

Cookies on GOV.UK

We use some essential cookies to make this website work.

We'd like to set additional cookies to understand how you use GOV.UK, remember your settings and improve government services.

We also use cookies set by other sites to help us deliver content from their services.

[Accept additional cookies](#)

[Reject additional cookies](#)

[View cookies](#)

 **GOV.UK**

▼ Topics

▼ Government activity



[Home](#) > [Government](#) > [Cyber security](#) > [Mapping informal cyber security initiatives for young people aged 5-19](#)



[Department for
Digital, Culture,
Media & Sport](#)

Research and analysis

Mapping informal cyber security initiatives for young people aged 5-19

Published 21 July 2022

Contents

[Executive summary](#)

- [1. Introduction](#)
- [2. The landscape of current initiatives](#)
- [3. What are initiatives doing?](#)
- [4. Current engagement with cyber security initiatives – results from an online survey with parents and young people](#)
- [5. Conclusion](#)

[Appendix 1: survey sample](#)

[Appendix 2: list of interventions](#)

 [Print this page](#)

Executive summary

Across the UK, there is a clear need for a larger proportion of the population to have sufficient cyber security skills. One strategy from the Department for Digital, Culture, Media and Sport (DCMS) is to ensure there are initiatives and educational opportunities available that encourage children and young people's awareness of and engagement with cyber security. However, there is currently no accurate picture of what programmes exist.

This research aimed to provide a first mapping of informal cyber security-related initiatives aimed at children and young people aged 5-19.

A multimethod approach was taken, including: systematic desk research; 13 interviews with experts and oversight bodies; a survey of parents and young people aged 14-18 to understand awareness, perception and participation in initiatives (n=862 young people and n=862 parents); 26 interviews with initiatives across 8 regions, [\[footnote 1\]](#) and interviews with end users to understand their experience of initiatives.

We found 72 overarching initiatives across the UK. This excludes programmes that are exclusively funded and run by the UK government. The subset of 26 initiatives we interviewed reached approximately 230,000 young people per year. [\[footnote 2\]](#) This total number represents around 2% of the population of young people

aged 5-19 in the UK.^[footnote 3] Some other key features of the landscape are:

- most initiatives were targeting ages 10-14
- most were running sessions face-to-face in small groups (10-15 participants) and were free for end users
- initiatives ranged from general technology to cyber security-focused content. From the 26 we interviewed, 9 were focused on technology, 14 in computer science and 14 in cyber security^[footnote 4]
- most initiatives were funded by private businesses, and many were a hybrid between being supported by businesses and the government or local authorities
- it was unclear how initiatives were measuring success, and it was difficult to assess their effectiveness

Experts and initiatives agreed that cyber security can come across as very technical and that jargon can put young people off. Initiatives were promoting themselves in a way to counter this perception by focusing on fun activities and linking in with topics young people are interested in.

Programme designers felt the following approaches were effective in engaging young people:

- connecting cyber security activities to the ‘real world’
- taking young people out of the school environment
- fostering interactions between young people and professionals working in the industry
- tailoring the content and activities for different age groups
- inviting speakers young people can relate to or look up to
- making space for physical play and exploration of curiosity

There was little evidence of networking, signposting or learnings being shared between initiatives. Some initiatives talked about needing a concise strategy in their area, wanting to learn from other initiatives, or knowing where else they could refer their students to when they had finished their current programme.

Four outcomes should be met to support young people into a career in cyber security. Initiatives seemed to be trying to achieve four distinct outcomes: to develop awareness, inspiration, affinity, and knowledge and skills. Even though the activities initiatives were carrying out might only meet one or some of these outcomes, all of these outcomes need to be met at some point in a young person’s journey to move into a career in cyber security.

These outcomes were consolidated into a framework, and could be seen in terms of a journey:

Figure 1: Outcomes targeted by initiatives



This framework may prove useful in prompting initiatives to further define their objectives or for future analysis of initiatives.

Experts and organisations reflected there is a risk in focusing on cyber security too early. They felt that young people could be put off cyber security before they have had a chance to understand what is involved – which may prevent them from engaging with it at a later date. They expressed it would be beneficial to move from a broader ‘tech’ perspective to introducing cyber security later as young people specialise, as is the case in other disciplines such as medicine.

When looking at the subset of 26 initiatives, this did not seem to be the case. Programmes did not seem to focus more on cyber security as the age of the young people they served increased.

In the subset of 26 initiatives, although awareness, inspiration and affinity were covered, more initiatives explicitly focused on developing knowledge and skills.

From this point of view, it could be said that although various programmes with a wide offer for young people exist, they may not be concentrating on the right topic or outcome at the right time – or in the right order.

1. Introduction

Background and research objectives

Mapping informal cyber security-related initiatives aimed at children & young people aged 5-19

As one of the leading digital nations, and with a further reliance on digital networks and systems since the Covid-19 pandemic (for both personal and business use), there is a clear need for a larger proportion of the UK population to have sufficient cyber security skills.

Not only is the increase of digital skills essential for our safety, but basic digital skills are vital to propelling and enhancing the workforce to help companies work more efficiently, securely and in a cost-effective way.

The Department for Digital, Culture, Media and Sport (DCMS) works with partners across government and industry to develop a sustainable talent pipeline that meets the skills demand both now and in the future. This includes a programme of initiatives and educational opportunities that encourage children and young people's awareness of and engagement with cyber security.

These programmes have proven popular, but there is currently no accurate picture of what exists or of planned developments for cyber security skills programmes for the youth sector by the wealth of players involved at national, regional and local levels.

This research aimed to fill this gap and provide a first mapping of informal cyber security-related initiatives aimed at children & young people aged 5-19.

It aimed to map characteristics of these initiatives, including geography, cost, format and channel, as well as explore what techniques and approaches are being used to engage young people.

Methodology

To answer the above research objectives, a multi-method approach was taken.

Phase 1 of the project involved developing a broad overview of the sector and scoping out initiatives that exist in this space, as well as child and parent engagement with initiatives. It consisted of:

- systematic desk research to identify relevant initiatives
- 13 interviews with experts and oversight bodies in this space to fill in gaps in knowledge from desk research and get a sense of good practice from their perspective
- a survey of parents and young people (aged 14-18) to understand awareness, perception and participation in initiatives, n=862 young people and n=862 parents

Phase 2 of the project involved focusing on selected geographical areas to understand characteristics and the operation of selected initiatives in more detail. It consisted of:

- 26 interviews with initiatives [\[footnote 5\]](#)
- shadowing events and gathering resources used by initiatives
- interviews with end users to understand their experience of initiatives

The 8 geographical areas were decided based on conversations with DCMS to include areas with different demographics, levels of socio-economic diversity and activity around cyber security. These regions were Belfast, South Wales, Edinburgh, London, Cornwall (focusing on Plymouth), West Midlands, Yorkshire (focusing on Bradford), and initiatives that had nationwide reach.

Limitations relating to the 'landscape map' of programmes

This research represents the best available mapping of the current landscape of cyber security initiatives and goes some way to understanding what exists, but it is unlikely to be a complete picture. It should be noted that:

- not all data the research team wanted to capture was publicly available – so there are some gaps in knowledge
- it was decided that 8 geographical areas would be focused on to give some boundaries to scoping activities – so it is likely there are other initiatives that aren't captured
- more information was recorded on the initiatives that were interviewed in-depth

- some conclusions are drawn from the data the research team gathered on all initiatives identified across the UK, but some are drawn from data on the subset of 26 initiatives that were interviewed in more depth (this is clearly marked where relevant — these numbers may not fully represent the full picture of the cyber security landscape)
- from the survey conducted as part of this research, we know that young people may participate in more than one informal initiative (however, initiatives interviewed were not able to account for potential overlap in their 'reach' data, all of which assumes unique participants)

The above considerations should be taken into account when reflecting on the data set out in this report.

2. The landscape of current initiatives

The first research activity involved mapping the current informal learning opportunities in cyber security skills available across the UK. We focused on collecting evidence from desk research and interviewing stakeholders from the sector.

Overall, we found 72 overarching initiatives across the UK^[footnote 6]

We focused on initiatives that are not exclusively funded by the government, and we broadened our search to include initiatives that included tech or computer science rather than limiting the scope to cyber security-only initiatives.

We looked into specific details about the format and delivery of these programmes. However there are gaps in the data we have been able to collect, which limited the calculations we were able to make. For example, not all data was publicly available and some of the attempts to get in touch with the initiatives were unsuccessful.

As a result, some overall conclusions are drawn from the data we have from all programmes we have found when scoping or from the initiatives we could talk to in more detail. But it might mean that the numbers do not represent the full picture of the cyber security landscape.

For example, it was sometimes unclear which initiatives were active. Covid-19 impacted the continuity of some programmes too. Three out of 26 initiatives we spoke to had been paused since the pandemic, but was not possible to know this for some initiatives by only looking at the websites. From trying to contact initiatives to speak with, many were unresponsive, which could be an indication that they were no longer active.

The subset of 26 initiatives we spoke to reached approximately 230,000 young people per year

Reach calculations were done taking into account the size of the groups or courses they run, their duration and number of times they run per year. We assumed that these are unique participants, that the group sizes are consistent, and they run the programmes in the frequency that they told us.^[footnote 7] We estimated the cumulative reach of these 26 initiatives to be approximately 230,000 young people per year, which is equivalent to around 2% of the population of young people aged 5-19 in the UK.^[footnote 8]

Based on our desk research, we believe 64 initiatives to be active. However, we understand the 26 initiatives interviewed to be the larger active initiatives, based on their visibility – how well advertised and well known they are – and the reach figures they were able to provide. As such, we do not believe it would be accurate to assume the 38 initiatives we did not interview have equal reach to the 26 engaged. To ensure we are not over-claiming potential annual reach, therefore, we are conservatively

estimating that the remaining 38 smaller initiatives have a reach of approximately half that of the larger, higher profile initiatives we interviewed (average of ~4,400 rather than ~8,800). Based on this assumption, we believe a reasonable estimate for the reach of all 64 active initiatives would be approximately 400,000+ per year (230,000 from the 26; ~170,000 from the remaining 38). This represents approximately 3.4% of the population of young people aged 5-19 in the UK.

In the survey we conducted as part of this research, 17% of all 12–18-year-olds surveyed reported having ‘ever’ (i.e. at any time in the past) participated in an informal cybersecurity-related programme. This is broadly consistent with our estimated annual reach of between 2-4% of young people potentially participating in cyber security initiatives per year.

How this looks across different geographical areas is set out below.

Table 1: Number of programmes and their reach per geographical area
[\[footnote 9\]](#)

Area	Number of programmes interviewed	Estimated annual reach of programmes interviewed
South Wales	6 (including several Code Clubs, Technocamps, NDEC, Code week)	~11,000 young people out of a population of 540,436 (in Wales as a whole)
Belfast	4 (Coder Dojo, Code Club NI, NI Cyber Gateway programme, Bring IT On)	~28,000 young people out of a population of 366,759
London	3 (MAMA Codes, Software Academy, Cyber Choices*)	~2,500 young people out of a population of 1,631,542*
Plymouth, Cornwall	2 (Bluescreen IT, TECGirls*)	~15 young people out of a population of 46,149 [footnote 10]
Edinburgh	2 (Young Scot* , Prewired*)	Unknown
West Midlands	1 (Digital Innovators)	~200 young people out of a population of 1,094,549
Bradford, Yorkshire	1 (Computer Xplorers*)	Unknown
Nationwide programmes [footnote 11]	7 (Exa Foundation – Raspberry Jam/Family Hack Jam, STEMettes, Digital Skills Education/Cyber Skills Live, FireTech, Qufaro, Career colleges, Cyber hub trust)	~194,000 young people out of a population of 10,090,908

Most initiatives were targeting ages 10-14

Across the 72 programmes, the ages targeted the most appeared to be 11 and 12,

with late primary and early secondary students having the most exposure to some initiatives. This engagement trails off slightly later in their educational journeys and slightly increases again at around age 16. As young people are deciding A Levels and potential careers, initiatives try to re-engage young people at this stage.

