SCOTTISH UNION LEARNING CYBER RESILIENCE

Evaluation Report 2017- 2024

CyberScotland

Scottish Government
Riaghaltas na h-Alba
gov.scot

SCOTTISH UNION LEARNING STUC

Summary

The following Evaluation Report provides feedback about the development, delivery, outputs, outcomes, and key impacts of seven Cyber Security projects funded by the Scottish Government's Cyber Resilience Unit.

The projects were developed to improve the cyber security skills of workers in partnership with training provider Digital Skills Education Ltd, during an abridged period of forty-eight months (four years), from August 2017 to the end of March 2024.

The overall objectives and outcomes outlined in the projects were aligned with UK and Scottish Government strategies and appropriate Action Plan Aims and Enablers which were relevant to the development of Learning and Skills, and the Public Sector contained in the following documents:

Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland, 2015
National Cyber Security Strategy 2016-2021, 2016
A Cyber Resilience Strategy for Scotland: Public Sector Action Plan, 2017-2018
Learning & Skills Action Plan for Cyber Resilience. 2018-2020
Strategic Framework for a Cyber Resilient Scotland, 2021
Cyber Resilient Scotland: strategic framework. Annex 3: Action Plans, 2021-2023.

Table of Contents

Initial Research and Workshop Development

To gauge the understanding of the importance of good personal cyber security practice in the workplace and explore demand, in early 2017 joint union and workplace learning meetings were held with six employers and unions in the Finance, Prison, and public sectors.

As a result of the meetings, an agreement was reached that three-pilot introductory level personal cyber security workshops would be delivered by Digital Skills Education Ltd with learners from AEGIS at AEGON, Prison Officers Association at Scottish Prison HQ, and with Union Learning Reps (ULRs) from across unions at the annual SUL Everyday Skills Event, 'Building a Resilient Workforce'.

In addition, unions, ULRs and learners had voiced concerns about the imminent changes in data protection laws as a result of the EU General Data Protection Regulation (GDPR) which was due to come into effect in May 2018.

To aid understanding about the changes and requirements regarding the Law, additional elements were included in the workshops on personal data protection skills.

Feedback from the three pilot workshops was overwhelmingly positive and 79 learners participated in the training. From the 79 learners, (one hundred percent) commented that the trainers and delivery of the training were excellent and 77, (ninety-eight per cent) commented that they had developed new cyber security skills and increased their confidence levels. A total of 78, (ninety-nine percent) of the participants commented that they would like the opportunity to develop their personal cyber security skills and requested further training by SUL. All employers and unions requested further training for workers in the future.

Following on from the employer and union pilots, more in-depth information about the potential for personal cyber security training in the workplace was gathered. A sample of six Union Learning Reps (ULRs) from ten unions were interviewed, 60 in total. These interviews were facilitated by ten union Project Workers. The ULRs then carried out face to face interviews with a sample of six workers from each union, 360 in total.

From the 360 workers, 342, (ninety-five per cent) of all the ULRs and workers reported that they knew very little or nothing about personal or workplace cyber security, 234 (sixty-five percent) reported that they had inadvertently opened personal or work-related phishing emails and 19, (fifteen percent) admitted that they had been subjected to a cyber hack. Ninety-eight per cent, (352) reported that they would welcome the opportunity to take part in cyber security training.

The pilots were delivered in early 2017 which was out with the scope of the earliest Cyber Security projects but, combined with the feedback from the unions mentioned above, provided the impetus to successfully apply for funding for the first Scottish Government Cyber Resilience project in 2017-2018.

To build momentum, a raft of marketing, publicity and promotional activities were carried out during 2017-2018 targeting employers, unions, reps, members, non-members, and external partners to encourage learners to improve their cyber security skills and knowledge by signing up to training.

These actions and additional feedback provided initially from 1142 learners requesting training in 2017-2018, provided the basis for further successful project applications from 2018 to 2024. The provision of additional funding ensured that the range of cyber security options could be delivered to improve cyber skills based on increasing levels of demand and need. (See addition information about Marketing, Promotional and Publicity activities for 2017 to 2024 on page 18).

Cyber Training Programme and Cyber Security Topics

By liaising with unions, employers, ULRs, members, workers, and external partners to ascertain cyber security skills demand and requirements in workplaces, training content was developed based on the guidance and support provided from the National Cyber Security Centre (NCSC) and in line with GDPR Regulations; the technical expertise and knowledge was provided by Digital Skills Education Ltd.

The results were the development of a suite of relevant workshop topics as follows:

Protecting personal data and accounts

- Protecting personal data online
- Using strong passwords
- Turning on two-factor authentication
- Setting up and using password managers

Recognising and responding to threats

- How to recognise phishing attacks
- How to report cyber threats
- Understanding social engineering
- Exploring how cyber criminals are using AI

Device and data protection

- **Setting up and using anti-virus software**
- **Backing up important data**
- **Protecting files and devices using encryption**
- **Staying safe on public Wi-Fi networks (using a VPN)**
- **Keeping smartphones and laptops secure**

Digital wellbeing

- **Take control of your personal data on your phone**
- **Reset your relationship with your phone**

'Train the Trainer' spin off

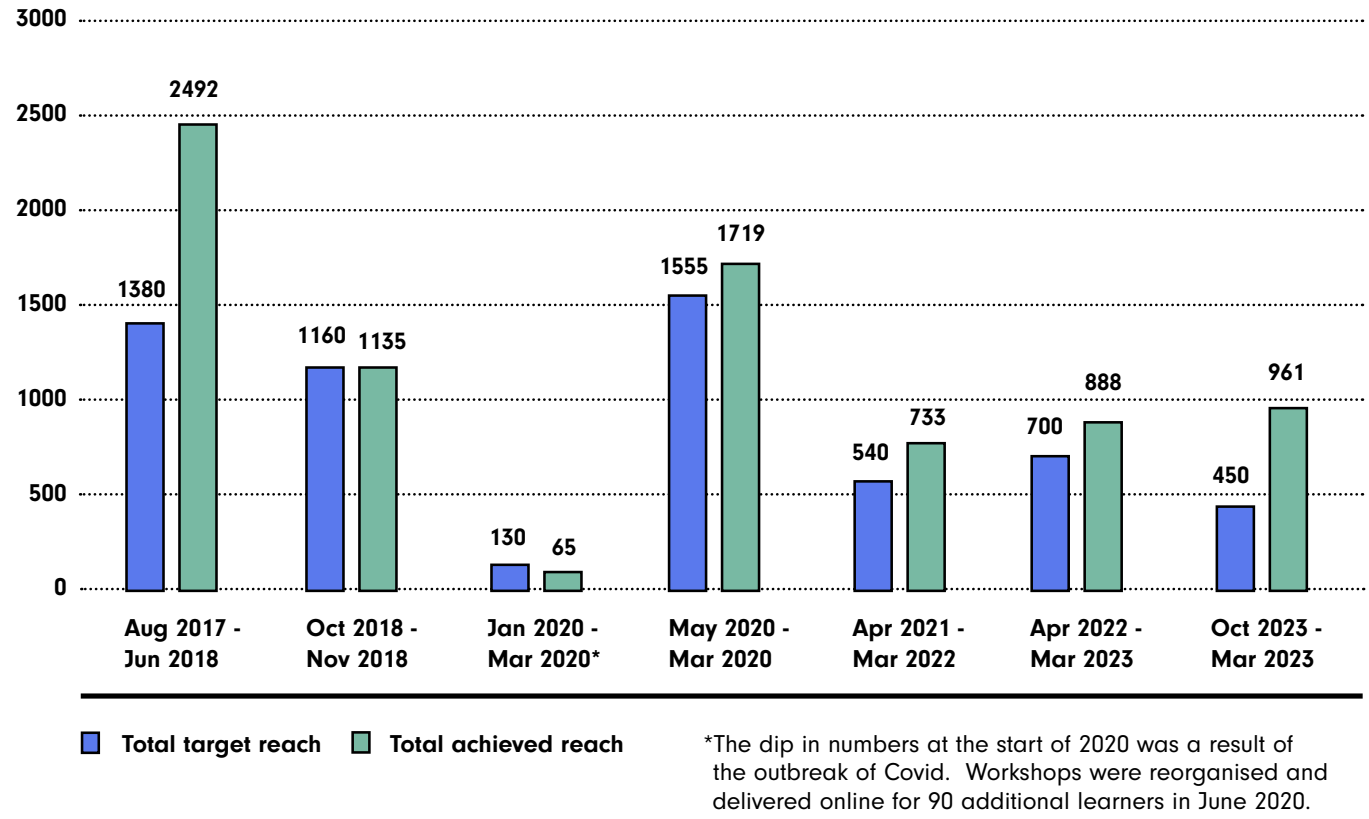
As a spin off from the workshops, further resources and training options were developed by Digital Skills Education Ltd which included piloting 'Train-the-Trainer' courses across Scotland; producing downloadable online resources which were available from 2017; a multi-media worker's toolkit which was available from 2021, and four video cyber lessons from 2022.

