
# CYBER SECURE SCHOOLS

by SWGfL

Safe, Secure, Online

## Preventing Digital Crime

Powered by Bitdefender

BUILT FOR RESILIENCE

# CYBER SECURE SCHOOLS

## Not long now...

Thank you for waiting

# CYBER SECURE SCHOOLS

by SWGfL
Safe, Secure, Online

Preventing Digital Crime

## 13.10.2021 13:00 -15:00

Powered by Bitdefender
BUILT FOR RESILIENCE

# Welcome

SWGfL is delighted to be able to host this inaugural CSS event.

With thanks to Bitdefender for supporting us

## Bitdefender

is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide.

Bitdefender
BUILT FOR RESILIENCE

## iCSS, University of Kent

is one of only 19 centres in the UK recognised as an Academic Centre of Excellence in Cyber Security Research.

GFCE University of Kent Institute of Cyber Security for Society (iCSS)

## Phoenix Software

are the UK's leading 100% Public Sector focused IT Solution and Service Provider.

PHOENIX

# Welcome

Ask any questions you have, at any time, in the Q&A, we'll get to these after all the presentations. Be sure to add the name of the presenter you're asking the question to.

Please complete our cyber security school survey at:
http://tiny.cc/CSSurvey

## SWGfL

are a not for profit charity ensuring everyone can benefit from technology free from harm. Part of the UK Safer Internet Centre, our experts advise schools, public bodies and industry on appropriate actions to take

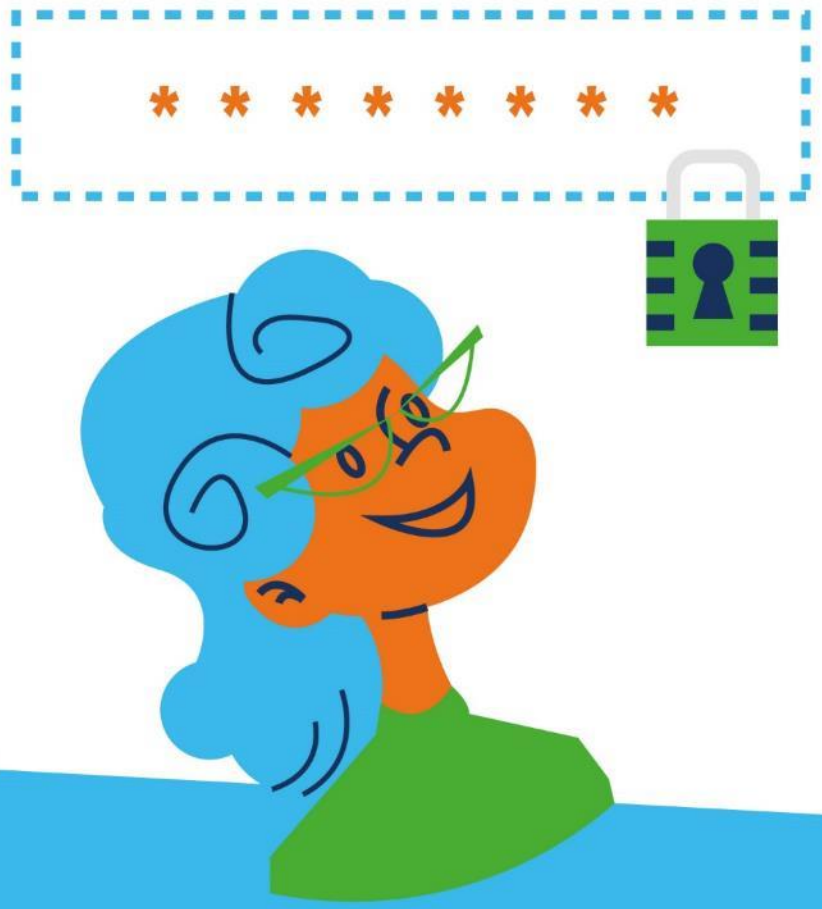
SWGfL
Safe. Secure. Online

## CySecAware

delivers cyber security training in real terms for real people in line with the best practices as stated by the UK's National Cyber Security Centre (NCSC). Providing expert knowledge of the threats and trends across all sectors.

CySecAware

# Education Threat Landscape



## Bitdefender

- Provides a vertical for threat actors to gain access to exploit sensitive information & intellectual property.
- Prime sector for cyber criminals due to valuable information stored on school networks & networks.
- Threat actors can use the foothold gained as a staging ground to target other industries.
- Targeting of business communications, research & relationships.
- Access to PII or financial information (grants, scholarship documentation, student and / or staff personal data).

Bitdefender®
BUILT FOR RESILIENCE

# ‘Prevention’ Reinvented

Modern security programs are outcome focused and designed to prevent *business impact*

MDR is 24/7 Security Operation, comprised of:

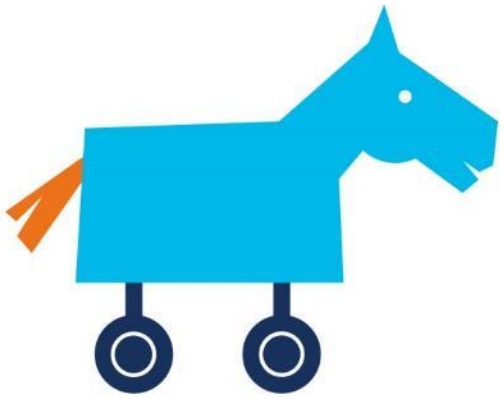
- People
- Process
- Technology

2 Key Questions:

1. If you were being attacked, would you know you were being attacked?
2. If you knew you were being attacked, could you respond to that attack?