However, because this calculation is based on data from the list of 72 programmes, it leaves out ones where we are unsure of their target audience. Additionally, this doesn't account for reach and impact, therefore this information only indicates which ages most initiatives supposedly cater for, as opposed to the ages and groups that are receiving more teaching.

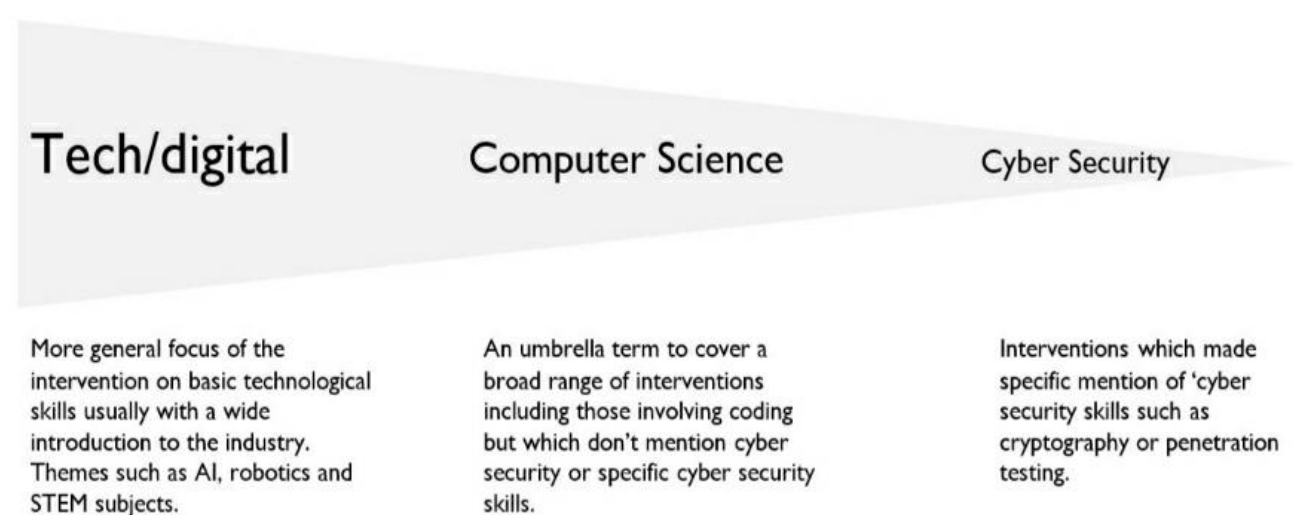
If we look at the reach of the subset of the 26 programmes we spoke to by age, it appears that the 10-14 age group is also the group that is being targeted the most.

Initiatives ranged from general tech to cyber security-focused content

As mentioned above, initiatives that weren't solely 'cyber security' were also included during scoping, as we noticed that some included certain disciplines related to cyber security. Some programmes had intentionally focused their initiatives towards general tech instead of specific cyber security as an entry level for younger people.

We categorised these disciplines as tech/digital, computer science and cyber security. There is a slight overlap in the definitions – and some programmes were targeting more than one of these disciplines, particularly when they had different activities or courses and each had a different focus.

Figure 2: Type of content initiatives were focusing on



From the programmes we scoped, 27 covered tech content, 45 computer science and 30 cyber security.^[footnote 12] From the 26 we interviewed, 9 were focused on technology, 13 in computer science and 14 in cyber security.^[footnote 13]

Initiatives were often run by businesses

Most initiatives were funded by private businesses. However, many initiatives were a hybrid between being supported by businesses and the government or local authorities. Charity-funded programmes also appeared within the landscape, although these were sometimes sponsored by a business. For a few programmes, it was unclear how they were funded or how they were operating.

Figure 3: How initiatives were funded (where known)^[footnote 14]

Scoped initiatives

Local Authority 3

Hybrid 5

Charity 20

Private business 36

Interviewed initiatives

Other 2

Hybrid 5

Private business 9

Charity 11

These initiatives often ran in small groups and face-to-face

The format and delivery of sessions varied across initiatives, and some were using more than one format. Most organisations ran their sessions in small groups, and face-to-face – with many running a hybrid model since the pandemic. Small groups were usually comprised of around 10-15 participants.

Out of these smaller initiatives, many would have at least one event throughout the year targeted at larger groups of young people.

Figure 4: How initiatives were delivered [\[footnote 15\]](#)



In line with the trend of a face-to-face format, after school clubs were the most popular format for the programmes recorded in scoping. Those who were self-directed were usually providing online resources or immersive labs that young people could complete at their own pace. Only a handful of initiatives were offering apprenticeships or work experience.

The duration of these programmes varied considerably. The most common format was regular/ongoing sessions (i.e. weekly, fortnightly, monthly), and one-off activities

– the latter due to the large events most organisations would offer at some point during the year.

On the other hand, a few organisations had options for intensive courses during school breaks or longer holidays.

Most of the initiatives were free for end users[\[footnote 16\]](#)

Approximately 60% of the initiatives are free for end-users. From those who charge money to their users, prices ranged from £11 per hour to £500+ per week for an intensive course. The cost rate was sometimes presented per hour or class, for the duration of the course (a few months, school term).

Measures of success were uncommon among programmes

For most programmes, it was unclear how they were measuring success. Even among those we spoke to in more detail, we didn't find any formal evaluations of programmes. Some had indicators of success, mainly via attendance to sessions or completion rates. Some asked for verbal feedback from schools that they work with about how students were performing at school or behaviours that had changed since taking part in their activities.

Not many initiatives track young people to see if they go into formal education routes. For most of them, feeding into education pathways is not one of their focuses (see next section). Therefore, it is hard to assess which initiatives are working better than others in motivating young people to follow a career in cyber security.

3. What are initiatives doing?

What topics and outcomes are initiatives focusing on?

Experts felt the learning pathway should follow a journey from 'broader tech' to 'cyber security' as children got older – but this was not the case in practice

Some experts and organisations reflected that it would be beneficial to move from a broader 'tech' perspective to introducing cyber security later as young people specialise. In other disciplines, such as engineering or medicine, we do not expect young people to specialise early in their educational pathways but instead provide a broader foundation of skills that will enable them to specialise later on.

“ There's a desire to get kids to choose cyber security early, but we don't do that in any other type of subject, like medicine.”

“ When they have the general skills, all you have to do is change the focus.”

Experts also felt that 'cyber security' is not always a term that means something to young people – they may come up with their own assumptions about what cyber security could mean which may or may not be accurate. There is a risk therefore that young people could be put off cyber security before they have had a chance to understand what is involved.

“ People don't understand the jargon and are scared of the industry as a whole, so we need to break that down and teach the basics.”

“ I think ‘hacking’ has this perception that it’s only for people who have committed some kind of crime, as opposed to a career. So they haven’t even realised [ethical hacking] can be a career.”

Taking this thinking forward, if we broke the initiatives identified in this study down into the three disciplines, we could expect that at the younger ages programmes would be more heavily driven towards technology, then developing through computer science and then to cyber security as we reach the higher age ranges.

In reality it is much more of a mixed picture. There was little pattern found in the initiatives.

A framework was developed to help describe the different outcomes initiatives were trying to meet

When they talked about what they were trying to achieve, initiatives stated that they had a range of different aims and desired outcomes.

This range included:

- trying to support young people to develop tech or cyber security-related skills earlier on in their lives
- inspiring young people to feel enthusiastic about the topic area of tech or cyber security
- making young people aware of what it is like to work in tech and cyber security
- attracting more diverse audiences to the field of tech and cyber security

Initiatives did not always have a clear language to talk about what they were trying to achieve, but from what initiatives said, there appeared to be four distinct outcomes for end-users of initiatives, as outline in the figure below.

Figure 5: Outcomes initiatives were targeting

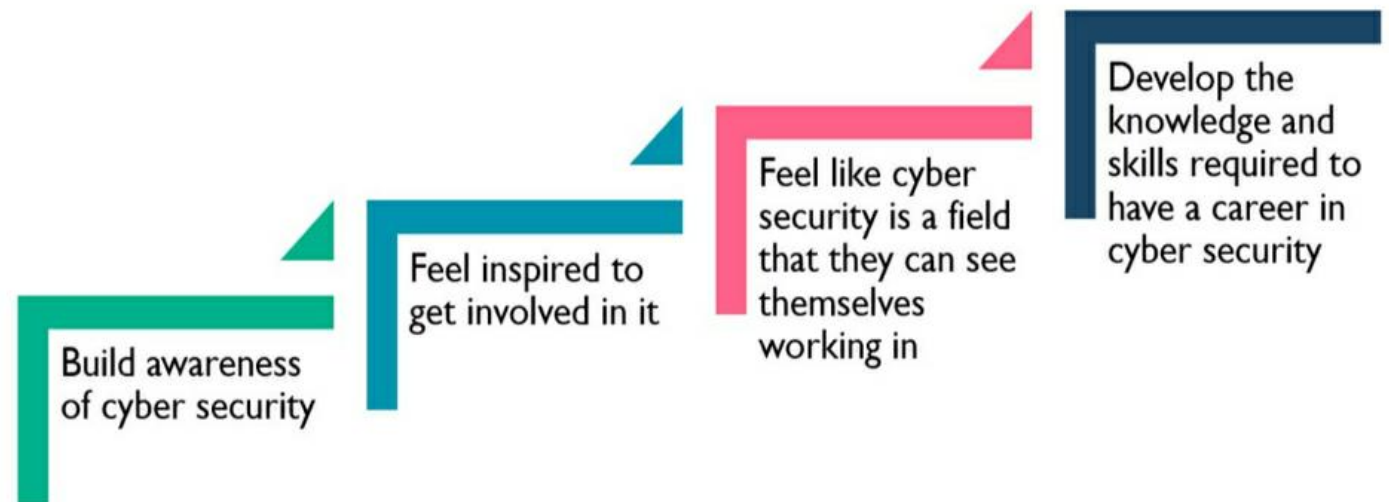


All these outcomes should be met to support young people to move into a career in cyber security

The activities that initiatives were carrying out might meet only one or several of these outcomes – but all of these outcomes need to be met at some point in a young person’s journey in order for them to move into a career in cyber security.