Output and Outcomes 2017-2024

During the four-year period, 7,993 learners participated in workshops which was a thirty-five percent increase from the original target of 5,915. The workshops were delivered in 30-minute, forty-five minute, one-hour and 90-minute sessions. A smaller number of learners, 520 (six percent) attended four-hour blocks of more in-depth training.

As the popularity of the training grew over time, learner targets were reached and often exceeded up to the end of the final project in March 2024. There is still a waiting list of over 100 learners who want to attend workshops in the future.

Target Number of Learners vs Achieved Numbers



*The dip in numbers at the start of 2020 was a result of the outbreak of Covid. Workshops were reorganised and delivered online for 90 additional learners in June 2020.

Overall Feedback

From the 7,993 learners who participated in the workshops, 7,594 (ninety-five percent) provided initial feedback and an average of ninety-three percent consistently reported that as a result of the training they:

- Had installed more secure passwords or a pass phrase on both their personal and work devices and forwarded or shared this knowledge with their work colleagues, families, and friends
- Were aware of and deleted phishing emails where appropriate when using devices in work, and their personal lives
- Were very satisfied with the training, felt more confident and were willing to learn more
- Were extremely satisfied with the overall standard of the workshops and the tutors.

In-depth Feedback
2017 - 2024

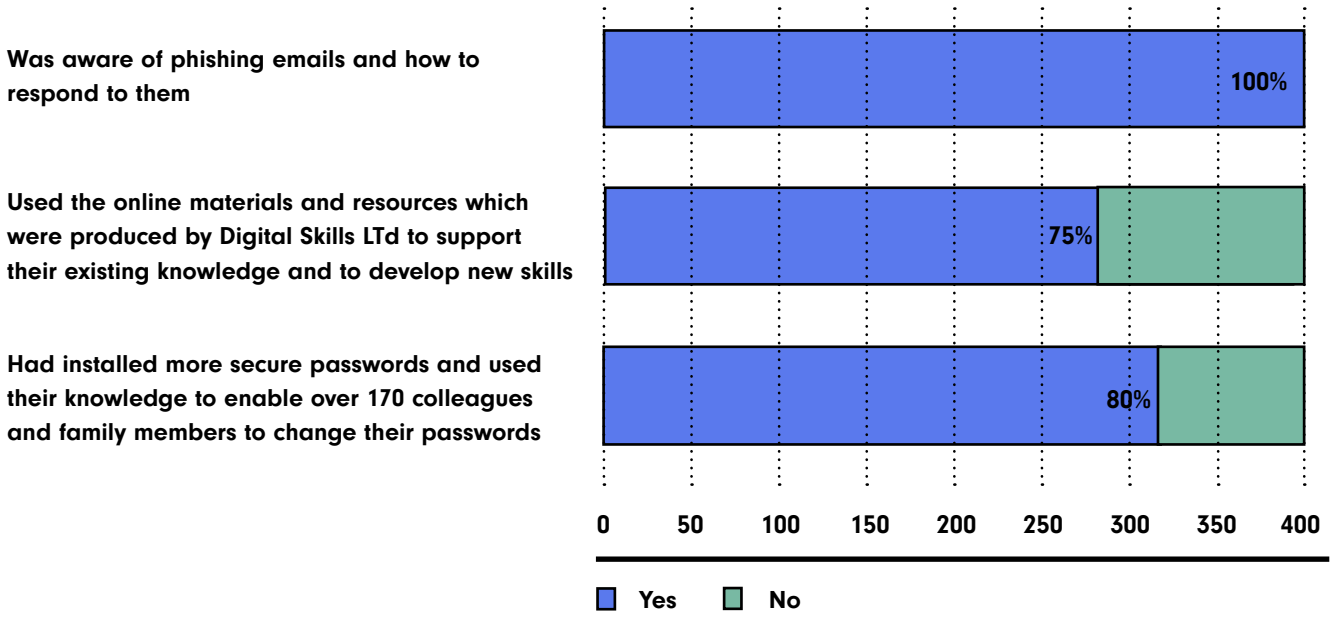
In order to provide more detail about learner experiences, the following feedback is based on the number of learners who responded to questionnaires and surveys and not on the total numbers who attended the workshops.

August 2017 to June 2018

From 819 learners who completed an initial questionnaire providing feedback about the training, 400 (49 percent) of the learners responded to a more in-depth follow-up survey in June 2018 and reported that they:

- Had installed more secure passwords 380 (eighty percent) and used their new knowledge to enable over 170 colleagues and family members to change their passwords
- Used the online materials and resources which were produced by Digital Skills Ltd to support their existing knowledge and to develop new skills, 280 (seventy percent)
- Were more aware of phishing emails, 400 (one hundred percent).

Learner outcomes 2017-2018



October 2018 to November 2019

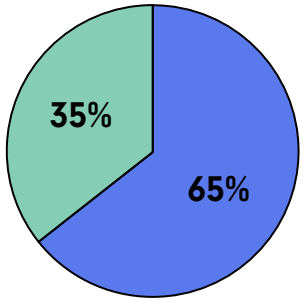
From 500 learners who completed an initial questionnaire providing feedback about the training, 100 (20 percent) of the learners responded to a more in-depth follow up survey in August 2019 and 65 (sixty-five percent) reported that they:

- Now used very secure pass phrases on all their devices
- Were either using or planned to use a password manager
- Were more vigilant about checking for scam emails at home and at work
- Felt knowledgeable about spotting unsecure websites.

Learner outcomes 2018-2019

Yes No

» **Now used very secure pass phrases on all their devices**
» **Were more vigilant about checking for scam emails at home and at work**
» **Were either using or planned to use a password manager**
» **Felt knowledgeable about spotting unsecure websites**



Covid impact 2020

The outbreak of Covid which started in early 2020 resulted in a massive shift in the method of workshop delivery not only for the Cyber projects but for all of SUL's core projects.

Fortunately, Digital Skills Education Ltd was already well prepared for these changes and managed, over a very short period of six weeks, to change the entire cyber workshop programme by amending and rewriting the training to make it interactive and deliverable online.

As virtual training was a new concept for many of the unions, ULRs, members, workers and employers, additional elements were included in the workshops covering training on the use of online platforms.

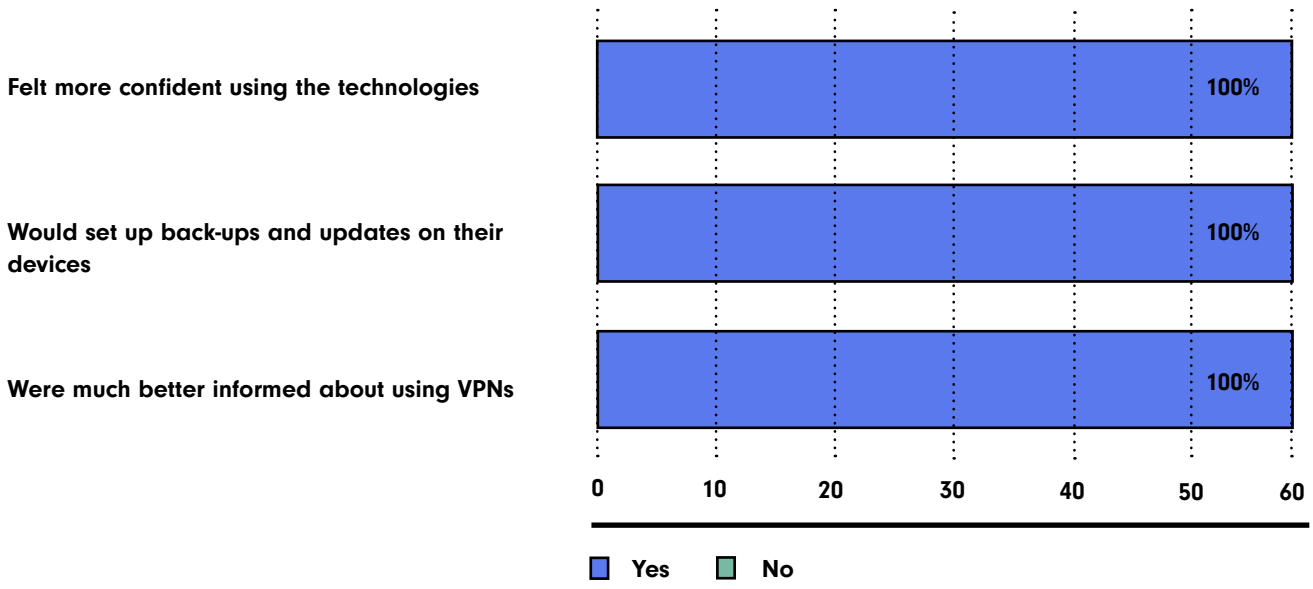
From 2020 to 2022, the number of learners attending workshops continued to increase as it was easier for many of them to participate in training online, as they were either furloughed and/or working from home.