# What we See

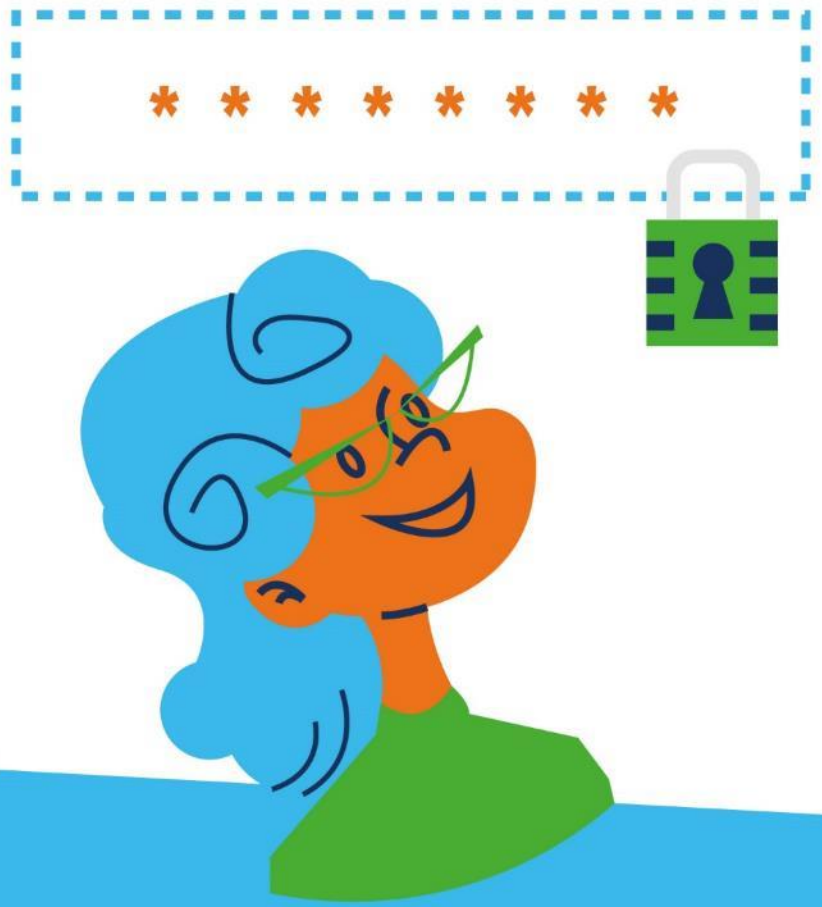
- School district email addresses discovered in various Darkweb database dumps.
- Over past 12 months, large volume of RansomWare attacks (Maze, Conti, Ryuk, Clop & Mailto).
- Targeted Phishing attacks.
- APT profiteering from access to sensitive personal, financial & research details.
- Hacktavists disrupting access through protest or to draw attention to a cause.



# How To Protect; What can you Do?

- EDUCATION!!! – Staff training and awareness.
- Comprehensive security & compliance plan that is “baked” into the organisation’s strategy & culture.
- Adopt a proactive means of monitoring to:
  - Detect rapidly
  - Respond immediately
  - Contain & remediate quickly
  - To minimise impact

# Understanding cyber security skills development in pre-university education



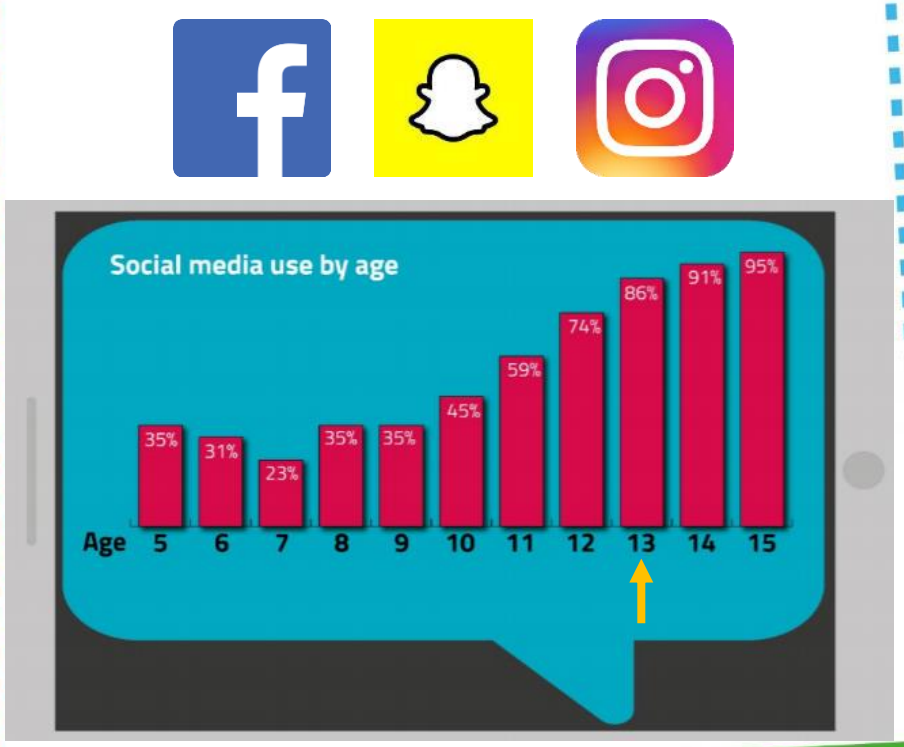
Virginia Franqueira,
University of Kent

Preliminary findings reported in this talk are part of an on-going research project funded by the GFCE (**Global Forum on Cyber Expertise**), and conducted by a group of researchers at the **Institute of Cyber Security for Society** (iCSS), University of Kent.