These outcomes could be seen in terms of a journey:

Figure 6: Outcomes initiatives were targeting along a journey



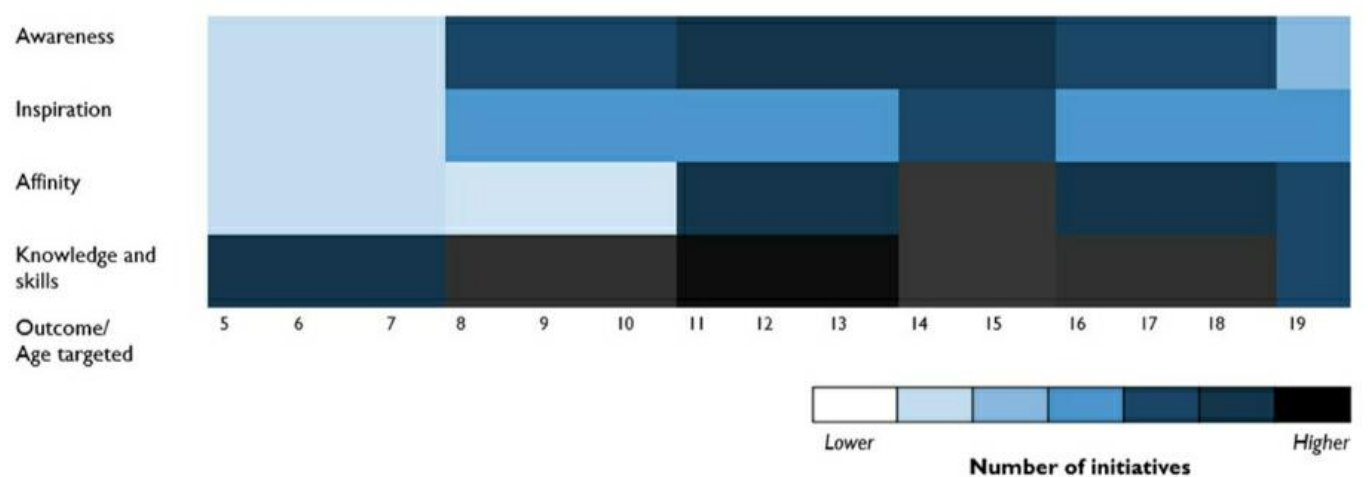
We could expect initiatives to initially aim at increasing awareness, building on this to inspire and create affinity. Once all three have been achieved the initiatives would then teach the necessary skills and knowledge. So we might expect to see more awareness-focused activities at young ages and more skills-focused activities at older ages.

Instead, it was a much more mixed picture.

Although various programmes exist, they may not be concentrating on the right outcome at the right time

When looking at the subset of 26 initiatives, more initiatives focused on developing knowledge and skills.

Figure 7: Heat map showing outcomes initiatives were targeting across age groups.



The figure above demonstrates the concentration of programmes, across ages and the four outcomes. There is an obvious darker concentration of initiatives targeting knowledge and skills. Most initiatives were targeting ages eight to eighteen, across all outcomes.

Many stated increasing knowledge and skills as their aim. The other outcomes were being covered in some initiatives – and undoubtedly whilst not explicitly identified, some initiatives were probably meeting other outcomes through activities targeted on skills development.

From this point of view, it could be said that although various initiatives with a wide offer for young people exist, they may not be concentrating on the right outcome at the right time – or in the right order.

Case study: How do these outcomes play out in one programme?

We spoke with an international initiative with a particularly large user base in Scotland, offering online activities and engaging children between the ages of 10-14 in cyber security. They run activities which can either be self-led or conducted in small group sessions.

Awareness - This initiative talks about different roles and courses students can do, and how much they could earn. Talking about careers and roles in cyber security is part of a criteria for this initiative to receive their funding.

Inspiration - The sessions are often linked back to real world scenarios such as the LinkedIn data breach, or the importance of setting up secure web addresses, highlighting the importance of tech and protecting the digital world. The organisation finds huge benefit in basing the activities around fun and exciting sounding topics, and using eye catching titles to gain children's attention.

Affinity - The initiative will often have speakers of different backgrounds and genders who work in cyber security industry attending the sessions. This enables the children to have a variety of role models and individuals to look up to and aspire to be. The avatars available during the online sessions are also representative of a variety of backgrounds.

Knowledge & Skills - The sessions teach processes which replicate those which would be used in real-life. The students are able to work through activities related to penetration testing, digital forensics, and ethical hacking in simulator style environments.

What activities are initiatives carrying out to meet these outcomes?

Initiatives were addressing each of these outcomes in a variety of ways. In this section we set out some common approaches that programmes were taking.

Because of the lack of evaluation data, it was hard to say which approaches were more effective in leading to better outcomes for young people. The following points reflect trends that were observed and which the initiative designers felt were most effective for young people.

Connecting cyber security activities to the 'real world'

Programmes offered activities or projects that young people could relate with real life

situations, and platforms with which they were already familiar – for example, simulating a hacking attempt so that young people could identify what was not working well and how it could be fixed.

Many coding clubs would include pathways about game design and programming that could show children how to programme for the particular actions they wanted to happen with each movement. This was aimed at moving young people from a passive use of technology to a more active one. As an example, an initiative talked about how they wanted to teach young people who liked gaming how the specific actions they could see were designed, which software was being used and how it worked.

Others were trying to solve problems that were occurring in real life, bringing the sessions to life. For example, simulations around stealing data based on incidents that happened in real life.

These types of activities were aimed at not only teaching new skills and processes, but at showing young people how important or useful training in cyber security could be. Many initiatives went further to show them the kind of jobs they could be doing in the future. Some people we spoke to mentioned that only when students had real experiences of what it is like to work in cyber security, did they consider pursuing a career in the sector.

“ In Digital Technology at GCSE, we learned about the names of the programmes of the malware and the viruses, and we learned about what they are and how they do it, but I never actually had a look, and was never shown what it actually looks like. But I was [when I went along to the initiative]. So it opened my eyes to that.”

(End user, 17, Northern Ireland)

“ They need to come up with digital solutions to real world problems.”

(Initiative, Nationwide)

This strategy was targeting Inspiration, Affinity and Knowledge & Skills.

Taking young people out of the school environment

Some initiatives were addressing outcomes such as inspiration and affinity by taking young people to company sites or universities. Initiatives wanted to make the experience more fun and memorable than being in a school environment.

Some initiatives mentioned this was very important as it was evident that some teachers lacked the digital skills they were trying to foster in young people, and so there was a risk that teachers, lacking confidence, could make the topic sound complicated or uninteresting.

A few programmes emphasised the importance of a change of scenery, not only to make it more engaging, but also as a more effective way of showing children the space they could work in. Particularly for underserved groups, this was an opportunity to bring them closer to this world and to visualise the kind of environment they could work in.

“ The kids don't think university or careers are for them. So, we bring them to the space to inspire them... We've found that most impactful.”

(Initiative, Wales)

End users, particularly girls, talked about having a great experience while on competitions outside school. Several end users from Northern Ireland we spoke to had participated in competitions. An end user in Wales talked about how the younger girls she had mentored won a competition and how satisfied she was to have pushed the school to apply.

Even though the competitions were sometimes during weekends, one end user we talked to was happy they took part and said they would do it again as it is something different and it was a fun experience.

“ Actually doing some courses or going to some talks or competitions, you can see how you might take that leap from the theory on computer science to applications of computer science.”

(End user, 18, Wales)

“ I just thought ICT [information communication technology] and technology was just a class you took at school. But I realised it's a much wider broader term.”

(End user, 13, Northern Ireland)

This strategy was targeting Inspiration and Affinity.

Interacting with people working in the industry

Many initiatives were raising young people's awareness of the type of jobs they could do in cyber security, by providing opportunities to interact with people who work in tech. For example, some organisations had guest speakers who were professionals in the field, sharing what a workday looks like for them. Different initiatives talked about how important it is to demystify what type of activities a tech or cyber security role involves, showing that it can be more diverse than what people think.

“ We talk about the different careers in cyber security and we show them they don't have to be a coder... They can be from an account manager to a solutions architect, so we bring different people doing these different jobs. We include the creatives too, the gamers, the designers, user experiencers, because they are also trained in tech.”

(Initiative, Nationwide)

Some initiatives were sponsored by industry partners who were acting as mentors for young people's projects and would come to the sessions. In some cases, participants would visit the offices these professionals worked in, having exclusive access into real-life work environments.

“ We partnered with a space agency for our programme and the children made some code that linked to a sensor and detected how much moisture there was in the air.”

(Initiative, Wales)

“ The projects are set by people working in the industry, and the kids present back to those people at the end.”

(Initiative, Midlands)

Several end users agreed that interacting with industry partners influenced developing their interest in tech and cyber security. Also, working with industry partners informed them about opportunities to work in tech they weren't aware of before.

“ In GCSE I did digital technology and multimedia, where we learned about cyber security. But nowhere near to the extent that I learned about it in the [programme] workshop...all the people that were teaching us actually work for the company and actually did all this stuff for their jobs, so it gave us a bigger insight.”

(End user, 17, Northern Ireland)

“ You see the inner workings of the company because they have to tell you about what happens in the company to actually design the product.”

(End user, 17, Northern Ireland)

End users talked about how much they liked doing practical learning and doing internships in real companies. For some, this motivated them to pursue a career in the industry.

“ I think ideally I would do an apprenticeship of some sort. I think that's the main thing I'm lacking, because even though I do think universities are valuable, I think a lot of the things you learn through university, you can teach yourself. Whereas getting professional experience working for a company, you can't really do.”

(End user, 16, Northern Ireland)

An end user from England told us that working with a real company specialised in cyber security had changed their perspective on what it was like from their self-teaching.

“ I've always focused on offensive cyber security and never defensive. Before, I would just want to hack things and not actually understand my motive...now I'm setting up networks or adding people to the networks, or hacking a client, which is probably the most fun that you're ever going to have.”

(End user, 15, England)

This strategy was targeting Awareness, Inspiration, and Affinity.

Tailoring the content and activities for different age groups

There were a handful of initiatives who instead of teaching specific skills to specific age groups, would take skills such as cryptography and slowly build that into the activities they were doing with the young people.

One programme in particular would start with children in year 3 and 4 by encouraging non-cyber security activities, e.g., sending secret messages using glow in the dark or water pens. As the children grow older in year 5 and 6, the initiative would invite the local rugby team in their sessions. The team would explain to the children how they send secret messages across the pitch to each other during games. The children would be able to experiment and make up their own signals themselves. It is only when the children get to the end of primary school that the club introduces more 'cyber security' focused activities, using pig pen diagrams to create games and challenges introducing basic cryptography techniques.

This strategy was targeting Inspiration.

Inspiring young people with speakers they can relate to or look up to

The initiatives we spoke to often had guest speakers aimed at presenting role models and positive examples for the children in the clubs to aspire towards. Particularly those programmes targeted at specific target audiences (i.e. girls, disadvantaged groups) would invite speakers of similar gender, characteristics and background who are already working in the industry, so the young people can relate to them more easily.

One club we spoke to ran girls-only networking events, where students were able to interact and ask questions to the women working in the industry. The events would demonstrate to the girls that the career path is both possible and enjoyable for people like them.

We also spoke to an end user who went to a similar tech talk organised around International Women's Day. She said that speaking to women in the industry was hugely encouraging and made her much more comfortable picturing herself in the industry, although she still found the idea of entering the industry very daunting due to the biases and barriers women still face.

“ Female representation in tech is something I've become really passionate about since attending the International Women's Day event in 2021. It is something that is discussed at many of the talks I go to. All of this has helped me become more comfortable with being a minority. We are two girls and six boys in my A Level class and around 20% of the students on the uni courses I have signed up for are girls. It has given me a great support network.” (End user, 18, Wales)”

This strategy was targeting Awareness, Inspiration, and Affinity.

Using physical play and encouraging curiosities

Some clubs were capitalising the fact that children are known to enjoy physical play, by introducing technology and cyber security in more hands-on activities.

“ We use a lot of non- computer-based activities, the kids like tactile things and getting up and moving.”

(Initiative, Nationwide)

“ The very youngest group is very much physical, moving around, acting out algorithms, singing, dancing. Bringing nursery rhymes to life so they sing it, draw it and they animate it.”

(Initiative, London)

Programmes would try and keep the topic 'light', especially in younger age groups,

allowing children to explore their passions and interest in the subject, building their confidence in a safe and fun environment.

“ Tech is about problem solving, learning from your mistakes, and making progress through failure. We need to get more people ‘doing’ and not overthinking it.”

(Initiative, Cornwall)

This strategy was targeting Inspiration.

How are initiatives attracting people?