January to March 2020 & May 2020 to March 2021

From 182 learners who completed an initial questionnaire, 100 (fifty-five percent) stated that they would be willing to provide further feedback about the training and 60 (sixty percent) from the 100 replied to a more in-depth follow up survey in March 2021. From the 60 who replied, one hundred percent reported that they:

- Felt more confident about using the technologies
- Would set up back-ups and updates on their devices
- Were much better informed about VPNs.

Learner outcomes 2020-2021

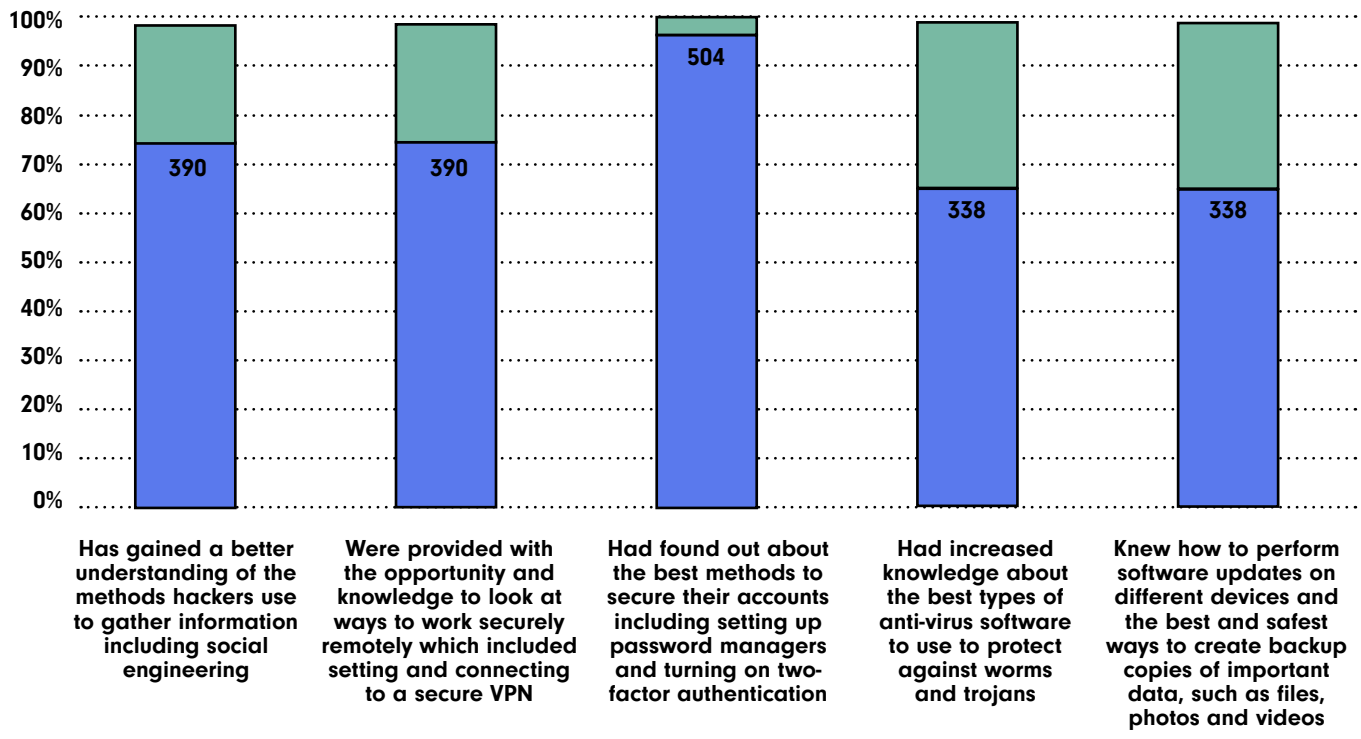


September 2021 to March 2022 & October 2022 to March 2023

As well as continuing to deliver core workshop training online from the period 2021 to 2023, highlights included the development of double bill, four-hour workshops which provided more in-depth knowledge for learners who wanted to cement their existing knowledge and increase their cyber skills levels. A total of 520 learners attended these workshops and reported that they:

- Had gained a better understanding of the methods hackers use to gather information including social engineering, 390 (seventy-five percent)
- Were provided with the opportunity and knowledge to look at ways to work securely remotely which included setting and connecting to a secure VPN, 390 (seventy-five percent)
- Had found out about the best methods to secure their accounts including setting up password managers and turning on two-factor authentication, 504 (ninety-seven percent)
- Had increased knowledge about the best types of anti-virus software to use to protect against worms and trojans, 338 (sixty-five percent)
- Knew how to perform software updates on different devices and the best and safest ways to create backup copies of important data, such as files, photos and videos, 338 (sixty-five percent)

Learner outcomes 2021-2023



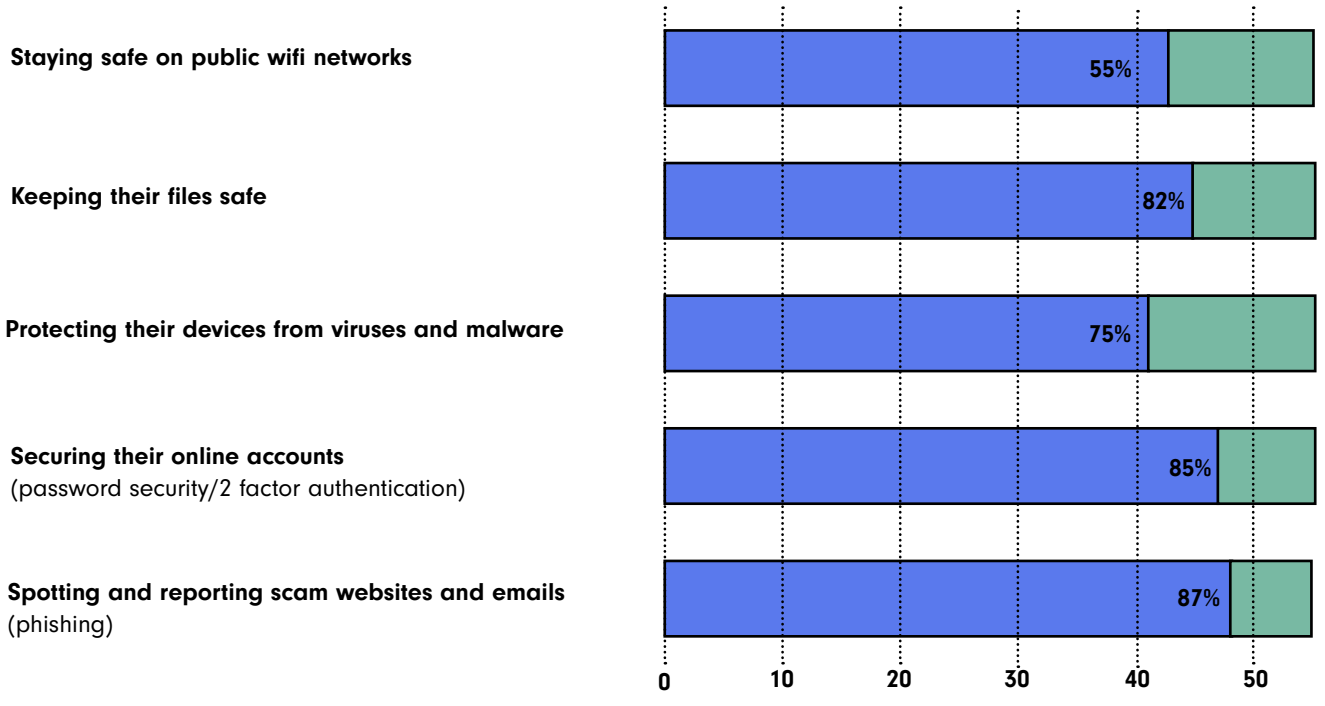
All of the learners who attended the double bill workshops received a CPD Certificate and badge.