GFCE
Global Forum on Cyber Expertise

University of Kent | Institute of Cyber Security for Society (iCSS)

# Children are increasingly online




In 2020:

- 82% of children aged 3-4 went online
- 97% of children aged 5-15 went online
- 42% of 5-12 used social media

*Children and parents: media use and attitudes report*
Ofcom (April 2021)

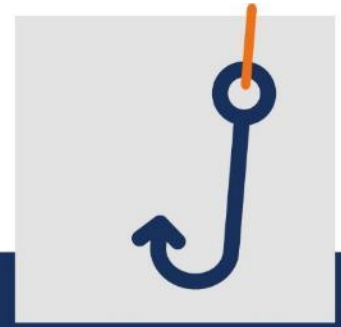
# Empowering children with skills to counter risks

## Access to content

- Inappropriate content
- Radicalisation
- Encouraging self harm

## Generation of content & personal data

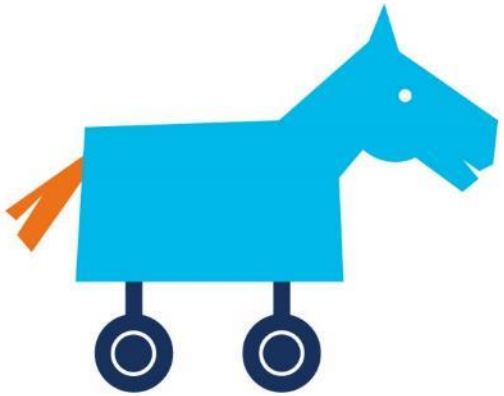
- Reputation damage
- Sharing with strangers
- Companies harvesting data



## Other risks

- Cyber bullying
- Pressure to spend money
- Excessive time online

*Children and parents: media use and attitudes report*
Ofcom (April 2021)



# Cyber security pre-university education

**We compared countries part of the UK and 5 other English-speaking countries in terms of…**

The extent of cyber security coverage and whether and how it is incorporated to pre-university curricula

# Countries in the UK

Different content coverage

Different approaches

## England

Cyber security is covered as **digital literacy** in the **Computing** subject of the national curriculum (academies do not need to comply).

## Wales

National curriculum does not incorporate cyber security content. Cyber aspects (e.g., identity, digital rights and online behaviour) are part of **Citizenship** according to the Digital Competence Framework (guideline).

## Scotland

The *Curriculum for Excellence* contains 'cyber resilience and internet safety' benchmarks for **digital literacy** – under the subject area **Technologies.**

## Northern Ireland

Cyber security (i.e., how to keep safe and display acceptable online behaviour) is covered in the national curriculum under **Using ICT** -- as cross-curricular skills.

# Cyber security / online safety coverage (UK)

| | Age reached in school year | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| **England** | x | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | * | * | x | x |
| **Wales** | x | x | x | x | * | * | * | * | * | * | * | * | * | x | x |
| **Scotland** | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | x | x | x |
| **NI** | x | x | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | x | x |

Start mandatory school

✓ compulsory
x not covered
* optional

**Cyber security content added:**

**England** – Computing
**Wales** – Citizenship
**Scotland** – ICT
**NI** – (Using ICT) across subjects

# Five other countries

Federal countries studied are adopting national frameworks, except Australia

## US

No national curriculum: a **K–12 Computer Science Framework** informs the development of state-level curriculum. **Cyber security** is embedded into core concept *Network and the Internet*, and **Safety, Law and Ethics** into the core concept *Impacts of Computing*.

## Australia

The national curriculum for Technologies has a **Curriculum Connections: Online Safety** – content is added to **different subjects**: Health and Physical Education, Digital Technologies, English and Arts. A curriculum review is expected to introduce cyber security to 4-5 years old.

## Canada

A **Digital World: A Pan-Canadian K-12 Computer Science Education Framework** is currently being designed to better align education across provinces. **Cyber security** will be embedded into focus area *Computing and Networks*, and **Ethics, Safety and The Law** into the focus area *Technology and Society*.

# Five other countries

Federal countries studied are adopting national frameworks, except Australia

## Singapore

Adopts a compulsory **Character & Citizenship Education** syllabus that covers cyber wellness, online safety and responsibilities of ICT users.

## New Zealand

The national curriculum covers cyber security under the **Technology** area focusing on *designing and developing digital outcomes* (e.g., **security and privacy** of devices, software, and data).

# Cyber security / online safety coverage

| | Age reached in school year | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| **US** | x | x | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Australia** | x | x | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | x | x |
| **Canada** | x | x | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Singapore** | x | x | x | x | x | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | x |
| **New Zealand** | x | x | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Start mandatory school