Initiatives were mainly using connections with schools or social media to reach out to end users

Programmes were using a wide variety of channels to reach out to teachers, parents, and children. This included:

- **Social media.** Initiatives were using platforms such as Instagram and TikTok to reach out to young people. Some were trying to use features of the platforms that are popular with younger people. For example, one initiative was using Instagram Live.
- **Promoting through schools / teachers.** A large number felt that reaching out through schools and teachers was effective and enabled them to reach a large audience.
- **Networks / links with other community groups.** A minority were using connections they had in the community to engage young people. One club was accessing what they felt were underserved groups through their links with the local authority and other leaders in the area.
- **Events / school fairs.** Some were setting up stalls at events and fairs.

Experts indicated that cyber security can come across as very technical – despite many roles in the sector not being technical ones

Experts interviewed as part of the research expressed concern that cyber security can come across as very technical. Often there is complicated jargon associated with cyber security which can put people off, especially if they don't already have an interest in the topic. This was supported by an experience from an end user in Wales, who signed up to receive emails and newsletters from several tech programmes, but appreciated that the language would not be accessible to those who aren't already interested in and knowledgeable about tech.

“ From the perspective of a Year 8 student, you've never seen any of those words before...why would I want to look at digital forensics – it doesn't mean anything to me.”

(End user, 18, Wales)

There was also an indication that cyber security jobs which require very technical skills are actually quite a small proportion of the cyber security sector. For example, roles can be based around sales, governance, human factors and innovation. However, there's little awareness about these types of jobs.

There is a risk that an overfocus on technical roles (e.g. coding) can put many young

people off, resulting in the sector not having the skills balance it needs.

From the survey data it appeared that young people did not think that cyber security came across as technical. This indicates that initiatives were taking this into account when promoting their programmes.

The way initiatives talked about their events varied – but most were trying to avoid making it sound too technical

Naturally, the way programmes were marketed depended on the audience they were trying to attract. Those aiming to develop the skills of young people who are already interested in cyber security were more often using more technical language that might already be familiar to their audience. Those which were trying to inspire new young people to get involved with cyber security were more likely to make their initiatives sound fun and avoid technical concepts.

Some examples of how initiatives framed their programmes are set out below.

Focusing on ‘fun’ – using games and interactive activities

Many initiatives were using activities or displays that emphasised the fun nature of the activities young people could expect to do if they were to join the programme. Showing the type of activities they would do instead of the content they would cover seemed to make it easier for initiatives to explain this too.

“ We sometimes have a stall with circuit boards and Minecraft on it. These function as cues to attract people. There is a slight element of dumbing it down to attract young people.”

(Initiative, Nationwide)

“ We are actually doing activities rather than just being on the stall [at school fairs] – whether it’s a quiz, or showing a simulated example of a hacking attempt...”

(Initiative, South-West England)

Linking in with other topics young people may be interested in

Some initiatives were trying to tap into topics that young people are interested in in their wider life – for example, gaming, design or sustainability. These topics were sometimes decided based on the partners that were funding the programmes. This was a technique to make it easier for young people to see the programme as relatable and useful to them.

“ Our interventions are reactive to the partner who is funding them...we’ve done ones around sustainability, or fashion for example.”

(Initiative, Nationwide)

Similarly, some introductory talks were emphasising how technology and cyber security would be included in any type of industry.

“ One of the things we try is to show them there isn’t a single industry that doesn’t have technology in it these days. So if they think about anything they’re interested in, from sport to health, everybody’s looking for a cyber analyst for example.”

(Initiative, Nationwide)

An end user had been to a talk by a tech professional working for a publishing company and it opened her eyes how the digital skills were transferred to different sectors. This end user felt the speaker was able to combine her own love of books and tech in a way that other more tech-specific initiatives had not done previously. This experience encouraged her to think of the opportunities available in tech outside of the 'usual' bigger tech giants.

“ So that opens up a lot more opportunities that you might not think about. Because if you think about tech, you think about Google and Amazon, your typical big companies, but there are so many opportunities out there.”

(End user, 18, Wales)

In line with using familiar topics, some initiatives were using well-known names and brands to attract young people's attention. They found that including the sponsors or partnerships with brands young people would recognise and admire, proved a useful strategy to attract young people.

“ We've got so many good brands involved... You've got to find names to engage them.”

(Initiative, Nationwide)

Not mentioning 'cyber security' or related technical terms

Some initiatives that were more cyber security-focused than others chose to avoid using the term 'cyber security'. Instead, they emphasised making activities sound fun. Some chose to use phrases such as 'creative digital projects' or framing programmes around the outcome users would be trying to achieve, e.g. 'how to steal a pizza'.

“ One of our sessions is based on the LinkedIn data breach. But if we'd called it something like 'Using Python to explore passwords from a LinkedIn data breach'...nobody would sign up for that.”

(Initiative, Scotland / International)

Testimonials

Programmes were sharing testimonials to attract young people, especially targeting those who might be doubting whether or not they were the 'right' person to get involved in the programme. Some initiatives were combining emphasising the enjoyable nature of the activities and showing the skills they would learn. On occasions, these testimonials were more of an effort to appeal to teachers or parents to sign up.

A few initiatives were using social media platforms to share videos or quotes of students' feedback, sharing what they thought and liked about the programmes.

“ We post a lot about what is the course about and we try to be really transparent about what they're going to learn on the course. Sometimes we ask students to

create a video clip that we can share on social media.”

(Initiative, Nationwide / International)

Including diverse people in marketing materials

Most initiatives wanted to attract a diverse range of end users, and were aware of the poor representation of some groups in tech and cyber security. Some were trying to counter this by using photographs or imagery of a wide range of end users, or even including avatars or characters in their materials. Initiatives were also promoting a range of speakers at events to make it more relatable to young people from different backgrounds.

“ You can pick an avatar that represents you, and we try and use diverse characters in our stories.”

(Initiative, Scotland/International)

Emphasising links to the curriculum

In some nations, initiatives were trying to advertise the links that their programmes had to the school curriculum. This was mainly in an effort to appeal to teachers and parents and to make it feel worthwhile investing time and, potentially, money in.

“ In Wales, digital literacy is now the same level as numeracy and literacy [as they are mandatory cross-curricular skills]. So the clubs link into the curriculum.”

(Initiative, Wales)

“ We try and hit certain key words or touch points with the education system, just so that it has some extra relevance for the teachers, but also the young people have something to kind of link in to what they’re doing in the classroom.”

(Initiative, Scotland/International)

How are initiatives linking together?

Some initiatives expressed interest in building better links with other programmes in their area

Not many initiatives had collaborative relationships with other initiatives. There was little evidence of networking, signposting or learnings being shared between different initiatives.

This disconnection was evident particularly after large events or competitions, where a large number of young people take part and the positive experience generates great interest. However, we heard from both initiatives and end users that there wasn’t always clear signposting of where they could go next. Despite some end users being interested in taking part in further programmes to continue developing the skills they have learned in the competitions, they did not know if there were initiatives available in their area, or where to find out more about them.

In Scotland and Wales, programmes were most likely to signpost young people on to

doing formal qualifications at their schools. Some initiatives have links to apprenticeship programmes or jobs that young people can apply for. Some initiatives were signposting onto programmes like CyberFirst.

Those initiatives who were working with the older cohort of young people were better linked with businesses. For example, partnerships between businesses and initiatives meant they were working together in the design of their programmes to ensure young people were trained in the skills that businesses were finding harder to find. Five initiatives were linked with companies to secure opportunities for apprenticeships and work experiences to their students.

Some initiatives talked about needing a concise strategy in their area, wanting to learn from other initiatives, or knowing where else they could refer their students to when they had finished their current programme.

4. Current engagement with cyber security initiatives – results from an online survey with parents and young people

During phase 1 of the project a survey was conducted with young people and their parents. This survey aimed to:

- Understand broad awareness of ‘cyber security’ and related concepts (e.g. computing) as an area of work or learning.
- Explore perceptions of cyber security and related concepts/areas as a potential career option.
- Understand people’s engagement with informal cyber security initiatives.
- Capture awareness and perceptions relative to other career paths/options.

The online survey was conducted with 862 parents and 862 young people aged between 12 and 18 in February 2022 (n=1,724 people surveyed in total).

Respondents were recruited into the survey via a commercial survey panel consisting of people who complete market and social research surveys in return for an incentive. Children were reached through each parent respondent, who gave permission (where required) for their child to complete the second half of the survey.

Sample for the survey was divided into two child age groups:

- N=431 12–14-year-olds (plus parent/guardian): to learn about a ‘pre-GCSE’ cohort who have opportunities to study subjects related to cyber security such as computer science.
- N=431 15–18-year-olds (plus parent/guardian): to learn about a ‘pre-university’ cohort who are slightly closer to university and starting to think about the world of work.

Having explored the landscape of cyber security and related programmes, the survey presents an opportunity to add useful context from the perspective of children and parents and provide a sense of scale.

It is important to note the survey sample is not perfectly representative of all children in the UK but provides a useful sense of awareness and participation that is indicative of the wider population. The sample included an even split of boys and girls, and a spread across regions, socioeconomic groups, and ethnicity groups.^{[\[footnote 17\]](#)}

While the questionnaire was developed with the intention of being as objective and clear as possible, it is important to note that there will be some level of subjectivity in how people respond to questions. For instance, what is meant by 'I know a little about cyber security' will differ from person to person. Therefore, we are predominantly interested in the relative differences between answers and certain groups in our sample, or whether reported awareness and participation is consistent across factors such as age and gender. Furthermore, it is important to note that in some questions, respondents were permitted to select more than one option. Therefore, the percentages for certain sections may add up to more than 100%.

Engagement with subjects related to cyber security

Fewer young people were studying computer science and ICT compared to maths and physics – with fewer girls studying these subjects compared to boys

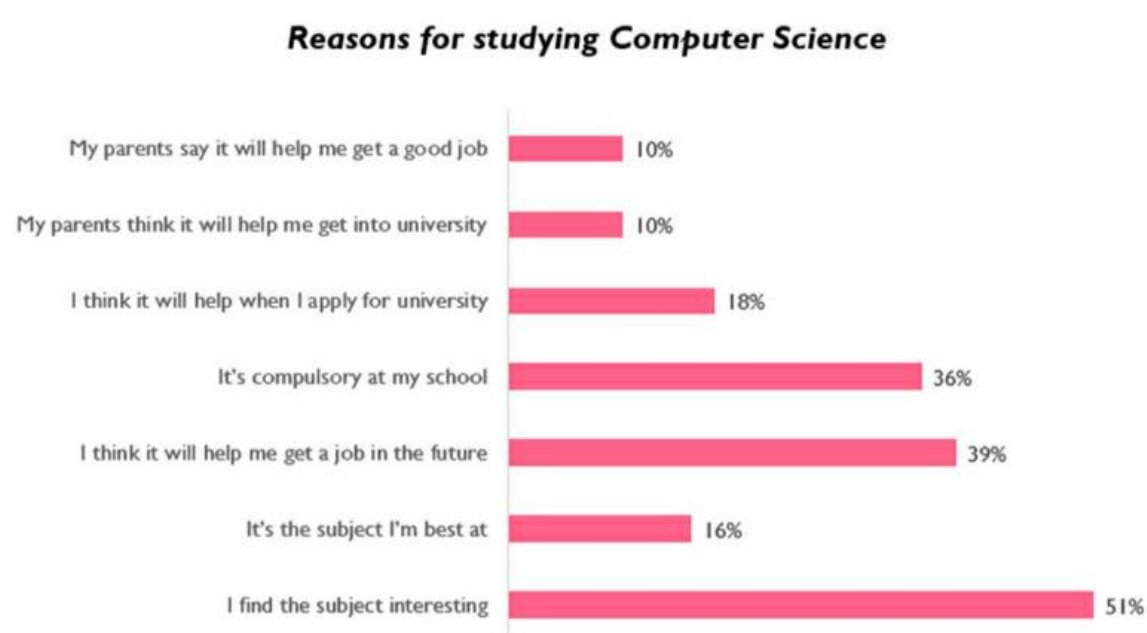
Respondents were asked about key subjects they study at school that relate to cyber security. There were some differences between the older and younger cohort as some subjects are compulsory for younger students.