April 2021 to March 2022

From 255 learners who attended 90-minute workshops and completed an initial questionnaire providing feedback about the training, 55 (22 percent) of the learners responded to a more in-depth follow-up survey in March 2022 and reported that they:

- Had spotted and reported scam websites and emails (phishing), 48 (eighty-seven percent)
- Secured their online accounts using password security and two-factor authentication, 47 (eighty-five percent)
- Protected their devices from viruses and malware choosing antivirus software updates, 41 (seventy-five percent)
- Keeping their files safe - encryption and backup strategies), 45 (eighty-two percent)
- Staying safe on public Wi-Fi networks using a VPN, 43 (fifty-five percent).

Learner outcomes 2021-2022



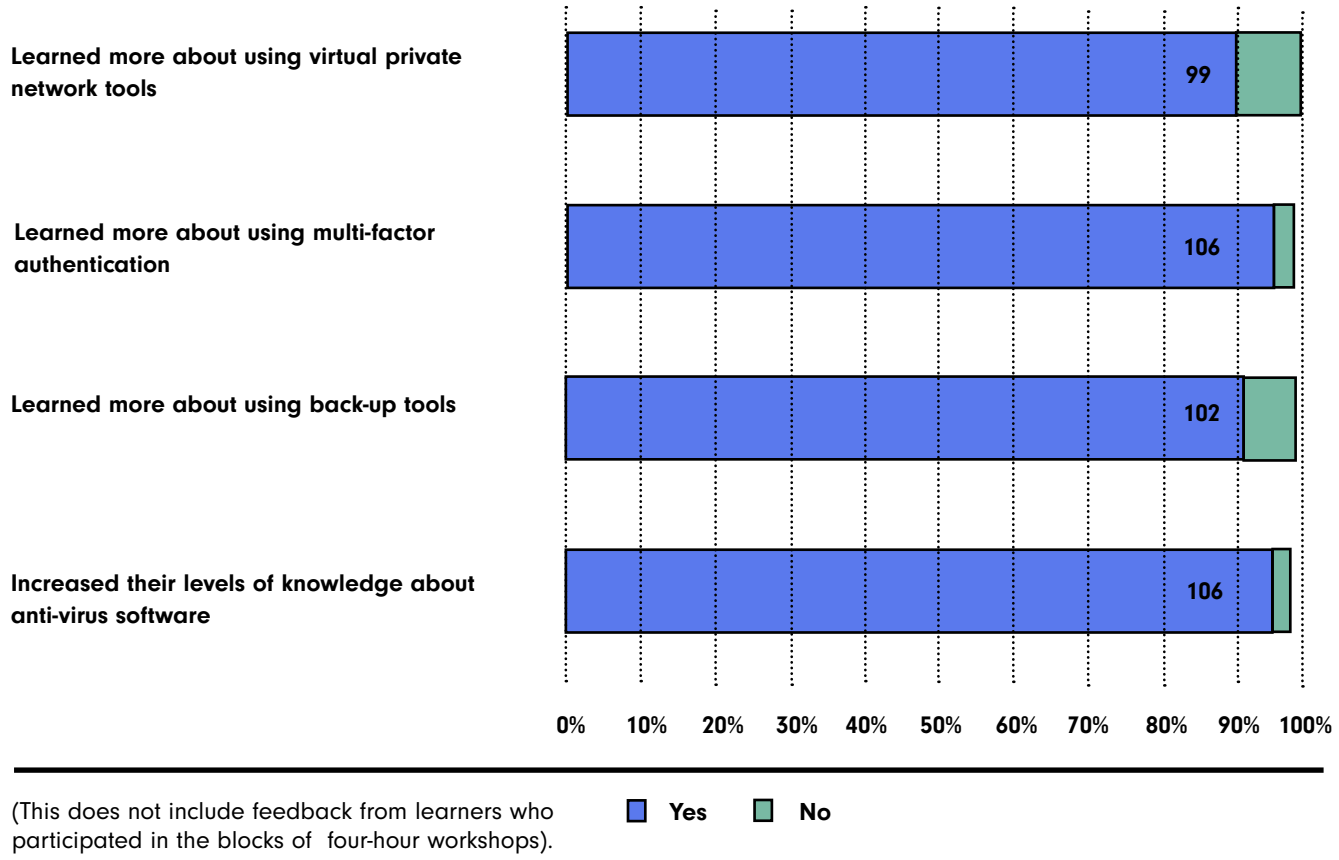
(This does not include feedback from learners who participated in the blocks of four-hour workshops).

September 2022 to March 2023

From 668 learners who attended 90-minute workshops and completed an initial questionnaire providing feedback about the training, 110 (16 percent) of the learners responded to a more in-depth follow-up survey in March 2023 and reported that they had:

- Increased their levels of knowledge about anti-virus software, 106 (ninety-six percent)
- Learned more about using back-up tools, 102 (ninety-three percent)
- Learned more about using multi-factor authentication, 106 (ninety-six percent)
- Learned more about using virtual private network tools, 99 (ninety percent).

Learner outcomes 2022-2023



(This does not include feedback from learners who participated in the blocks of four-hour workshops).

October 2023 to March 2024

The overall objectives and focus changed during the last project in 2023-2024. Based on demand from unions, ULRs and workers a new 'Digital Wellbeing' topic was introduced and included building cyber resilience using mobile phones.

Workers had reported that digital wellbeing combined with cyber security was a growing concern, and this was particularly true in sectors where workers may be from disadvantaged and/or underrepresented backgrounds; employed in emotionally challenging and often low-paid jobs with little or no chance for career development.

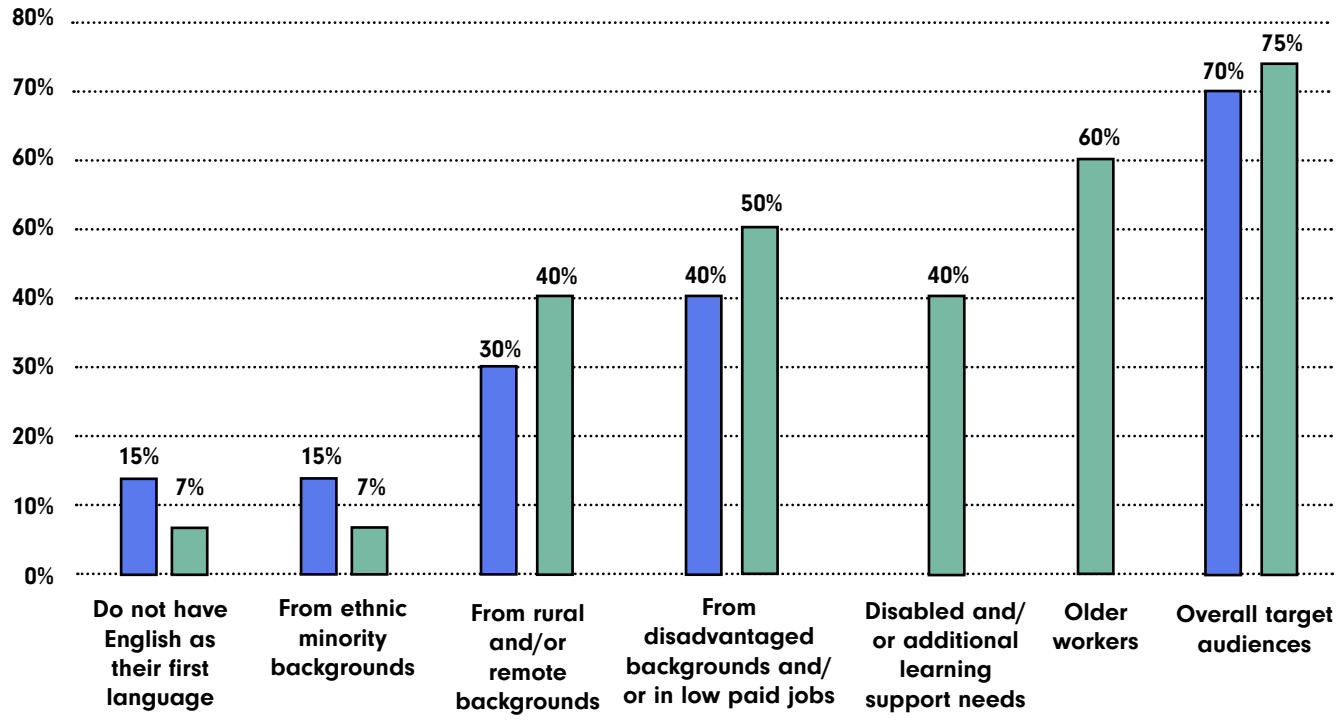
From a cross-union sample of 150 workers in early 2023, 105 (seventy percent) reported that they had concerns about the impact of technologies and digital services on their emotional health and were worried about their information getting stolen or being misused online.

