# Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland

## Learning & Skills

Daniel Sellers





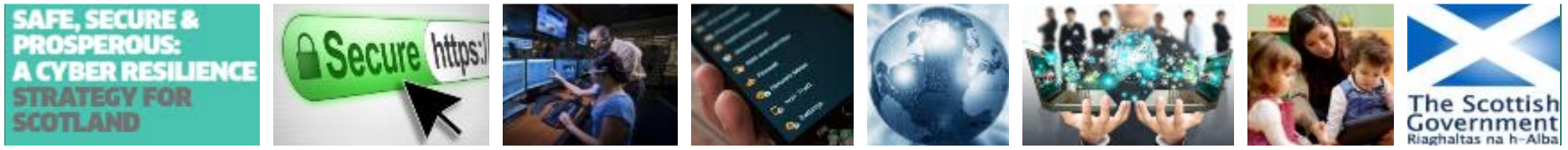

# Strategic Themes

Leadership and Partnership Working

Awareness Raising and Communication

**Education, Skills and Professional Development**

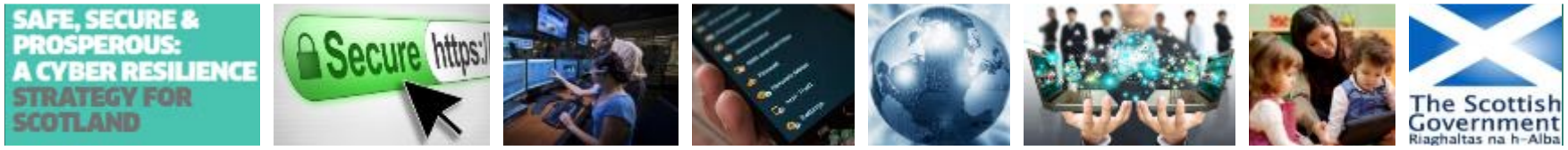
Research and Innovation



**Education**: the basics for all citizens

**Professional Development**: the basics for all workers using digital technologies (at all levels in workplaces) "digital end users"

**Skills**: cyber security specialist technical skills



We believe Scotland can be a nation that can claim, by 2020, to have achieved the following outcomes:

**people are informed and prepared**

**growing and renowned cyber resilience research community**

**businesses and organisations recognise the risks**

**global reputation as a secure place to live, learn and do business**

**trust in our digital public services**

**innovative cyber security industry**



# Continuum of learning and skills

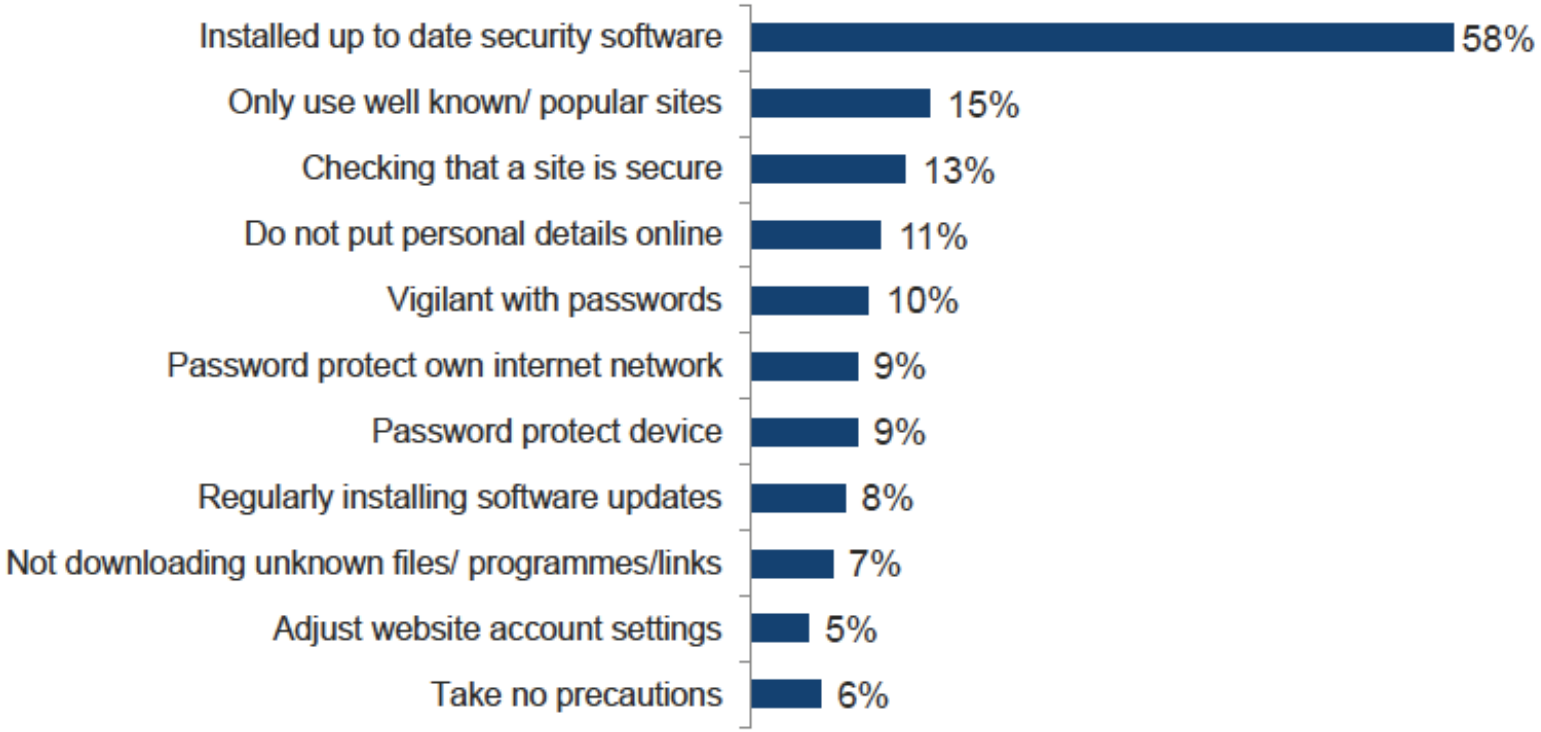
| activity → | awareness raising activity | embedding cyber resilience in curricula | embedding cyber resilience in workplace learning | developing cyber security specialist skills | upskilling in cyber security | building research capability and capacity |
|---|---|---|---|---|---|---|
| section of population targeted | general population | people, particularly young people, in education system, including in youth work and community learning | digital end-users in workplaces, employers | future cyber security specialists (currently in education or seeking retraining, or digital specialists wanting to increase their knowledge and skills) | existing ICT/digital specialists who need to increase their knowledge and skills in cyber security | research specialists, subject experts, innovators |
| sector of the education system | all, and beyond the education system | non-formal and formal (schools, colleges, universities, youth work, community learning) | non-formal and formal learning (workplace) | non-formal and formal learning (schools, colleges, universities, youth work, community learning) | workplace and/or specialist training (colleges, universities, private training providers) | formal (universities and research institutes) |