**Cyber security content added:**

**US** – Computer Science

**Australia** – across subjects

**Canada** – Computer Science

**Singapore** – Character & Citizenship

**New Zealand** – ICT

✓ compulsory

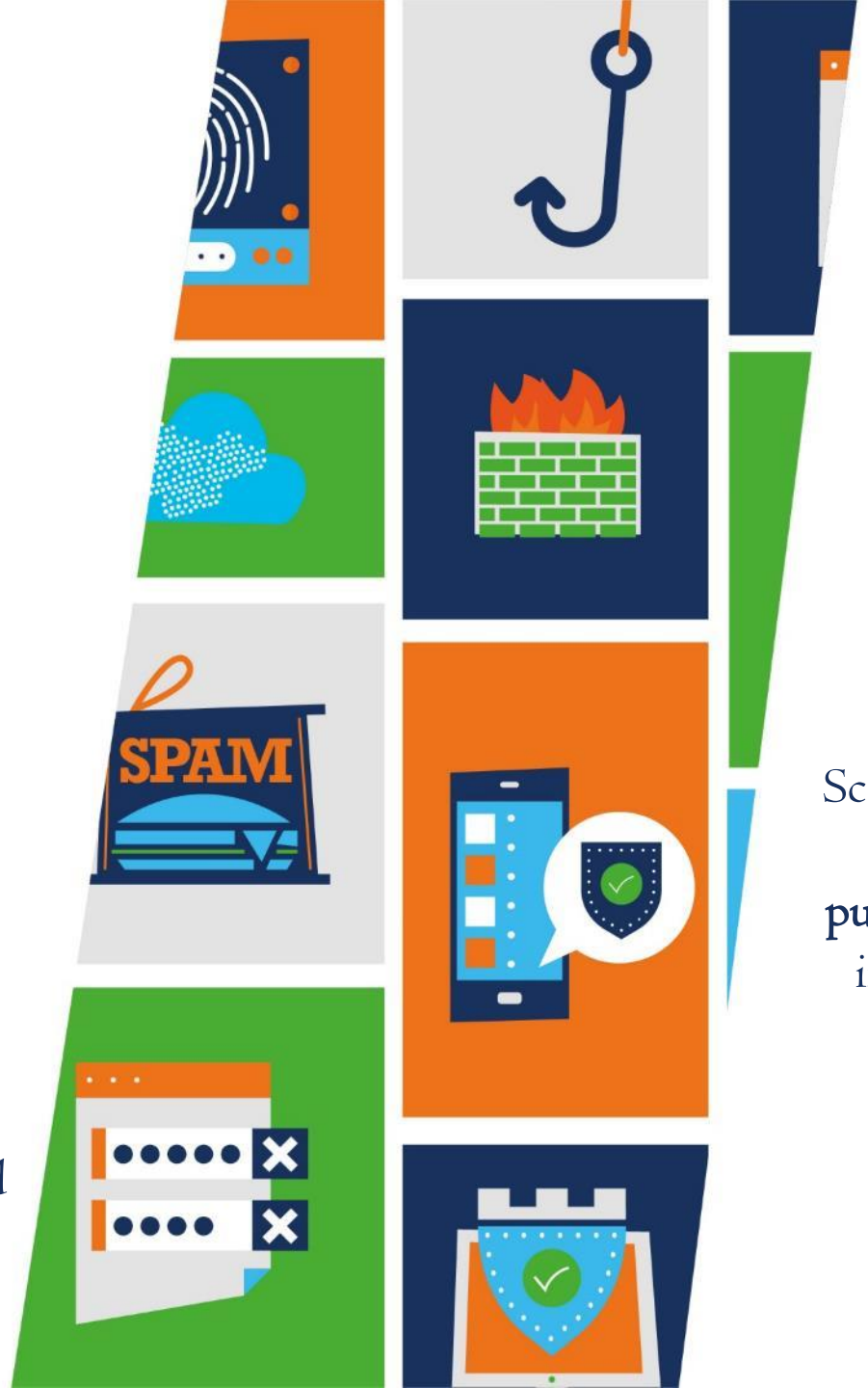
x not covered

* optional

# Conclusion

**The majority of countries incorporate cyber security content into ICT / Computing / Computer Science while others incorporate it across subjects (e.g., NI, Australia)**

**Level of coverage** of cyber security content vary --
Lighter: Wales, Singapore, New Zealand
Deeper: Australia, Canada, US, England, NI, Scotland





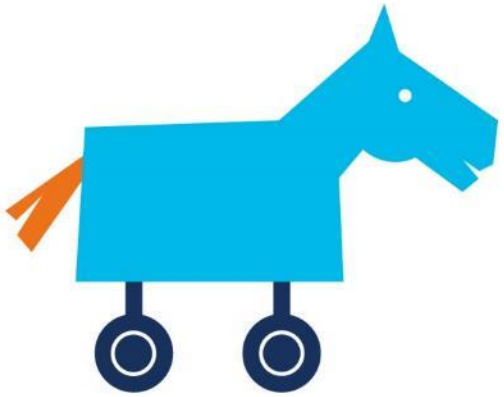
Scotland, Canada & Australia are **targeting very young pupils** (4-5 years old) to first introduce cyber security / digital literacy

Please complete our **cyber security school survey** at:
http://tiny.cc/CSSurvey

Part 1: basic information about school and role(s) of participant

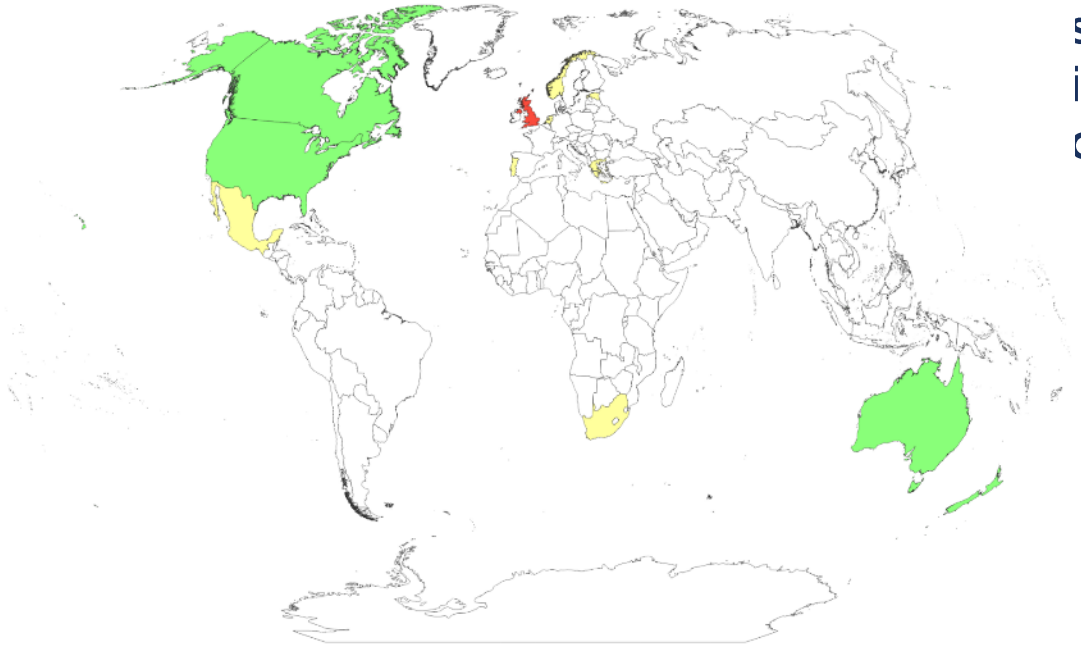
Part 2: cyber security practices at the school

Part 3: cyber security education offered to pupils at the school



# Stay tuned!

We are studying the extent of cyber security coverage and whether and how it is incorporated to pre-university curricula in other countries as well.