In order to support and develop the skills of workers, a new course was developed that combined digital wellbeing and improved the cyber resilience skills of workers. The 'wellbeing' theme and focus attracted a wider audience of workers who would not normally attend a traditional cyber security course.

In addition, new objectives were set by and agreed with the Cyber Resilience Unit with a request that seventy percent of the learners should identify themselves from one or a combination of the following underrepresented groups:

- Disadvantaged backgrounds and are in low paid jobs
- English is not their language
- Ethnic minority backgrounds
- Live in rural and/or remote communities
- Disabled and/or have learning support needs
- Older people.

Learner outcomes 2023-2024



(Targets for learners who do not have English as their first language and learners from ethnic minority backgrounds were only partially met, despite liaising with relevant groups. Specific targets were not set for Disabled/ALSN or Older workers. However, overall targets were exceeded and many people identified as coming from multiple underrepresented groups).

From the 961 learners who completed an initial questionnaire, about the training, 961 (one hundred percent) reported that they:

More in-depth follow up feedback is available in the Impact Report submitted by Digital Skills Education Ltd.

- Felt much more confident about being able to spot and deal with a cyber threat
- That the standard of training provided was excellent
- Felt there had been an improvement in their digital wellbeing and levels of cyber resilience
- Had learned more about the tools available on their mobile phones to help to keep them more secure

Train the Trainers

In order to extend the reach of the cyber security training, the Scottish Cyber Resilience Unit requested that the development and delivery of a cyber security 'Train the Trainer' programme should be included in the 2018-2019 funding application, which was further extended into the 2020-2021 application. To support the training a downloadable resource pack and lesson plans were produced.

The targets across the two years were to train a minimum of 180 ULRs to deliver the training to a minimum of five learners each, in their workplaces. Although the targets were exceeded for the number of ULRs attending the training 391, they found it very difficult to get release to deliver a half-day, one-day or two-day course in their workplaces. In addition, it was difficult to get release for the learners to attend a longer course and only 100 learners received in-depth cyber training.

The delivery of the 'Train the Trainer' course ceased in May 2021 and subsequently the number of workshops were increased as it was easier to negotiate release for shorter courses and encourage more learners to attend the training.

Workers' Toolkit

In 2021-2022 an interactive toolkit was developed with Digital Skills Education Ltd and a small Focus Group of Union Project Workers from CWU, EIS and RMT. Developments included checking accessibility and, for example, potential usage blockages on work devices. The content was based on the previous Cyber Aware Campaign covering the six actions outlined but was adapted for Scottish workers. Interactive prototypes for modules were successfully developed and tested on CWU work devices. The toolkit included a:

- multimedia presentation (slides, video, narration)
- tutor lesson plans including frequently asked questions and recommended responses
- key discussion points, and quiz questions to check learning and understanding.

The Toolkit was rolled out and four demonstrations were delivered with over 100 cross union ULRs and workers by the end of March 2022.

The Toolkit currently gets used by approximately 100 learners each month and has reached over 4000 learners across Scotland.

To date, four unions have embedded the Toolkit in their Learning Platforms. Feedback from a sample survey found that one hundred percent of the learners felt the toolkit was useful and informative, and one hundred percent faced no technical issues using the toolkit. Names and details of learners using it are not stored. The Toolkit superseded the downloadable resource pack and lesson plans.

Video Lessons

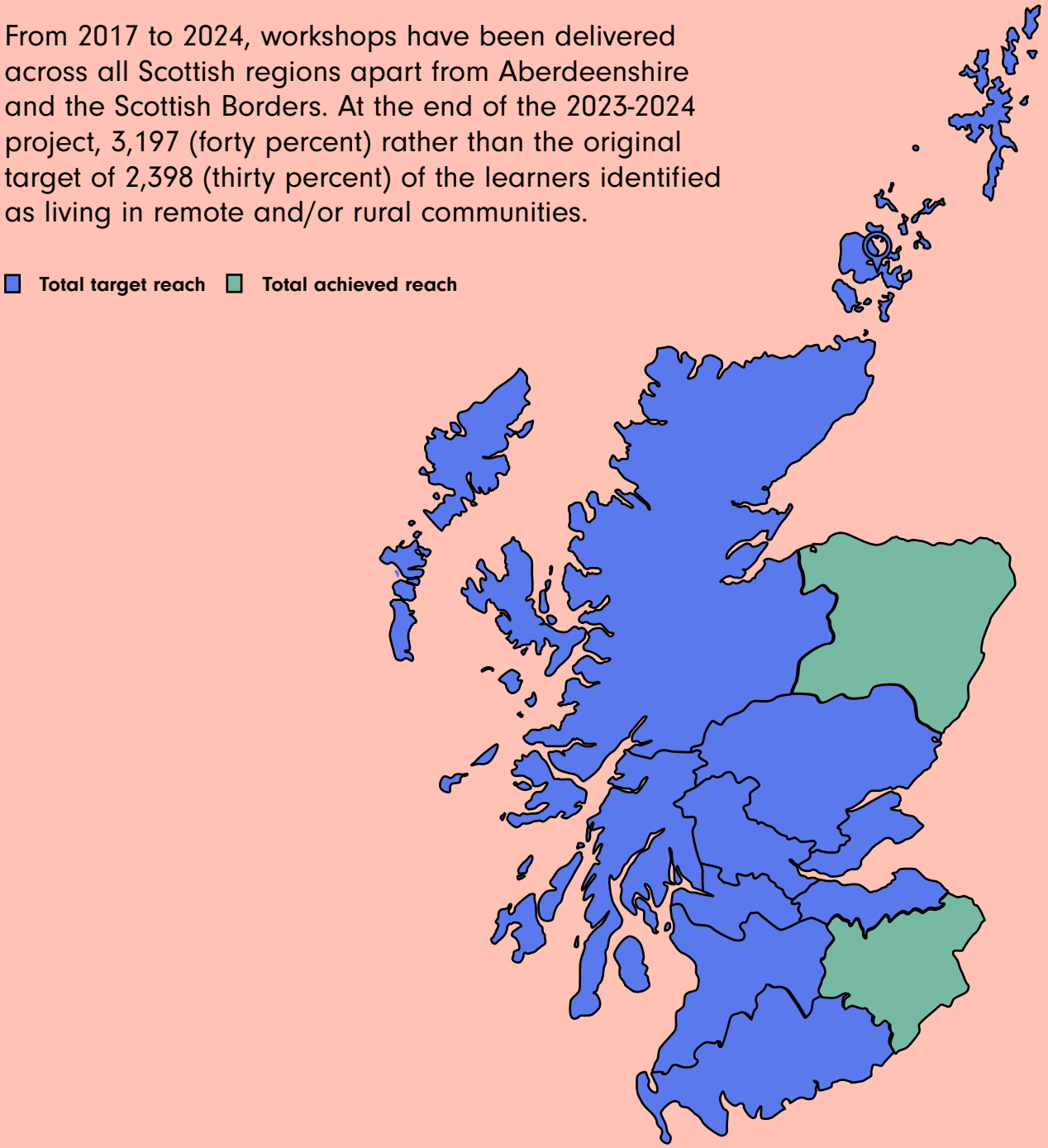
To supplement the Toolkit, four stand-alone videos were produced by Digital Skills Education Ltd in 2022-2023 to provide learners with the opportunity to complete cyber security training online. To date, over 900 learners have completed the training.

Sectors

From 2017 to 2024, 5,595 (seventy percent) of the learners identified as being employed in the public sector 1,599, (twenty percent) from the private sector and 799, (ten percent) from the Third Sector or did not respond to the question. This feedback is in line with the original targets.

Geography

From 2017 to 2024, workshops have been delivered across all Scottish regions apart from Aberdeenshire and the Scottish Borders. At the end of the 2023-2024 project, 3,197 (forty percent) rather than the original target of 2,398 (thirty percent) of the learners identified as living in remote and/or rural communities.



Unions

Throughout the lifetime of all the projects, the development and delivery of the training was supported by 37 unions. These unions provided access to employers and learners from practically every sector in Scotland. In addition, they helped to recruit learners through promotional and publicity initiatives and provided access to a network of ULRs in workplaces.

Partners

Throughout all the projects, partnerships continued to be developed with 35 external organisations to promote the cyber workshops and over 200 learners from partner organisations attended workshops.

Marketing, Promotions and Publicity

From the start of the first project in 2017-2018, a major marketing and publicity campaign was delivered to make employers, unions, ULRs, members, workers, and partners aware of the cyber security projects and to attract learners to participate in the training.

By the time the 2020-2021 projects were delivered, it was no longer necessary to focus on a marketing drive as information about the training had effectively been spread by Word-Of-Mouth (WOM), which was based on the quality of the provision, reputation, and trust in the training provider. In addition, there was a waiting list of learners who wanted to participate in the workshops at the end of each project year and the restrictions imposed by COVID from 2020 prevented many potential face-to-face interactions at public activities, and events.