33% of our sample of young people said that they study ICT. Small gender differences appear here, with 36% of males studying the subject compared to 30% of females. Unsurprisingly the younger cohort were more likely to be studying this than the older cohort (46% compared to 19%), given that the subject may stop being compulsory at older ages.

36% of young people in our sample reported studying Computer Science, but there is a notable gender divide: 42% of boys reported studying the subject, compared to 31% of girls.

Of those studying Computer Science (36% of the total sample), 51% said that they 'find the subject interesting' while 39% said they thought it would help with finding a job in the future. 36% of Computer Science students also said they study it because it is compulsory at their school.

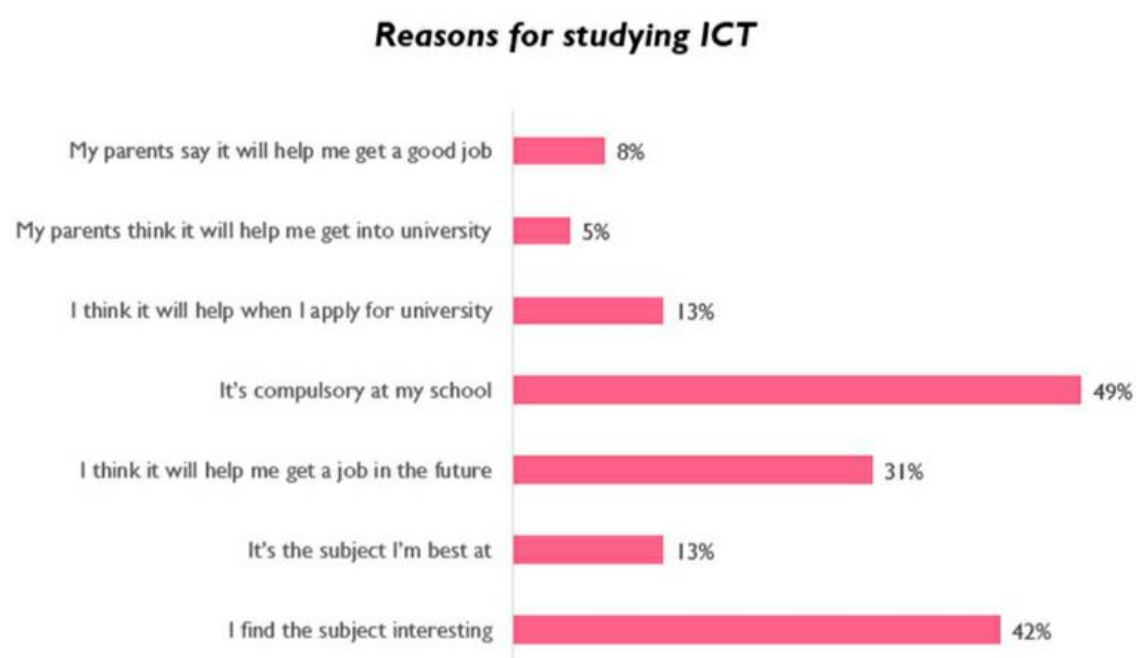
Figure 8: Graphic illustrating young people's reasons for studying computer science



BASE: All young people study computer science, n = 311

Of those studying ICT (284 respondents), 49% said they study it because it is compulsory at their school. 42% said that they 'find the subject interesting' while 31% said they thought it would help with finding a job in the future.

Figure 9: Graphic illustrating young people's reasons for studying ICT^[footnote 18]



BASE: All young people study ICT, n = 284

Physics was studied by 47% of the sample of young people. A larger proportion of the younger cohort were studying physics (59%) compared to older cohort (37%)

Awareness of, and engagement with, cyber security

80% of young people reported that they were aware of the term 'cyber security'

Participants were asked about their awareness of cyber security, whether they had learnt about it and whether they had taken part in any informal initiatives.

When asked about familiarity with concepts related to technology and computing (including 'cyber security', 'hacking', 'software development', 'computer viruses'), 95% of young people said they 'knew a little' or 'knew a lot' about at least one of these concepts.

80% reported that they 'knew a little' or 'knew a lot' specifically about cyber security.

65% of young people in our sample said that they had learnt about cyber security before. Looking into the differences between the age groups, the older cohort were slightly more likely to tell us they had learnt about cyber security before – 68% among 15–18-year-olds vs. 61% among 12-14 year olds.

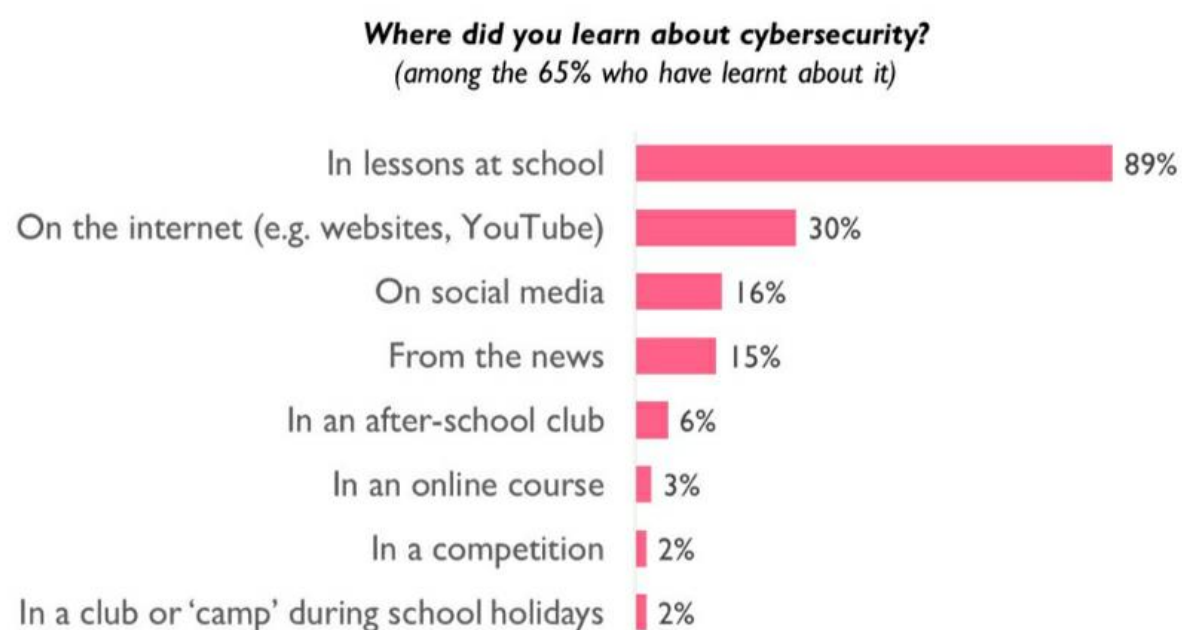
Most young people were learning about cyber security at school

Among those who had learnt about cyber security before, 89% (57% of total sample) said they had learnt about it in school lessons while 30% (19% of total sample) had learnt about it on the internet.

Only 6% of those who had learnt about cyber security before (4% of the total sample) said they had learnt about cyber security in an after-school club while only 2% of these children (1% of the total sample) said they had learnt about it in a holiday camp.

Those in the older cohort (15-18 years) were slightly more likely to report having learnt about cyber security on the internet. 33% among the 15–18-year-olds who had learnt about cyber security before, had learnt about it online, compared to 26% of the same group from the younger cohort (12-14 year olds).

Figure 10: Graphic illustrating where did young people learn about cyber security



BASE: All young people who have learnt about cybersecurity before, n=557

A smaller number of young people had heard of or taken part in informal cyber security initiatives

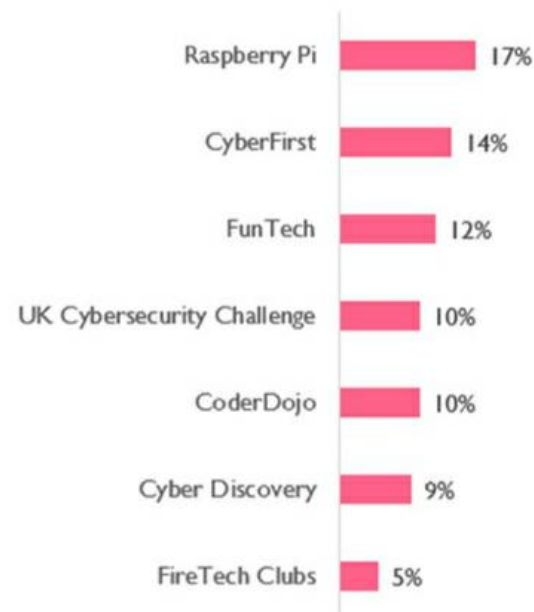
Participants were presented with some tech and cyber security-related initiatives, which included CyberFirst, Cyber Discovery, Raspberry Pi and FunTech.

41% of young people told us they had heard of one or more of these informal programmes. 14% said they had heard specifically of CyberFirst and 9% of Cyber Discovery.

Among those children who reported being aware of cyber-security related initiatives, most reported learning about them through their school. The second most commonly cited channel was through their friends, while social media was the third.

Figure 11: Graphic showing awareness of informal programmes

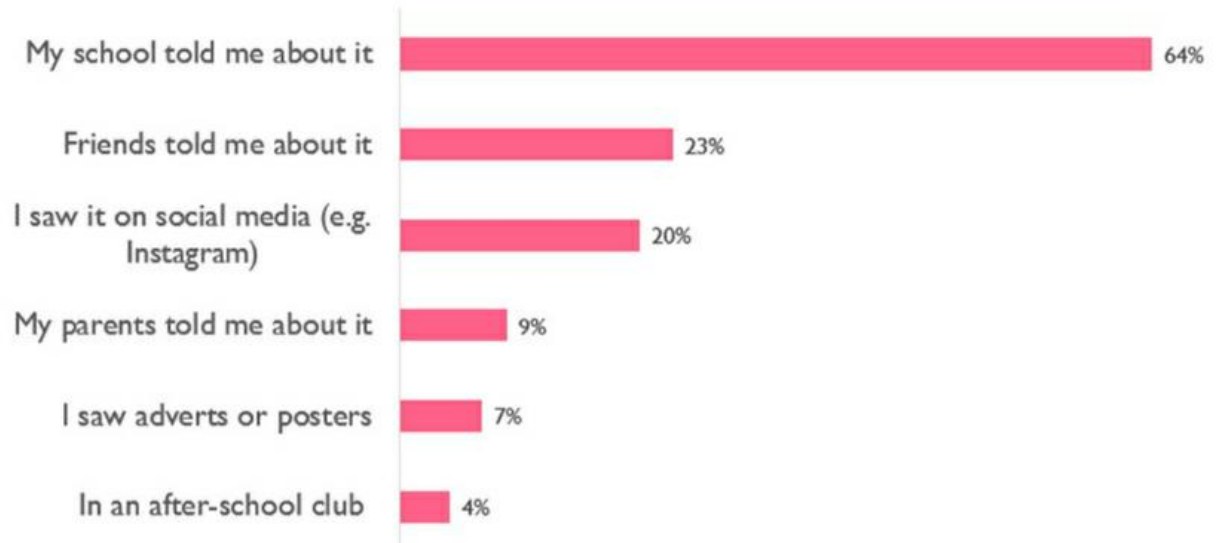
Percentage of respondents who have heard of informal programs



BASE: All young people, n = 862

Figure 12: Graphic showing where respondents have heard about programmes

Channels through which respondents heard about informal programmes (Among the 40% who have heard about them)



BASE: All young people who had heard of informal interventions, n = 352

17% of the young people in our sample (150 respondents) had ever participated in one or more informal programmes. Raspberry Pi and CyberFirst were the programmes most commonly cited (by 7% and 6% of the total sample of young people respectively).