# General population

*When you are using the internet, what precautions if any, do you take to protect yourself online?*




Base: All who use the internet (888). Data collected 24th-30th August 2015

Source: Ipsos MORI




# Skills:

**Worldwide?**

In 2015 there were likely to be "more than 1 million unfilled security jobs worldwide" (CISCO)

As many as "3.5 million unfilled cybersecurity positions by 2021" (Cybersecurity Ventures)




# What we know (cont …)

**UK?**

UK has the third highest demand for cyber security professionals in the world, after Israel and Ireland.

UK has second biggest gap between employer demand and skills supply in the world: supply at under 50% of demand: 2 jobs for every applicant

Indeed Spotlight: the Global Cybersecurity Skills Gap 2017




# What we know (cont …)

**UK (cont …)**

Estimates:

18,000 – 24,000: number of filled cyber security posts in the UK between per year
3,600 to 4,800: number of posts vacant or or filled by contractors.

“conservative” forecasted growth rate of 20% p.a.

# What we know (cont …)

**Scotland?**

2017: 360 – 480 vacant or temporarily filled posts

2018: 430 – 580
2019: 516 – 700
2020: 620 – 840
2021: 740 – 1010

Outstripping the growth rate of digital technologies, which itself outstrips average sector growth rates




# Funded activity

**Learning:**

- Scottish Union Learning workplace programme
- UHI Perth “Managing Cyber Risk” qualification

**Skills:**

- SQA: New materials, new quals (HNC, HND, PDA)
- SDS: cyber security career promotion
- YoungScot: Cyber Security Challenge UK
- Cyber Security Xmas Lectures
- Cyber Bus

# Actions to improve cyber resilience learning …

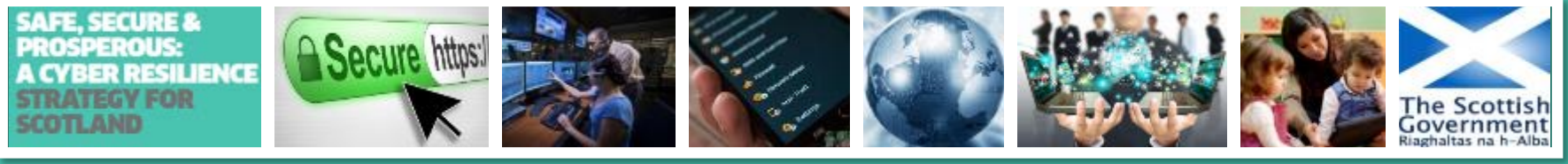



# Actions from draft action plan:

work with Regional Improvement Collaboratives to ensure the development of cyber resilience features explicitly in their regional planning

embed cyber resilience into appropriate skills frameworks - for example, with Scottish Qualifications Authority (SQA) on its review of the ICT Core Skill

collate and disseminate existing learning and teaching resources that support the learning of cyber resilience within the curriculum area of Digital Literacy, by spring 2018.



work with organisations involved in non-formal learning to develop and publish guidance for providers on the delivery of cyber resilience learning

strengthen the focus on cyber resilience in initial teacher education for teachers in schools and lecturers in colleges

embed cyber resilience in the reviewed quality framework for colleges, How Good is Our College?, within the principles of leadership, governance and curriculum




work with local authorities and colleges to establish cyber resilience as a key part of digital career-long professional learning for school teachers and college lecturers

explicitly identify cyber resilience within the upcoming review of the Professional Standards for Lecturers in Scotland's Colleges

work with the National Parent Forum of Scotland to identify activity to develop parents' abilities to support their children to be more cyber resilient




work with key partners involved in supporting the upbringing of children and young people, to identify activity to develop carers' abilities to support children and young people to be more cyber resilient

ensure that National Occupational Standards for professionals in supporting or caring roles include competences relating to supporting people to be more cyber resilient




# Find out more:

www.getsafeonline.org

https://twitter.com/cyberresscot

Scottish Government cyber resilience blog (which contains links to the public sector action plan consultation)

# Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland

## Learning & Skills

Daniel Sellers