From 2017 to 2024, 10,840 primary interventions were achieved as follows by:

- Delivering promotional activities using stalls at AEGON; HMRC in Edinburgh and Livingston; the Hutton Institute in Dundee, Lloyds Bank the STUC in Glasgow; Inverness Council; ASLEF and RMT train stations; FDA and PCS at DFID in East Kilbride; Usdaw Tesco stores and Tesco Bank across Greater Glasgow and the office in Glasgow
- Delivering promotional activities at Conferences and Events at the EIS AGM in Dundee and Conference in Glasgow; GMB Women's Conference in Glasgow; POA Conference in Peebles; Zero Waste Scotland Event in Hamilton, Newbattle Abbey College Conference; STUC Congress; STUC Women's Conference; SUL Conference and SUL Everyday Skills Event and H&I Conference
- Delivering promotional activities at 15 Book Week Scotland stalls with CWU, EIS, NUJ, RMT, UNISON and Usdaw
- Distributing promotional flyers to unions, workers, employers and partners
- Sending emails and electronic promotional newsletters to unions, ULRS and workers SUL and unions using social media to tweet and retweet cyber messages
- Producing articles for union magazines
- Producing case studies for reports and promotion in the SUL Annual Reports.

Marketing, Promotions and Publicity

Marketing and promotional activities were limited from 2020 to 2024, unless specialist training was delivered, as word-of-mouth (WOM) referrals based on the high-quality reputation of both the trainers and training on offer resulted in workshops being regularly oversubscribed and the subsequent growth of waiting lists each year.

Challenges and Solutions

Delayed Start Dates
Delivered more workshops over a shorter period of time to reach targets during the timescale of most projects.

Workers did not have time to participate in drop-in, bite-sized sessions at promotional stalls during the first couple of years of the projects.
Promoted and delivered shorter interactive presentations and workshops to provide learners with a better-quality experience, and additional skills.

Takes up to six weeks to negotiate release with employers and often it was necessary to 'sell' the benefits of training to employers
Increased awareness raising, promotion and negotiations helped to bring employers on board. There was a strong emphasis on the importance of changes in data protection laws as a result of GDPR and organisational benefits of having more 'cyber aware and skilled' workers. Word-of-mouth (WOM) proved to be an invaluable incentive, as those who participated in the workshops informed employers, managers and supervisors about the high standard of the training and skills development opportunities on offer. This encouraged them to organise release for workshops in the future and in turn, increased demand and improve cyber safety.

Often proved difficult to differentiate reps from members and workers and members from non-members as not all the participants provided this feedback in the evaluation forms
Reps were easily identifiable at SUL Conferences, Everyday Skills Events and ULR Development Days. As all reps and members are workers, they were counted together and included in the workplace statistics. In addition, workshops are open to all, regardless of union membership.

Delivery of some of the workshops were delayed due to the outbreak of Covid in 2020
The method of delivery was changed to online and delayed workshops were rescheduled and exceeded targets in June 2020.

Due to the repercussions of Covid, workshops could no longer be delivered face-to-face
Workshops were adapted and content re-written to deliver virtual learning online.

From 2020 identification of participants and feedback became more problematic as normally there was one hundred percent feedback from face-to-face workshops. This resulted in a lower than anticipated initial feedback response online
Followed up with online questionnaires and surveys with the participants who left their contact details and produced feedback and statistics based on the information available.

Delivery of the SMS pilot phone course with 125 learners in 2020-2021. Due to technical difficulties and delays with the text messaging software, the SMS pilot phone course was not delivered
Increased the number of workshops to compensate for any potential shortfall in numbers. As an alternative, used mobile phones as delivery devices for the workshops during 2023-2024 project.

Impact and Legacy

The following key examples highlight some of the short-term and long-lasting impacts the cyber skills training has achieved in workplaces:

- Where employers understood the benefits of cyber training, senior managers and supervisors attended workshops with workers, for example with FDA at DFID and GMB at STUC. This changed employer perceptions and provided opportunities to develop future cyber security strategies between employers, unions and workers.

- As a result of the intensive awareness raising campaign, marketing and publicity strategies and success of the workshops, unions are more aware of their cyber and data protection responsibilities as employers and have been consistently negotiating to instigate changes in their workplaces.

- In 2024, SUL received 27 applications for SUL Development Fund projects and stand-alone Learning Fund projects which included plans for digital and cyber resilience at strategic and operational levels in their 2025-2027 bids.

- Cyber updates are now regular items on the agendas at the Everyday Skills Group meetings reaching over 20 unions and partner organisations Dyslexia Scotland, Dyslexia Scotwest and the WEA, every quarter.

- As a result of attending SUL's cyber security and data protection, and 'Train the Trainer' workshops, the Communication Workers Union (CWU) offered an NPA, SCQF Level 6 accredited cyber qualification for BT workers. This is the first union in Scotland to organise an accredited cyber qualification and over 50 workers registered to attend the training. To date, 15 BT engineers and call centre workers from BT Consumer and Business departments attended the course. The training is provided by Glasgow Clyde College and is funded through SUL's Learning Fund budget, and runs for 20 weeks, (60 hours in total). There is no funding from the employer for this type of training.

- As a result of the cyber security and data protection, and cyber 'Train the Trainer' workshops delivered for Usdaw, Digital Skills Education Ltd delivered Cyber workshops for Usdaw in England. Although this is out with the funding and scope of the Scottish projects, it demonstrates how WOM has extended reach to other parts of the UK.

- There are waiting lists for workshops at the end of every financial year and over 150 potential learners are on the current waiting list.

As a result of and Cyber Security projects, additional bespoke courses were developed and delivered by Digital Skills Education Ltd that have either been paid for by the SUL Learning Fund or by unions. To date, these include specialist bespoke courses for:

- workers with additional learning support needs at RSBi in Glasgow with Community
- teachers with EIS
- professional footballers with PFA (Scotland)
- learners who are dyslexic with Unite and Dyslexia Scotland
- SEPA after a major security breach in 2021
- RMT Calmac, which are now included on a permanent basis as part of the apprenticeship training.

Conclusion

Based on the levels of participation from unions, ULRs, workers, employers and partners, there is no doubt that the funding for the Cyber Security projects has helped to increase the cyber security skills of thousands of learners across Scotland and made them feel more confident and secure when they are using new technologies.

Feedback from learners has been overwhelmingly positive about the content and quality of the training and the flexible approach and professionalism of the Digital Skills Education tutors.

The following case studies provide a snapshot of some of the successful cyber security interventions that have taken place in workplaces.

Appendix

Personal Cyber Security

Community Union and Whistl

Eleven members of Community Union at the Whistl Depot in Tannochside participated in a Personal Cyber Security workshop in September 2017, delivered by Digital Skills Education Ltd. Based on the feedback from the evaluation forms at the end of the workshop, all the participants said that the training provided them with the incentive to learn and were more confident in their ability to learn.

Prior to taking the course, five learners said they had "basic knowledge" of cyber-related issues, one learner said "medium knowledge" and the rest said, "none." After the course, 100% agreed that they had more knowledge of cyber-related issues.

The learners responded that they had different things to take back to the workplace, including:

- how to keep online accounts safer and secure;
- to never use the same password for accounts;
- to be more protective of personal passwords; and
- the importance of cyber security and online security.

The learners also responded that they found it most interesting to learn:

- how to secure a computer;
- to protect important data from breaches;
- the importance of strengths of passwords;
- how to create passwords that are safe and spot fake websites; and
- how easy it is for your computer to be hacked if it is not secure.

> "Very eye opening experience! I enjoyed every minute of the workshop, it has made me become more aware about password security and hacker organisations and how to spot fake emails/text messages."
>
> - Learner, Community Union -

Cyber Resilience

Three Unions, Three Sectors, Three Perspectives

POA Scotland

POA Scotland represents Uniformed Prison Grades and staff working within the field of Secure Forensic Psychiatric Care. One learner attended an interactive presentation at the POA Conference in Ayrshire in October 2017, and a workshop at the Scottish Union Learning Conference in November 2017. The POA learner knew a reasonable amount of information about cyber security prior to the course, including phishing, spam, passwords, etc., and used digital skills on a regular basis at work and at home. However, since taking part in the training, the learner indicated that he knew more about weak passwords and making passwords more secure, which he plans to use in his workplace and personal life. He said: "As a direct result of the workshop, I have installed and am now using 'sticky password' to be more secure." The learner has shared his new knowledge about how to set secure passwords and spot fake emails with at least 30 reps and members across the prison service.