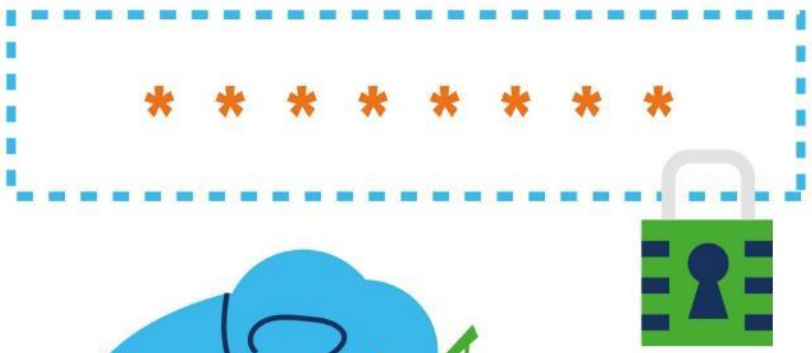

Questions at the end or contact me:

Virginia Franqueira
v.franqueira@kent.ac.uk

Project team:

- Krysia Waldock
- Vince Miller
- Shujun Li

# Headteachers! Cyber and Information security isn't just for the IT department.




Andrew Williams, SWGfL

SWGfL
Safe. Secure. Online

Technology photo created by rawpixel.com - www.freepik.com

From OWASP Foundation

ITPro. Business Cloud Hardware Infrastructure Security Software Technology Resou

# 15 schools in Nottinghamshire crippled by cyber attack

The Nova Education Trust is unable to access its IT systems to conduct remote lessons


Schools across Nottinghamshire have had to shut down their IT networks after a central trust that manages their systems was hit by a cyber attack.

All 15 secondary schools that are part of the Nova Education Trust are currently unable to access emails or their websites, and are still unable to conduct lessons remotely.

- Hackers hold Newcastle Uni student data to ransom
- Exams cancelled after Northumbria University cyber attack
- What is ransomware?

The trust has alerted the National Cyber Security Centre (NCSC) which is currently working with its central IT team to resolve the matter. The incident has also been reported to the Department of Education (DfE) and the Information Commissioner's Office (ICO).

The attack was first discovered on Wednesday morning, prompting the trust to [illegible]

the potential impact of the attack

Each school associated with the t

# Fears as 'thousands' of cyber attacks launched against British [illegible]rsities

W

We

# ISLE OF WIGHT SCHOOLS NEED DATA AFTER CYBER ATTACK

News Home | More from Isle of Wight News

Tuesday, August 24th, 2021 10:28am

By Oliver Dyer @oldyer


**Parents of students at Isle of Wight schools hit by ransomware attacks are being asked to get in touch after vital data was lost.**

As Isle of Wight Radio first reported, cyber attacks left school websites inaccessible and data 'frozen' earlier this month.

Staff at Medina and Carisbrooke College, as well as the Island VI Form, were affected, as were Barton Primary, Hunnyhill Primary and Lanesend Primary.

As such, affected schools are carrying out a data collection exercise. This would usually happen at the start [illegible]


Most read in UK

IE NEWS FEATURES COMMENT WEBINARS PODCAST EVENT REPLAY DIRECTORY PROFILE LOGIN

Independent Education Today | For leaders of independent schools

# The growing importance of cybersecurity in schools

*Sponsored: iSAMS explores the most effective ways schools can protect themselves against cyber scammers*

Contributor

In 2020, the UK's Department for Digital, Culture, Media and Sport conducted a Cyber Security Breaches Survey with a section focused specifically on the education sector. Its findings made for perturbing reading. The results of the survey showed that 41% of primary schools, 76% of secondary schools and 80% of further education institutions had identified at least one cyber-attack or security breach in the previous 12 months.

Hackers and cybercriminals appear to be increasingly turning away from larger organisations in favour of targeting smaller institutions – seen as low hanging fruit – that may be less well equipped to deal with a scam or hacking attempt. The fallout from a security breach can have devastating consequences for schools.

Previous attacks have resulted in significant financial losses, sensitive data on students, parents and staff being lost or published online and have even forced temporary school closures. With schools firmly in the crosshairs of cybercriminals, the importance of a secure digital infrastructure has never been greater.

One of the most effective ways to protect against cyber scammers is training staff to spot phishing attacks and malicious downloads, and implementing safety checks such as 2FA (two factor authentication) for all school systems.

*Hackers and cybercriminals appear to be increasingly turning away from larger organisations in favour of targeting smaller institutions*

Cybercriminals can embed malware in email attachments, which if downloaded can spread through a school's network

fe news.co.uk

HOME - PUBLISH - SEARCH -

# 93% increase in cyberattack sector

fe news by Check Point Research Published: 23 August 2021 Hits: 125

*As back-to-school begins, Check Point Research (@_CPResearch_) found the education sector to have the highest volume of cyber attacks for the month of July. Cyber criminals are seeking to capitalize on the short-notice shift back to remote learning driven by the Delta variant, by targeting people of schools, universities and research centers who log-in from home using their personal devices.*

- Global education sector saw a 29% increase in cyber attacks, and an average of 1,739 attacks a week, in July, compared to first half of 2021
- Top 5 most attacked countries were India, Italy, Israel, Australia and Turkey
- UK/Ireland/Isle-of-Man region experienced a 142% increase in weekly cyber attacks targeting the education sector; East Asia region marked a 79% increase

Check Point Research (CPR) sees an increase in cyberattacks against the global education sector, as back-to-school season gets underway. During the month of July, the education sector experienced the highest volume of cyber attacks compared to other industry sectors that CPR tracks, with an average of 1,739 cyber attacks documented per organization each week, marking a 29% increase from the first half of 2021.