It appears that across each of the initiatives, there is roughly a 1 in 3 conversion rate from children having heard about it to children participating. These conclusions are based on small numbers of respondents who report participating in an informal programme. We cannot conclude with certainty whether one initiatives participants differ from another's.

If we exclude participation in CyberFirst and Cyber Discovery as they are beyond the scope of this work, the proportion of our sample of young people who have ever

participated in an informal programme reduces to 14%

A very small cohort (6% of the total sample) had taken part in more than one programme. While 3% of the young people in the sample had taken part in 2 initiatives, 3% had taken part in 3 or more programmes.

There appears to be a correlation between taking part in informal initiatives and studying related subjects. Over 64% of young people who had taken part in informal programmes reported studying Computer Science and/or ICT. In contrast, 47% of those who hadn't taken part in an informal programme reported studying these subjects.

How does this participation data compare to the estimated reach of initiatives from the scoping activity?

17% of young people surveyed said they had taken part in selected programmes. The reach of the initiatives identified during scoping activities suggests that 2% of young people are reached – which is obviously much lower.

There are some important notes here:

- The survey asked about participation in initiatives ever, whilst our reach estimation is a per year estimation.
- Our estimated reach calculation doesn't include CyberFirst or Cyber Discovery. If we exclude participation in CyberFirst or Cyber Discovery from our survey data calculations, 14% of our sample had taken part in informal programmes.
- But similarly, the list of initiatives in the survey doesn't include some that are included in the scoping (although there was space for respondents to enter additional programmes that they had participated in).
- As we mentioned, our reach estimation is very much a best guess and likely an underestimate. The survey data suggests that the estimation is indeed likely to be an underestimate.

Parents were slightly more likely to have heard of 'cyber security' than their children but less likely to have heard of informal cyber security initiatives

83% of the parents in our sample said they 'knew a little' or 'knew a lot' about cyber security, compared to 80% of young people. But when asked about informal programmes, only 37% of parents had heard of one or more informal programmes, compared to 41% of young people – showing that young people are slightly more likely to hear about these programmes than their parents. [\[footnote 19\]](#)

Most parents had come across informal programmes on social media. School was the second most popular channel.

What did we learn about awareness and participation in CyberFirst and Cyber Discovery?

14% of the sample of young people had heard of **CyberFirst**. 6% had participated in it.

9% of the sample of young people had heard of **Cyber Discovery**. 3% had participated in it.

Among those who had heard about CyberFirst and Cyber Discovery, over half reported that they had heard of it from their school. Many had also heard

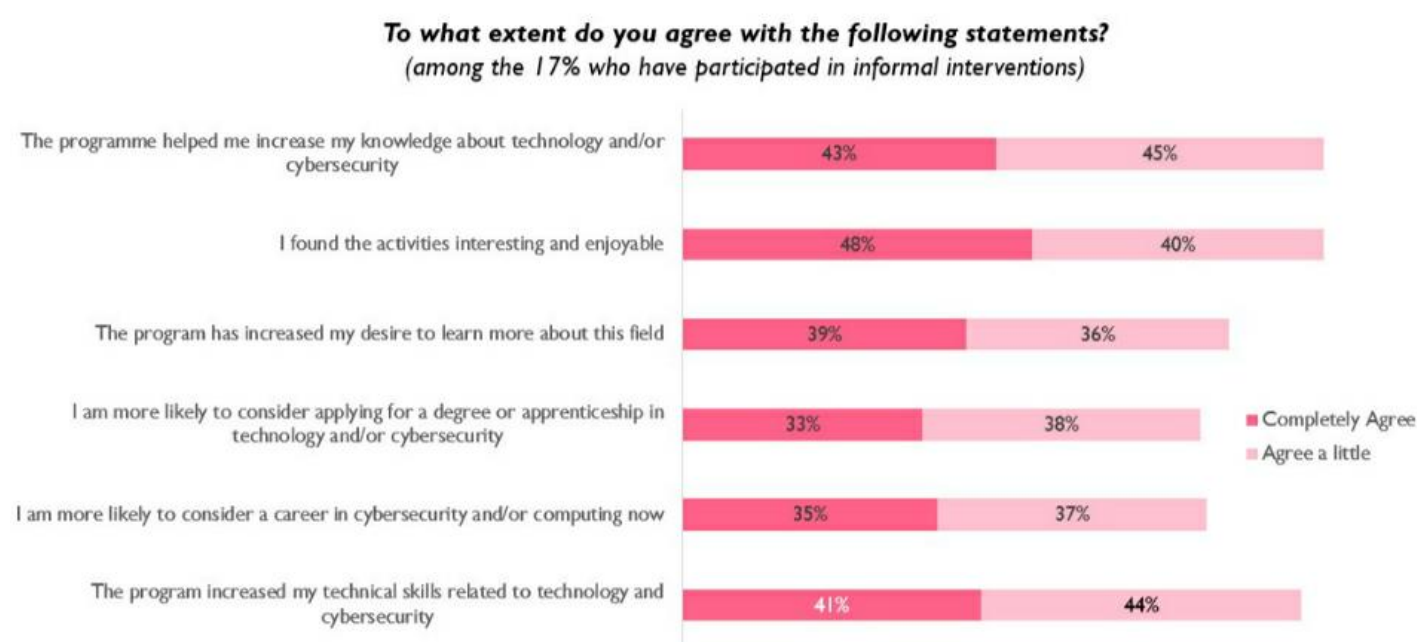
of the programmes through friends and social media.

Note: Cyber Discovery was also branded CyberFirst, so respondents may have conflated participation in one programme with participation in the other

Most young people who participated in informal initiatives report having a positive experience

Those who had taken part in informal programmes (n=150) reported having a positive experience, as the graph below shows.

Figure 13: Graph showing young people’s perception of the programmes they took part



BASE: All young people who had taken part in an informal intervention, n= 150

Perception of cyber security careers

Parents were more likely to view cyber security careers favourably

Respondents were asked to report how pleased they would be if their child pursued a career in a variety of areas. Parents ranked cyber security (as a career field) quite favourably, with 81% saying they would be pleased if their child pursued it (assigning it 6-10 points on a 10-point scale). It is important to note that parents’ view of most skilled professions was favourable, with 82% viewing professional services (e.g. law, finance etc.) favourably, and 68% viewing healthcare favourably. In contrast, retail (36% pleased) and hospitality (45% pleased) fared the worst.

Generally, fewer young people reported all career fields as being less appealing when compared to parents. 61% of young people said they found a career in cyber security appealing (assigning it 6-10 points on a 10-point scale) – 20 percentage points lower than parents. Much like parents, young people also looked upon retail and hospitality as the least appealing career fields.

Young people had the perception that cyber security was a valuable field but were more uncertain about how easy it would be to find a job in the sector

Respondents were given a set of opposing statements related to working in cyber

security. These statements were placed on either end of a spectrum from 0 to 10 and people were asked to pick a number indicating which statement they leaned towards.

Among young people, cyber security was felt to be an interesting and valuable field to work in with 67% of young people leaning towards saying that cyber security was ‘interesting’ and 81% thinking that it ‘makes a positive difference to people’s lives.’

Table 2: Young people’s perceptions of working in cyber security^[footnote 20]

Statement 1	Percentage of young people leaning towards the statement (0-4 points)	Statement 2	Percentage of young people leaning towards the statement (6-10 points)
Boring	23%	Interesting	67%
Does not make any difference to people’s day-to-day lives	6%	Makes a positive difference for people	81%
Poorly paid	6%	Pays really well	76%
It is difficult to find a job in this field	24%	It is easy to find a job in this field	54%
Learn things that are not useful outside of work	13%	Learn skills that are really useful outside of work	71%
Requires a lot of experience/expertise with technology and computing to get started	6%	Doesn’t require any technical computing skills to start working (e.g. entry level)	83%
Few jobs available	25%	Lots of jobs to choose from	53%
Need a lot of experience to be able to get a job	9%	Can start without experience	73%

However, 1 in 4 young people thought that there are few jobs available in the field.

It was a similar story for parents. They leaned towards saying that cyber security is ‘interesting’ (73% agree), ‘makes a positive difference to people’s lives’ (85% agree) and pays well (85%). Similarly to young people, approximately a quarter of the parents also thought that it is difficult to find a job in cyber security.

Table 3: Parents’ perceptions of working in cyber security

Statement 1	Percentage of parents leaning towards the statement (0-4 points)	Statement 2	Percentage of parents leaning towards the statement (6-10 points)
--------------------	---	--------------------	--

Monotonous and boring	13%	Varied and interesting	73%
Does not make any difference to people's day-to-day lives	5%	Makes a positive difference for people	85%
Poorly paid	4%	Pays really well	85%
It is difficult to find a job in this field	24%	It is easy to find a job in this field	52%
Provides skills that are not useful outside of work	9%	Provides skills that would be really useful outside of work	78%
Fixed hours – no flexibility to fit around other things	15%	Flexible hours (to fit around social/family life)	66%
Limited range of jobs to choose from	20%	Wide range of jobs to choose from	63%
An environment where sexism is common	14%	Somewhere with modern attitudes to women and non-binary people in the workplace	66%
Requires a lot of experience / expertise with technology and computing to get started	9%	Doesn't require any technical computing skills to start working (e.g. entry level)	79%
An environment where things like racism and homophobia are still present among the workforce	8%	Somewhere with a diverse workforce and progressive attitudes	74%

5. Conclusion

This project was the first attempt to map the landscape of informal cyber security programmes aimed at ages 5-19. Whilst there are undoubtedly gaps in the data set out in this report, some tentative conclusions can be made.

Most initiatives were targeting ages 10-14, ran in a small group format and were free for end users

There are a fair number of initiatives aimed around tech, computer science and cyber security in the UK. It is currently unclear how many are still active. The Covid-19 pandemic had an impact on the operation of some initiatives – causing some to stop or to move from face-to-face to online.

Most initiatives were targeting ages 10-14, given this is the age group where decisions are being made around subjects to study further.

A very approximate estimation of reach is 230,000. The survey data suggests that this estimation is likely to be an underestimate.

In terms of format, most were running sessions face-to-face in small groups and were free for end users.

It was unclear how initiatives were measuring success. Some had some KPIs and data that they were recording but it was difficult to assess effectiveness of many of the programmes.

Initiatives were using interactive activities based on real-life scenarios to engage young people

In terms of promotion and activities, there was an awareness that being overly technical could risk putting potential end users off. Many were using games or interactive activities, linking to other interests that young people had, and sometimes not even mentioning cyber security until later on in the programme. Connections with schools and social media appeared to be the most used promotional channel.

There was little evidence of networking, signposting or learnings being shared between different initiatives

Some expressed interest in building better links with other programmes in their area. Some talked about needing a concise strategy in their area, wanting to learn from other initiatives, or knowing where else they could refer their students to when they had finished their current programme.

Four outcomes should be met to support young people to move into a career in cyber security

Initiatives did not always have a clear language to talk about what they were trying to achieve, but from what initiatives said, there appeared to be four distinct outcomes for end-users of initiatives, which were consolidated into a framework:

Figure 14: Outcomes targeted by initiatives



The activities that initiatives were carrying out might meet only one or several of these outcomes – but all of these outcomes need to be met at some point in a young person’s journey in order for them to move into a career in cyber security. These outcomes could be seen in terms of a journey.

This framework may prove useful in prompting initiatives to further define their objectives or for future analysis of initiatives.