> "Training on personal cyber security is very important for prison officers. For example, one PO had to change all his personal details on Facebook because of offensive posts from an ex-prisoner. Security training and social media awareness are essential to keep our families and personal lives safe."

ASLEF

ASLEF is Britain's trade union for train drivers. An ASLEF learner attended a Personal Cyber Security workshop in February 2018. Although he knew a fair amount about cyber security prior to the workshop, he was really interested in protecting himself online. After the workshop, the ASLEF member said he uses the information he learned about password security in the workplace and shared the information and tips he learned. He said: "I told my wife and a fair few of my friends. I feel better knowing that they are being safer online, too." The learner feels he now has more knowledge on cyber security and wants to learn more. He said: "I certainly know now how to look out for spoof emails and spoof websites, and I'm more aware of what phishing looks like. I will be on the lookout for Cyber Security and GDPR as both are updated."

Usdaw

Usdaw is the union of shop, distributive and allied workers. Prior to attending a Personal Cyber Security workshop, one Usdaw learner had very limited knowledge on the subject, and had just heard through the media about cyber attacks. She said: "I learned so much about passwords, and not using the same one for everything. I also learned to check for 's' in 'http://' for genuine, secure websites." The Usdaw learner has shared what she learned with friends, family and colleagues, and has changed her own passwords to be more secure. She would like more courses like this to be offered in the future, to bring cyber security to the attention of more members in her union.

Cyber Resilience

PFA Scotland

PFA Scotland handles sensitive information about its union membership of 1,300 football players across Scotland, many of whom are regularly exposed to media scrutiny and at risk of unwanted intrusion into their personal lives.

Aware of imminent changes in data protection laws to tighten up on personal and workplace cyber security, combined with an identified need to improve the way they hold and use footballer data, workers based at PFA Scotland HQ were invited to attend over four hours of training on personal cyber security and personal data protection in November 2017.

The PFA HQ Office Manager had reasonable knowledge of the importance of cyber security and impending legal changes based on the introduction of the new General Data Protection Regulation (GDPR), but the other team members had very little knowledge about cyber security and the legal implications of mishandling data. In addition, the workers were somewhat reticent about attending the workshops, thinking that the subject matter might be dull, and resented spending a day away from their core work. However, after attending the workshops, all workers stated that they were very satisfied with the course content and the level of knowledge and abilities of the tutors. In addition, they felt that the workshops provided them with the incentive to learn more, increased their confidence levels and their ability to learn. They were surprised how much they enjoyed the workshops and particularly liked the inclusion of 'shock factors' in the content to emphasise the cyber security message! They now felt they had an understanding of the relevance of the training for both their personal and working lives.

Overall, workers gained a better understanding about the reputational damage and financial risks a personal data breach could cause for the organisation, if details about their members are leaked and used for inappropriate purposes. PFA Scotland is currently exploring how to safely update 1,300 members' contact details and liaising with Scottish football clubs about cyber security and data protection practices.

From November 2017 to March 2018, PFA Scotland has worked to embed cyber resilience into its personal and workplace structures and systems and procedures in place, including:

- the office has been fitted with a double-lock and extra security;
- all manual records and data are now secured and locked in a safe;
- an additional worker was appointed, on a short-term basis, to scan all manual records and data, which were entered onto an online Customer Relationship Management System (CRM). The worker was briefed on the updated PFA Scotland internet, social media and security policies and signed a confidentiality agreement;
- all workers changed their passwords to make them more robust and secure; and
- the Office Manager sends a monthly email reminder to the team, to continue to keep manual and electronic records secure. Regular notifications about cyber security are also put on the staff noticeboard.

PFA Scotland has requested further training from Scottish Union Learning. This includes participating in personal cyber security refresher workshops to keep their skills up-to-date. Now that they understand cyber security basics, PFA Scotland would benefit from more advanced, or in-depth training on social media and data protection.

> "Really interesting session. Well delivered. Given me lots of things to think about regarding IT and security."
>
> - Office Manager, PFA Scotland -

Personal Cyber Security
CWU, BT Glasgow

Communication Workers Union (CWU)

CWU represents members in postal, telecom, mobile, administrative and financial companies including Royal Mail Group, UK Mail and BT, Telefonica O2, Virgin Media, EE and Santander, as well as outsourcing company Capita.

Telecommunication members from CWU at BT in Glasgow attended a cyber security workshop in September, 2018 which was delivered by Digital Skills Education Limited.

The workshop covered essential cyber security issues such as how to browse online safely, increase password strength and spot scam websites, and phishing attacks.

All of the learners who attended found the workshop to be a good length, felt more confident about what they learned and planned to share the knowledge with their colleagues.

Overall, feedback was positive with several members reporting that they found 1Password a very useful tool for remembering all their individual passwords and making it easy to log in to multiple sites.

Another member thought the equipment was great and the tutors were knowledgeable, explained content details clearly, listened to what people had to say, were easy to follow and very helpful.

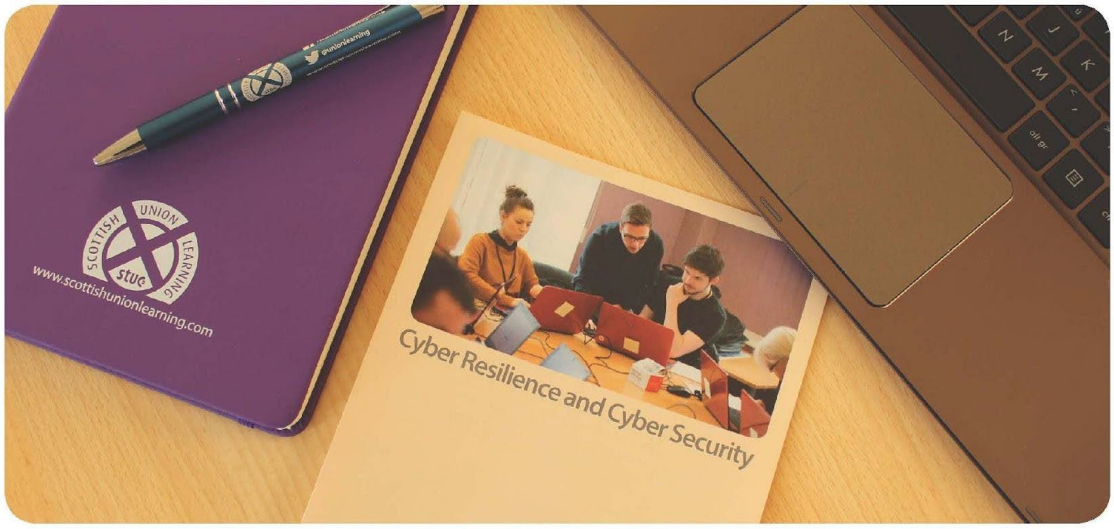
All the members were interested in attending further cyber security training.

"Really enjoyed the content. Delivered in a fun and interesting way. Learned a lot today, thanks."

"Very well presented, easy to understand the content. Learned something new."

Learners, CWU

Personal Cyber Security
BDA, NHS Shettleston Health Centre



British Dietetic Association (BDA)

The BDA is a trade union and professional body representing the professional, educational, public and workplace interests of the whole dietetic workforce, including practitioners, researchers, educators, support workers and students.

Members of the BDA attended a personal cyber security workshop delivered by Digital Skills Education Limited at NHS, Shettleston Health Centre in October, 2018. The members learned about the importance of protecting their passwords online, how to spot a phishing attack and identify fake websites.

All of the members indicated that attending the workshop had increased their confidence and would share their new knowledge with colleagues.

One member found the information about passwords particularly helpful and advised that they would now use a password manager to secure their online data. Another member found the additional security provided by the application of 'Two Factor Authentication' very useful.

All of the members who provided feedback advised that they had changed their passwords, which is a fantastic result and drives home the importance of cyber resilience training.

In addition, all the members who completed the evaluation form reported that they would recommend the workshop to others, and over half of these learners were interested in further training.

> "Really interesting and effective training course in a subject I previously found rather dull and uninteresting. Well done, I really enjoyed it and learned loads."
>
> Learner, BDA

Personal Cyber Security and 'Train the Trainer'
RMT and Scotrail

The National Union of Rail, Maritime and Transport Workers (RMT)

Nicola Melling is a Union Learning Rep (ULR) at RMT. She works as a Ticket Examiner for ScotRail, where her duties include inspecting, checking and selling tickets to passengers, providing them with information, and assisting travellers with reduced mobility.

Aware of the importance of cyber security in both her personal and working life, Nicola attended a personal cyber security workshop and a personal cyber 'Train the Trainer' workshop delivered by Digital Skills Education Ltd at the STUC, in October 2018.