## Why we are contacting you?

The Department for Education and the National Cyber Security Centre (NCSC) has been made aware of an increasing number of cyber-attacks involving ransomware infection affecting the education sector at this time. The purpose of this letter is to make you aware of the threat and provide high-level information and advice to support your ongoing cyber security preparedness and mitigation work.

In all cases the NCSC has been working with the department and the affected providers to contain and support post-incident outcomes. However, these attacks and incidents have had a significant impact on the affected education provider's ability to operate effectively and deliver services.

These incidents appear to be financially driven but opportunistic, taking advantage of system weaknesses such as unpatched software, poor authentication systems or the susceptibility of users to misdirection.

Whilst I would urge you to ensure that your systems, processes and awareness training are up to date, I also want to make you aware of the steps you should take if your educational setting is affected.

teiss News CISOs Threats Culture & Education Opinion Events Video teissTalk White Papers

# Harris Federation suffers a ransomware attack, shuts down email and telephone systems

March 31, 2021


**Education charity Harris Federation has become the fourth multi-academy trust to have suffered a ransomware attack since late February. The ransomware attack has forced the charity to shut down IT systems, and temprarily disable its email system and switchboard services.**

The Harris Federation, which now runs fifty primary and secondary academies in London and Essex with more than 36,000 pupils enrolled, announced on Monday that it suffered a ransomware attack last Saturday that enabled hackers to access its IT systems and encrypt their contents. The charity is presently working with cyber security experts to investigate the attack and restore all affected systems.

In a press release, Harris Federation said that after discovering the ransomware attack, it disabled its email system used by more than 40,000 students, as well as its telephone systems and switchboard services as a precaution.

Home Information for... Advice & guidance Education & skills Products & services News, blogs, events...

Home » Alert: Further ransomware attacks on the UK education sector by cyber criminals

NEWS

# Alert: Further ransomware attacks on the UK education sector by cyber criminals

The NCSC is responding to further ransomware attacks on the education sector by cyber criminals.

PUBLISHED
4 June 2021

NEWS TYPE
Alert

WRITTEN FOR
Large organisations
Small & medium sized organisations
Cyber security professionals
Public sector

Download / Print Article PDF

Share

Was this article helpful?
Yes No

IN THIS ALERT
1 Introduction

# Safeguarding implications

What would be the implications for you, your staff and your pupils if personal information was leaked onto the dark web?

### Database records

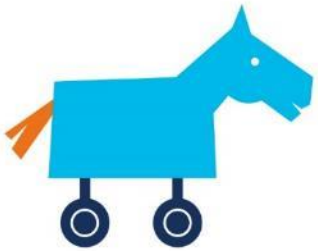
Parental contact details, pupil records, third party contact details…

### Computer controlled systems

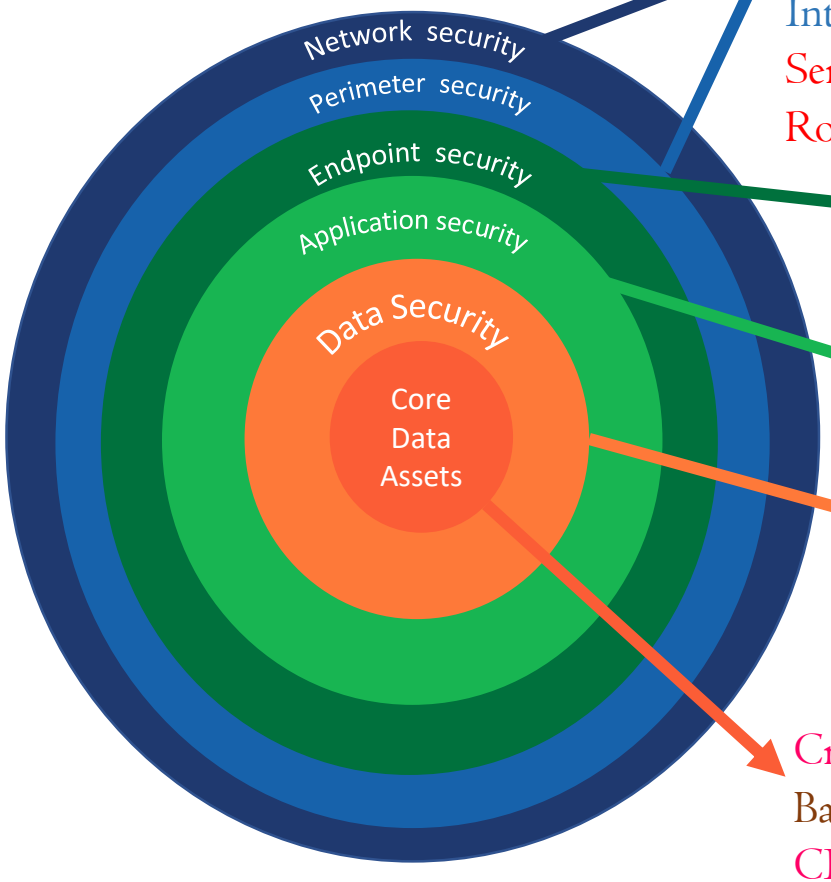
Telephone systems, email, CCTV, door/gate access control

### Information access

The internet, file servers, remote access systems



# Layers of protection




Firewall
ISP
Filters
Monitoring
Intrusion detection systems
Servers/switches
Routers

Anti-virus
Anti-malware
Ransomware protection
Anti-exploit
Fileless attack prevention
Asset management
MDM
Device firewall

Software
Hardware
Software/Hardware
Systems – Policy/People

Software patching
Automatic updates
Logging systems
Access controls
Password security