Although various programmes exist, they may not be concentrating on the right topic or outcome at the right time

Some experts and organisations reflected there is a risk involved in focusing in on cyber security too early. They felt that it would be beneficial to move from a broader ‘tech’ perspective to introducing cyber security later as young people specialise, as is the case in other disciplines such as medicine. They also felt that young people could be put off cyber security before they have had a chance to understand what is involved – which may prevent them from engaging with it at a later time.

The focus of initiatives we looked at did not reflect this idea. There was not a pattern of initiatives focused on younger age groups being more tech-focused and those focused on older age groups being more cyber security-focused.

When looking at the subset of 26 initiatives, although awareness, inspiration and affinity were covered, more initiatives explicitly focused on developing knowledge and skills.

From this point of view, it could be said that although various programmes with a wide offer for young people exist, they may not be concentrating on the right topic or outcome at the right time – or in the right order.

Appendix 1: survey sample

Parents survey sample

Characteristic		Incidence	Number of Respondents
Age	18-24	0%	2
	25-34	12%	105
	25-44	41%	356
	45-54	36%	310
	55-64	10%	83
	65+	1%	6
	Gender	Male	28%
Female		72%	622
Region	Northwest England	15%	127
	Northeast England	8%	73
	West Midlands	11%	92
	East Midlands	10%	85
	London	10%	83
	East of England	9%	74
	Southeast England	13%	116
	Southwest England	6%	53

Young people survey sample

Characteristic		Incidence	Number of Respondents
Age	12	15%	131
	13	18%	151
	14	17%	149
	15	19%	167
	16	15%	125
	17	11%	94
	18	5%	45
	Gender	Male	49%
Female		50%	431
Non-binary		1%	7

Region	Northwest England	15%	129
	Northeast England	8%	71
	West Midlands	11%	92
	East Midlands	10%	85
	London	10%	85
	East of England	9%	77
	Southeast England	13%	115
	Southwest England	6%	52
	Scotland	8%	69
	Wales	6%	48
	Northern Ireland	3%	25
Ethnicity	White British	81%	699
	White Irish	2%	13
	Eastern European	0%	4
	Any other white background	1%	11
	White and Black Caribbean	2%	18
	White and Black African	0%	4
	White and Asian	3%	22
	Any other mixed background	1%	9
	Indian	3%	27
	Pakistani	2%	13
	Bangladeshi	1%	7
	Sri Lankan	0%	2
	Any other Asian background	1%	6
	Caribbean	0%	4
	African	2%	15
	Chinese	0%	3
	Any other	0%	2
	Prefer not to say	0%	3

Appendix 2: list of interventions

Please note: the table below lists all the initiatives identified through desk research, undertaken between October 2021 and March 2022. It is not a live list, and therefore, some initiatives may not have been identified.

Name of Overarching Programme	Name of Intervention(s) (if applicable)	Description	Status	Link
Fun Tech		After school and holiday clubs in person or virtual. A variety of courses for ages 7 to 17	Live	Fun Tech
Cyber Security Challenge UK (NCA)	CyberCenturion and CyberLand competitions	3-round team-based online competition	Live	CyberCenturion and Cyberland competitions
	CyberGames	Series of online games which cover a wide range of skills	Live	CyberGames
The Smallpeice Trust		School event days and scholarships encouraging careers in cyber security/technical design backed by charities, parents, teachers, universities and corporate partners	Live	The Smallpeice Trust
NI Direct Government Services	Cyber gateway aptitude programme	Online training programme. Once completed, you can access jobs specific to cybersecurity	Live	Cyber gateway aptitude programme
ASDConnect @ YMCA Port Talbot		Coding aimed at children with autism	Past	ASD Connect
Coder Dojo	General	Programme run outside of school. Community led and on a voluntary basis. They offer resources / guidelines / content for other dojos to open and to run clubs providing a very informal and open	Live	Coder Dojo

		space that children can come to and explore their curiosity with peers		
	Coder Dojo Belfast	Programme run outside of school. Community led and on a voluntary basis. They offer resources / guidelines / content for other dojos to open and to run clubs providing a very informal and open space that children can come to and explore their curiosity with peers		
	CyberSafe Scotland	Provide training, support, and resources to children, schools, and parents on how children can stay safe online	Live	CyberSafe Scotland
	Cyber Skills Live	Online lessons, activities and games aimed at children to help them learn various cybersecurity-related skills	Live	Cyber Skills Live
	Activity Book for Kids	A printable limited-edition Activity Book for Kids to introduce them to cybersecurity in a fun way	Live	Activity Book for Kids
	Metropolitan Police: Cyber Choices	A prevention program targeting young people with already developed cybersecurity skills to raise awareness of the Computer Misuse Act 1990, and encourage them to use their skills in a positive way	Live	Metropolitan Police: Cyber Choices
STEM from	STEM from	Downloadable	Live	STEM from

Home	Home: Cyber Security	STEM based activity packs for children aged 6 – 14, produced by CGI (an IT consulting firm) as a CSR initiative		Home: Cyber Security
Bluescreen IT Academy	i-Steps Program	Teach kids who have some knowledge/skills to make good use of these, instead of risking doing bad things and end up in trouble	Live	Bluescreen IT Academy: iSteps Academy
	HACKED	Program to raise awareness about illegal cyber activity and rehabilitate those who may have been involved; includes a private bug bounty program	Past	Bluescreen IT Academy: HACKED
	BIT Traineeship	Traineeship schemes for 16-24 years old. Lasts up to 6 weeks, including instructor-led training and work placement	Live	Bluescreen IT Academy: BIT Traineeship
WarGames		Online games to learn and practice security concepts	Live	WarGames
Code Club Network	Code Club (General)	An international network of free coding clubs for students aged 9-13, program run by Raspberry Pi foundation	Live	Code Club
	Todmorden High School Code Club	Weekly after school club, implied was open to the general public as well	Live	Code Club Network: Todmorden High School Code Club
	Leeds Central Library	Evidence of a code club that ran since 2015 at Leeds central library. Unsure if it ran after the	Unclear	Code Club Network: Leeds Central Library

COVID-19
pandemic

	Newport Library	Children learn to create images, animations and even simple computer games using Scratch. These Newport Libraries sessions run for 12 weeks during term-time and need to be booked in advance	Past	Code Club Network: Newport Library
	Code Club: Liverpool Central Library	Tech North announced a partnership with Code Club during the new, ran as weekly after-school sessions in Liverpool Central Library, for school children between 9 – 11	Past	Code Club Network: Liverpool Central Library
	Code Club Belfast	Part of a UK network of volunteers and teachers running free coding classes and clubs for children in Belfast	Live	Code Club Network: Belfast
	Code club Penarth Library	Penarth code club is run in Penarth Library, every Tuesday afterschool. Having closed during Covid as a result of not being able to access the library computers, the club was restarting with increased interest	Past	Code Club Network: Penarth Library
The Hacking Lab		Ethical hacking and Cyber Security challenge centre, run by TechTalent Academy	Live	The Hacking Lab
Blue Shift Coding	Online Classes; Camps; Private	Provide coding lessons through	Live	Blue Shift Coding

	tuition	camps, online courses, and private tuitions		
The Institute of Coding	Computer programming for everyone (University of Leeds)	Teach how coding and basic computer programming can be used to solve problems.	Live	The Institute of Coding
Barclays	Code Playground	Aim to empower people through code literacy via interactive live classes. Use free online resources, access detailed lesson plans or a book a school visit with one of our Barclays Digital Eagles	Live	Barclays: Code Playground
Cypher Coding School		Coding lessons (both online and F2F) for children aged 6-12	Live	Cypher Coding School
University of Bristol Cyber Security Group	CyBOK (Cyber Security Body of Knowledge) project	Funded by the National Cyber Security Programme, provides numerous resources for different types of audiences, including a comic book series and games for students/young people	Live	CyBOK
Pennine Kids CyberStreet	General	An initiative for local businesses to spread awareness about their career options to students	Live	Pennine Kids CyberStreet
	Yorkshire STEAM	Initiative in partnership with the Yorkshire Cyber Security Cluster, to inspire schoolgirls to consider careers in STEAM	Past	Pennine Kids CyberStreet: Yorkshire STEAM

(Science, Technology, Engineering, Arts and Mathematics) – the foundation blocks for building a career in cybersecurity

Young Scot	Cyber Scotland Week	Annual cyber event aimed at young people in Scotland. The focus of 2020's session was online safety	Live	Young Scot: Cyber Scotland Week
	DigiKnow	Raising awareness of cyber through online resources for young people in Scotland	Live	Young Scot: DigiKnow
Girl Guiding Scotland with Skills Development Scotland and Education Scotland	Digital Scotland Challenge	Digital challenge with girl guides in Scotland to get them more engaged and interested in STEM	Live	Girl Guiding Scotland: Digital Scotland Challenge
Cybersafe Kids (NI)	Cybersafe Kids (NI)	Charity group that gives tools, e-learning, talks and research into being safe online. Equipping kids with the digital skills to be safe online	Live	Cybersafe Kids (NI)
NI Cyber Security Centre	Cyber Champions	A resource pack of games, posters and activities for teachers, youth leaders and clubs explain cyber security to the kids they have contact with. You can be a Champion, Guardians, Prefects, Partners	Live	Cyber Champions
DigiLocal		Weekly clubs held across four libraries, and involve building games and simple computational	Live	DigiLocal

		thinking		
Code Ninjas		Kid coding franchise, which teaches kids how to code, build games, problem solve learn STEM skills in a 'safe and inspiring environment'. Also ran a summer camp in 2021	Live	Code Ninjas
Player Ready Virtual Reality	Pathfinder Kids Club Plymouth: Minecraft Club	Half term and after school clubs, using Minecraft to build, create and tackle STEM subjects. Also run coding and streaming clubs too.	Live	Player Ready Virtual Reality: Pathfinders Kids Club Plymouth
IT Career swap	Junior Cyber Security Engineer	Students study their online courses, take the exams and practice on their online placements. Then they help you find a job	Live	IT Career swap: Junior Cyber Security Engineer
TECGirls		Tec Girls are trying to increase the appeal of tech careers to young girls in Cornwall, holding workshops, publishing magazines, and producing free resources for kids, teachers and parents to use.	Live	TECGirls
Software Cornwall	Mission to Mars	An education outreach programme, for companies and budding developers. Using code to programme robots, problem solve and 'deploy their rovers'	Past	Software Cornwall: Mission to Mars
	Tecademy	A weekend event demonstrating and	Past	Software Cornwall:

		training teachers about the resources available to them to educate and use in their classes		Tecademy
	Cornwall Tech Jam	Bi-monthly drop-in days where anyone (all ages and abilities) can learn about coding outside of the classroom. The kit is provided by Raspberry-Pi	Live	Software Cornwall: Cornwall Tech Jam
DATA Plymouth	#GIRLCODE	Free coding class for girls to learn with industry professionals how to code and use programmes	Past	DATA Plymouth: #GIRLCODE
Cyphra-Security Enabling Business (NI)	Social Responsibility	Support the Cyber First scheme, being a promoter and helping NCSC bring it over to Ireland. Hosts career talks	Live	Cyphra: Social Responsibility
Teaching Cave (NI)	Crazy Coding	Privately run afterschool clubs for 4–11-year-olds playing games and challenges to learn through Sphero, Osmo and Tynker	Live	Teaching Cave: Crazy Coding
YouthFed	YouthFed Cyber Academy	Workshops designed to make young people aware of cybersecurity and provide real-world work experience for young adults interested in a career in cyber security. Funded by DCMS	Past	YouthFed: Cyber Academy
	YouthFed Cyber Safety	Live and pre-recorded online sessions on cyber safety for young people aged 14-18, to teach them how to protect	Live	YouthFed: Cyber Safety

		themselves from online hackers		
Club Hub		Provides computing clubs in Leeds (about 10 miles away) for children (including those with SEND) aged 8-18 around and after school in the week and on weekends	Live	Club Hub
Wakefield College and Wakefield Children's University		Y4 students (age 8) could take a six-week coding course at their own pace and receive an accredited qualification at the end of it	Unclear	Wakefield College and Wakefield Children's University
Wakefield Library	Code Club	Appears to be evidence of a code club that ran at Wakefield Libraries. Also have a YouTube channel with tutorial videos in this name	Unclear	Wakefield Library: Code Club
Coop Academy Parkland, Bradford	After school clubs	Run after-school clubs for students across many different age groups. Have organised STEM and technology related activities in the past.	Past	Co-op Academy Parkland, Bradford: After school clubs
Cyber Scotland Partnership - NCSC	Youth Link Scotland: Cyber Aware	Developing digital skills relating to cyber: malware, phishing, firewalls	Live	Youth Link Scotland: Cyber Aware
DressCode	Turing Testers 2.0	Aim to inspire the next generation of Scottish Cyber talent through competitions and education	Unclear	Dress Code: Turing Testers 2.0
Edinburgh Science	Edinburgh Science Learning	STEM programmes for those aged 16-24 in Edinburgh	Live	Edinburgh Science: Learning
Edinburgh	Edinburgh	Life sciences	Live	Edinburgh