During the cyber security workshop, Nicola found out how to set secure passwords, spot fake websites and keep data safe online. During the 'Train the Trainer' workshop, Nicola was provided with the tutoring skills to deliver "bite sized" cyber security modules on how to choose safe passwords and safer web browsing.

Shortly after attending both workshops, Nicola delivered a two hour cyber security training session with RMT members in her workplace. The session covered how to create strong passwords and use password managers such as 1Password, Dashlane and iCloud Keychain. Nicola discovered that the learners really enjoyed testing the strength of their current passwords against an online password checker, and completing the interactive 'Diceware' random password generator exercise to create more secure passwords.

Nicola thought that taking part in the 'Train the Trainer' workshop made her feel more confident about sharing her knowledge with others, and gave her the best tips to deliver a session herself. She suggested incorporating role-play into future workshops, but would definitely recommend it to other colleagues. Nicola was impressed with what she learned on both workshops and has been sharing this information with others.

> "I would definitely be interested in attending an additional workshop to develop my cyber tutoring skills, as I feel this would be an ever changing topic which would be a continual challenge in the future as hacking advances."
>
> Nicola Melling, RMT

Personal Cyber Security
GMB, Cartcraig Depot Glasgow

General and Municipal Workers' Union (GMB)

GMB is a general union which represents members from a wide range of jobs in the public and private sectors.

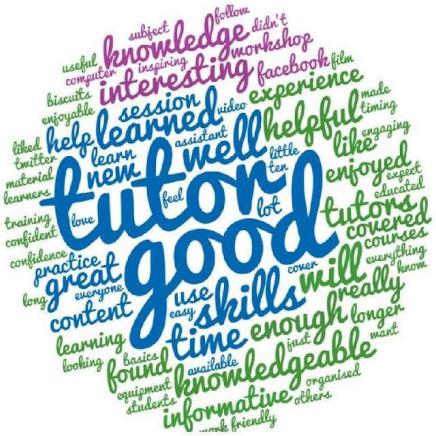
Digital Skills Education Ltd delivered a series of cyber security workshops for GMB members at Gartcraig Depot in Glasgow on 17 and 19 December, 2018.

The workshops were delivered in the Depot bothy and all the members found the information and interactive activities about setting secure passwords very helpful. They were surprised to learn that setting up a longer passphrase, consisting of unrelated words, was one of the best methods available to outwit computer hackers!

In addition, they found it useful to find out how it easy it was for hackers to get access to their details by sharing too much personal information on social media.

Most of the members who attended the workshops were manual workers who didn't use computers on a regular basis as part of their jobs. However, they did think that the skills they learned at the workshops would be useful when using their hand-held and mobile devices.

All the members reported that they would like further cyber training and half of them were interested in gaining 'Train the Trainer' skills.



"Learned how a password manager works. How to test a password and create a good one, or at least try to find helpful websites."

"Really good, learned loads in a short space of time and would like to be more clued up."

Learners, GMB

Keeping Online Meetings Safe and Secure

UNISON (delivered online)

UNISON, the public service union

Sixteen reps and members of UNISON attended a virtual Cyber Security workshop on the subject of 'Keeping Online Meetings Safe and Secure' – an increasingly important topic due to the mass home working undertaken as a result of the coronavirus pandemic.

As workers had to adapt to and be increasingly dependent on technology for both work and recreational purposes, this course used advice from the National Cyber Security Centre to share tips on how to keep video conferencing cyber safe. It included sensible steps participants could take to protect their privacy when using conferencing platforms such as Zoom, Skype, Hangouts and Teams.

This workshop was offered on three different time slots, on two separate days. This increased the accessibility of the course, allowing participants to work around working patterns and caring commitments. Feedback was overwhelmingly positive, with all learners reporting a high level of knowledge and understanding of the subject at the end of the course, and many requests for further workshops of this type.

"I have learnt so much from these courses. I think they are excellent, as I previously knew nothing at all about the subject, but the courses were presented extremely well in easy and interesting bite-sized learning sessions. The pace of the course is excellent and is very well taught."

"Love these short modules, would be great to have regular updates and also possible follow up sessions."

"I've never felt confident about computers before but have learnt so much from these courses. I feel more confident about using computers which will be very useful for my work."

Staying Safe on Social Media
UNISON and Unite (delivered online)

UNISON, the public service union, and Unite the Union, the UK and Ireland's largest union with members working across all sections of the economy, came together for this webinar in July 2020 to learn more about 'Staying Safe on Social Media'.

The 33 UNISON members and ten Unite members were joined by an additional 68 attendees, 42 of whom were members of 12 other trade unions, and 26 of whom were not trade union members. The webinar had been promoted as widely as possible, due to the increasing relevance of the subject in the post-Covid landscape, and uptake exceeded expectations.

Attendees learned how they could protect themselves and their families when using social media, and how to recognise some of the current socially engineered cyber-attacks related to Covid-19.

All participants who gave feedback indicated that their knowledge of Staying Safe on Social Media had increased as a result of the webinar.

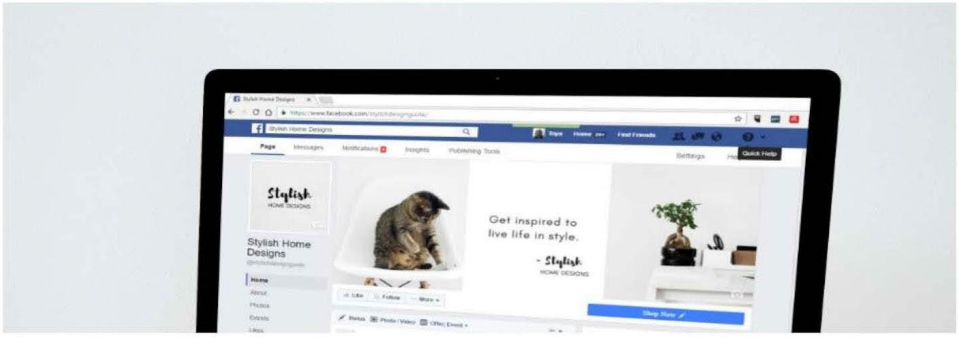
"Very effective at looking at how to spot

"Great update/ reminder on staying safe online."

"Excellent information at an easy-to-understand level."

"... highlighted issues I was unaware of and gave useful advice to protect myself."

"Great course. Everyone should watch this before registering on any social media."



Personal Cyber Security
USDAW, USDAW HQ, Glasgow

Union of Shop, Distributive and Allied Workers (USDAW)

Shop and depot workers attended a Cyber Security workshop at the USDAW office in Glasgow, to learn about how to stay safe online using stronger passwords and spot scam websites.

Feedback from the workshops was extremely positive with all the learners stating that they felt more confident about the subject, would be sharing their new knowledge with their colleagues, and had the incentive to learn more.

The workers developed new skills such as how to use a password manager app for multiple passwords on different sites.

They learned the importance of choosing a longer passphrase consisting of unrelated words, rather than a shorter password which was easier to guess. In addition, they found out about additional security options such as the benefits of switching on two factor authentication.

All of the learners said they would change their habits in the workplace after the training.

They indicated that they were interested in attending future "Train the Trainer" workshops and would deliver their own cyber security sessions with colleagues and union members using the cyber online toolkit designed by Digital Skills Education Ltd. This additional training will be delivered in Spring 2019.

"A new way of thinking about password security".

"Very well presented and easy to understand".

"Will change my passwords and use a password manager".

Cyber'Train the Trainer'

Scottish Union Learning Everyday Skills Event

Two, one-hour taster Cyber 'Train the Trainer' sessions were delivered at the Scottish Union Learning Everyday Skills Event at the end of February 2019.

Fifty-three cross-union Learning Organisers, Union Learning Reps and tutors participated in the sessions, and they all reported that they felt more confident about basic cyber security as a result of the training.

Forty-eight of the participants asked for the opportunity to develop their tutoring skills and attend more in-depth cyber 'Train the Trainer' workshops, in the future. In addition, they said that they felt confident enough to deliver basic cyber security password sessions with their colleagues in workplaces, show them how to use automatic ad blocking, and explore tracking protection options on easy-to-use private browsers.

"I am more confident about passing on the skills learned on the course".
BFAWU ULR

"The rest of the course looks really interesting and it will provide some great tools we can use with the different groups we work with".
UNISON Rep

"The ice-breaker was great, I look forward to attending the full session!" An engaging session from Craig, with some new online 'toys' to play with".
PCS Branch Learning Co-Ordinator

"Craig was an excellent tutor. He was very patient and delivered his presentation in a very professional manner. I particularly enjoyed the 'bingo' password session. It was a fun but informative workshop".
PCS Rep