Policies
Record of Processing Activities
Maps of critical data
Data access controls
Retention and disposal

Critical data identified and protected
Backed up
CIA
Data Loss Prevention
Security Information and Event Management (SIEM)

Underpinned by staff training at all levels

# 3 Key threats

### Insider threats

- Train your staff
- Monitoring
- DLP
- Audit and identify core data

### Ransomware

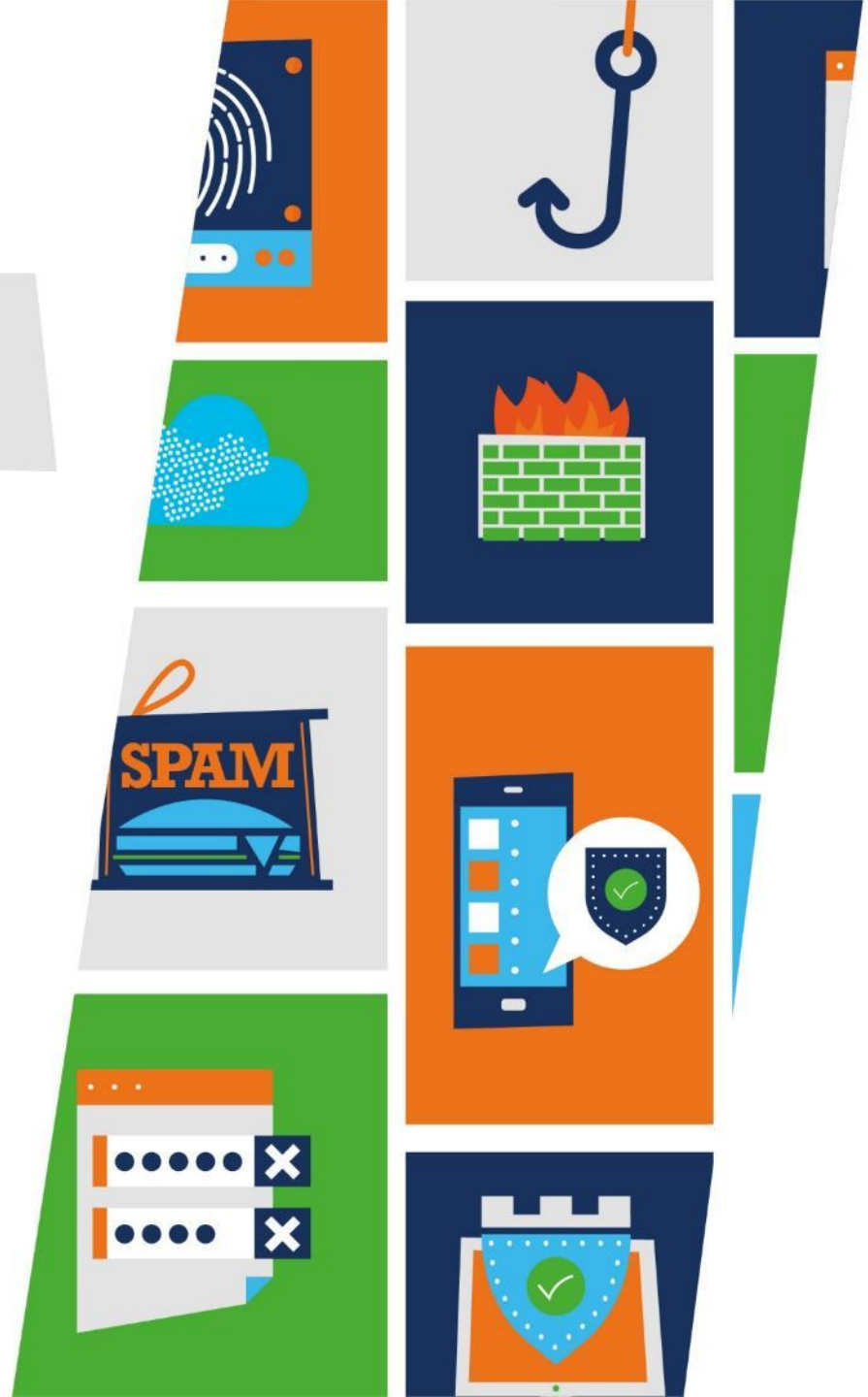
- Backups
- Prevent attack with training & software
- Organisational device controls
- Incident response plan

### Phishing

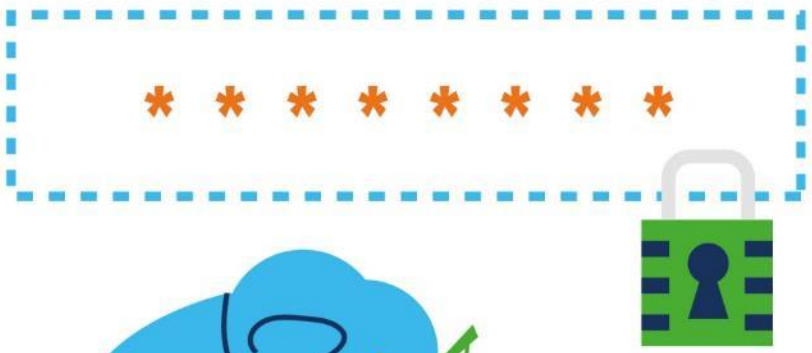
- Layers
- Train your staff
- Software protections
- Respond quickly

# Key approach?

## Staff Training




# How good backup routines help provide quick recovery.



**Poppy Angell,**
**Phoenix Software**

In the event of your primary data failing, like in a malware/ransomware attack, you need the assurance that your secondary copy of data can be accessed as a backup – hence the term.

