- Phishing attacks and dealing with suspicious emails
- Using passwords to protect your devices and data
- Sextortion emails; how to protect yourself
- A guide to recovering your online accounts
- Buying and selling second-hand devices
- Data breaches guidance for individuals and families
- A glossary of terms

Available here: https://www.ncsc.gov.uk/information/infographics-ncsc#section_1