BioQuarter	BioQuarter STEM clubs	centre encouraging STEM education among young people		BioQuarter: STEM clubs
FireTech		Tech courses for young people where kids could get their hands dirty and experiment with a wide range of technology-related concepts	Live	FireTech
Prewired	Prewired+	Edinburgh based programming club for under 15s	Live	Prewired
GeekyKids		LIVE Virtual classes in Python, Scratch, Minecraft, and Roblox	Live	GeekyKids
Create My Next		Tutor-led online 1-on-1 coding classes for 7–17-year-olds	Live	Create My Next
Twin Science		Twin School offers subscription-based STEM education with Twin Kits & App for a brighter future. For ages 8-11	Live	Twin Science
WhizzKids		A small computer club for children and adults, engaging them with programmes such as Raspberry Pi, and Python	Live	WhizzKids
School of Coding		Teach computer science, coding and digital skills to children and adults across the UK & Europe. Provide coding lessons online and at their education centres	Live	School of Coding
Computer Xplorers	General	ComputerXplorers is part of a franchised network	Live	Computer Xplorers

technology and computing education for children from the age of 3 to 13. Uses age-appropriate software, peripherals and curriculum

ComputerXplorers
North Yorkshire

ComputerXplorers North Yorkshire provides specialist computing classes for ages 3 and over across Harrogate, York, Leeds, and surrounding areas, both in person and online.

Live

[Computer Xplorers: North Yorkshire](#)

National Digital Exploitation Centre (NDEC), a collaboration between the University of South Wales, Thales and the Welsh government

University of South Wales leads the Education strand at the National Digital Exploitation Centre. Working with schools and community groups, helping inspire young people to consider careers in cyber security and digital industries

Live

[National Digital Exploitation Centre](#)

Technocamps

They work with secondary schools through their STEM Enrichment programme and primary schools through our Playground Computing programme. They also provide training and professional development for teachers to prepare them for the challenges of delivering in a technical and dynamic environment

Live

[Technocamps](#)

STEM NI	Running a number of educational programmes in Northern Ireland and work with teachers and volunteers to deliver these programmes to students of all ages across many educational institutions	About to launch	STEM NI
Bring IT On	They showcase the opportunities and benefits of careers in IT for you by raising awareness on the great diversity of options in this exciting and ever-changing sector. They run events, speak at schools, attend job fairs and work with employers, careers advisers, IT teachers, parents, and carers to promote job opportunities available in IT throughout NI	Live	Bring IT On
London School of Mathematics and Coding	Maths, programming, and robotics programs for kids aged 4 to 18	Live	London School of Mathematics and Coding
Quantum Technology Club	Free Code Club in Ormskirk for children aged 9-16, learning Scratch, HTML, CSS and Python. Single site at Cottage Lane Mission Church	Past	Quantum Technology Club
Codebug	Physical coding programme, where any beginner can learn to code using a physical device with 25	Live	Codebug

	LED lights that give you the opportunity to scroll messages, make games, and experiment with electronics		
Shiftclick	Online platform designed to kickstart a career in tech, with two courses: introduction to coding and full stack web development	Live	Shiftclick
Edublocks	Online resource with introductions to Python 3, HTML, BBC micro:bit, CircuitPython, and Raspberry Pi. Appears to be intended for teachers wanting to improve their coding capabilities, and perhaps pupils too	Unclear	Edublocks
Manchester Girl Geeks	Run events to provide opportunities for women in STEM to get together in a relaxed environment, network and meet like-minded people.	Unclear – Last event was in August 2021	Manchester Girl Geeks
Digital Innovators	Focus on developing soft skills necessary for tech-related careers through a structured DI Skills Programme	Live	Digital Innovators
Software Academy	Teach coding, basic skills and game design through online classes	Live	Software Academy
MAMA. Codes	Coding classes for 3-12 on scratch	Live	MAMA. Codes

		junior, online and in-person		
STEMettes		Organisation promoting STEM and technology careers among young women and girls and non-binary people	Live	STEMettes
Exa Foundation - Raspberry Jam / Family Hack Jam		Monthly and one-off events for 8-14yos - trying to give them a taster of computer science - but in a subtle/disguised way. Supported by Exa Networks	Live	Exa Foundation: Raspberry Jam / Family Hack Jam
CII Sec / Qufaro - Cyber EPQ	Cyber Extended project qualification (EPQ)	The CyberEPQ is the UK's first and only Extended Project Qualification (EPQ) in Cyber Security. This unique Cyber Security qualification has been developed by a consortium of education and Cyber Security partners to help provide a starting point for anyone considering a career in Cyber Security; to go to university, start an apprenticeship or change career	Live	Cyber Extended Research Project
	Head Start course in Cybersecurity	Similar to the EPQ, where participants take the 10 core modules but don't do the extended project at the end		
Career Colleges	AWS Digital project	Aim to help young people prepare for a career in tech, by helping them keep up to date with latest industry developments and	Live	Career Colleges: AWS Digital Project

		business needs		
Cyber Hub Trust	Secure Operations Centre	Use a training room in a space and do a course to upskill young people in cybersecurity. Provide them with real world experiences of the type of things they would have to do in local businesses, facilitating training and work experience for students and Cyber Security services for local businesses	Live	Cyber Hub Trust: Secure Operations Centre
The Code Zone: Cambridge		Coding Courses for ages 6-14. Free Access to animation and simulation studies and using their tools for their own projects. Also run a 'Hack Club', an online live weekly session to collaborate with other children led by the mentor to "hack" games and make them your own. Also can have one to one sessions with your mentor. Also run in-person and/or one-on-one sessions if in demand.	Live	The Code Zone: Cambridge
Tech Studio Cambridge ICT Club		Have intermediate courses in technology, computer science, animation, and robotics, and a holiday club for ages 7-14	Live	Tech Studio Cambridge ICT Club
Kainos Work Experience		A 3-day virtual work experience,	Live	Kainos Work Experience

proving practical experience of web development, and building skills like communication, problem-solving, teamwork

Try Hack Me

TryHackMe is an online platform that teaches cybersecurity through short, gamified real-world labs. Its content for both complete beginners and seasoned hackers, incorporation guides and challenges to cater for different learning styles.

Live

[Try Hack Me](#)

Hack the Box

Hack The Box is a large hacking playground, and a community of over 988k platform members. Has an online cybersecurity training platform that allows individuals, businesses, universities, and organizations globally to level up their offensive and defensive security skills through a fully gamified and engaging learning environment

Live

[Hack The Box](#)

-
1. Belfast, South Wales, Edinburgh, London, Cornwall (focusing on Plymouth), West Midlands, Yorkshire (focusing on Bradford), and programmes that had nationwide reach.[↵](#)
 2. Reach calculations were carried out considering the size of the groups or courses the organisations were running, their duration and number of times they run per year. This estimation assumes attendees are unique people, assumes the group sizes are consistent and run in the frequency that they told us.[↵](#)
 3. Based on a population of 11,876,207 (ONS 2020 data).[↵](#)

4. Some covered more than one discipline.[↵](#)
5. 27 interviews were carried out but one was discounted due to being a government-funded initiative.[↵](#)
6. Where there were multiple programmes run by one overarching organisation, we have only counted the organisation once. For example, there are multiple Code Clubs under the Code Club brand, but we have only counted this once.[↵](#)
7. The average number of young people these initiatives reached was approximately 11,000 while the median was significantly lower at approximately 280 young people. The reach of the initiatives varied a lot, with one reaching 15 per year, and another over 80,000 per year.[↵](#)
8. Based on a population of 11,876,207 young people (ONS 2020 projections)[↵](#)
9. The asterisks in this reach table denote those programmes or reach calculations where reach data was incomplete or unknown, and thus the consequent reach data calculations are based on the programmes that are not asterisked in that area[↵](#)
10. This is using the population of young people in Plymouth, as Bluescreen IT is only active in Plymouth, and we do not have the reach data for TECGirls.[↵](#)
11. For simplicity, we have used the term nationwide to mean any programme that operates in multiple regions. across the UK, or globally.[↵](#)
12. Some covered more than one discipline[↵](#)
13. Some covered more than one discipline[↵](#)
14. For some initiatives, it was unclear how they were funded. These figures therefore do not add up to the total number of scoped initiatives.[↵](#)
15. For lots of initiatives, there were multiple options for types of classes and direction they offered, and the numbers here represent totals for all types of direction available. These numbers therefore far exceed the number of scoped initiatives, due to the multiplicity of direction available.[↵](#)
16. This data is calculated from the initiatives we were able to evaluate in terms of payment. Some initiatives were not clear about whether they were free or paid, and a couple had free online resources that you could upgrade to a paid premium package to access more exclusive content.[↵](#)
17. A full sample breakdown can be found in appendix 1.[↵](#)
18. It is possible that some respondents understood Computer Science and ICT to be the same things.[↵](#)
19. It is hard to determine what level of knowledge respondents may associate with the option 'know a little.' From experience, it can be as little as having heard the term a few times.[↵](#)
20. High numbers of children and parents reported that they did not think that technical computing skills were needed to start working in cyber security. However, several experts highlighted that one barrier to entry for many people was a perception that cyber security did require a level of technical knowledge. It is possible that the framing of the question in the survey – explicitly highlighting “entry level” roles – had an impact on how people responded, setting an expectation that there are not significant pre-conditions to entry.[↵](#)

[↑ Back to top](#)

Is this page useful?

Yes

No

[Report a problem with this page](#)

Topics

[Benefits](#)

[Births, death, marriages and care](#)

[Business and self-employed](#)

[Childcare and parenting](#)

[Citizenship and living in the UK](#)

[Cost of living support](#)

[Crime, justice and the law](#)

[Disabled people](#)

[Driving and transport](#)

[Education and learning](#)

[Employing people](#)

[Environment and countryside](#)

[Housing and local services](#)

[Money and tax](#)

[Passports, travel and living abroad](#)

[Visas and immigration](#)

[Working, jobs and pensions](#)

Government activity

[Departments](#)

[News](#)

[Guidance and regulation](#)

[Research and statistics](#)

[Policy papers and consultations](#)

[Transparency](#)

[How government works](#)

[Get involved](#)

[Help](#) [Privacy](#) [Cookies](#) [Accessibility statement](#) [Contact](#) [Terms and conditions](#) [Rhestr o Wasanaethau Cymraeg](#)
[Government Digital Service](#)

OGI All content is available under the [Open Government Licence v3.0](#), except where otherwise stated



© [Crown copyright](#)