Depending on how critical the primary data is, will depend on how protect that data – here are my best tips:

# Backup and DR best practice:

## Test

Routinely test your backups AND restores, at least once a week, as well as updating your RTO and RPO

## Three copies

Follow the NCSC guidelines of 3-2-1 – three copies of data, 2 devices and 1 offsite (or offline/immutable)

## Cloud?

Consider a cloud backup to keep a physical separation of your backups for disaster recovery purposes

# Backup and DR best practice:

## Update!

Ensure you're running the most up to date software or updates for your chosen backup tool (even if appliance based)

## Immutable?

Consider an immutable backup solution for your workloads, or an immutable backup target if not

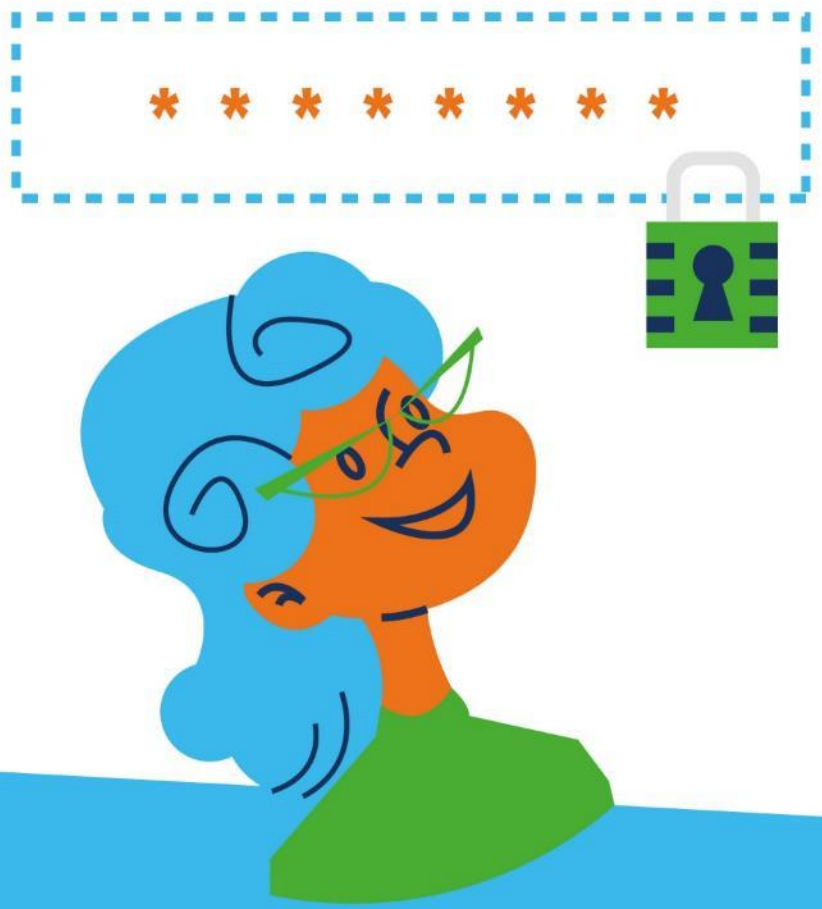
## Parallel running

Run your backup and disaster recovery plan in parallel to any cyber security plans/solutions you have in place already

## Future-proof

Make sure you're considering the future when deploying/updating/managing your backup/DR plan

# The Cyber Secure tool



Department for Education/SWGfL

Cyber Secure

Developed in partnership by the Department for Education and SWGfL. Currently in pilot and expected to launch in early 2022.

With 23 aspects, the free tool will help experts and non-experts improve and strengthen defences against attack.

## Level 2

- All staff, including new starters, receive a comprehensive set of foundational training in cyber and information security. Staff acknowledge the receipt of this and their inherent responsibilities.
- At least annually, all staff acknowledge their obligations under the Acceptable Use Agreement (AUA) before access to systems is provided.

## How to Achieve Next Level

Updated: 1 month ago

Define different categories of staff who require differing access to technology systems, such as; office, teacher, SENCO. Identify the core technology systems that each category of staff may need access to.

Develop an induction programme which covers those systems. Identify extended training options for induction to supplement and support any in-house provision.

Identify what processes may need to occur when an employee leaves the establishment. Identify what systems and devices are revoked and returned defining how/when this would take place.

Using the identified information, develop a process identifying what cyber and information security process should be in place when an employee leaves the establishment.

Plan for a process to ensure staff understand their cyber and information security obligations when moving between roles within the establishment. Identify categories of users and what networks/systems/software they need to have access to in order to fulfil their role.

Enter Current Position

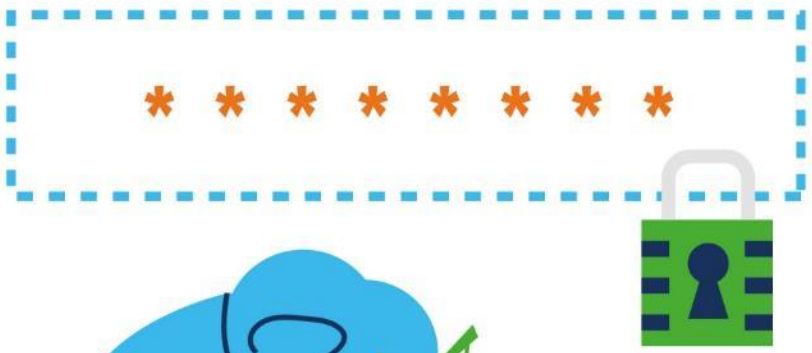
Enter Evidence

Enter Improvement Actions

## Level 3

- New staff members receive a training package describing the establishment's cyber and information security policies, processes and practices.
- The establishment has a simple and consistent staff exit process identifying what systems, applications and devices are to be revoked and how/when this would take place.
- A process for all staff changes in roles is in place. This process ensures that staff only have access to those systems, applications and devices to which they are entitled to as defined by their role.

# "The rocky road of recovering from a cyber incident in school"



A quick journey through how things never go to plan (if you have a plan!) including uncovering the unexpected.
CySecAware

CySecAware

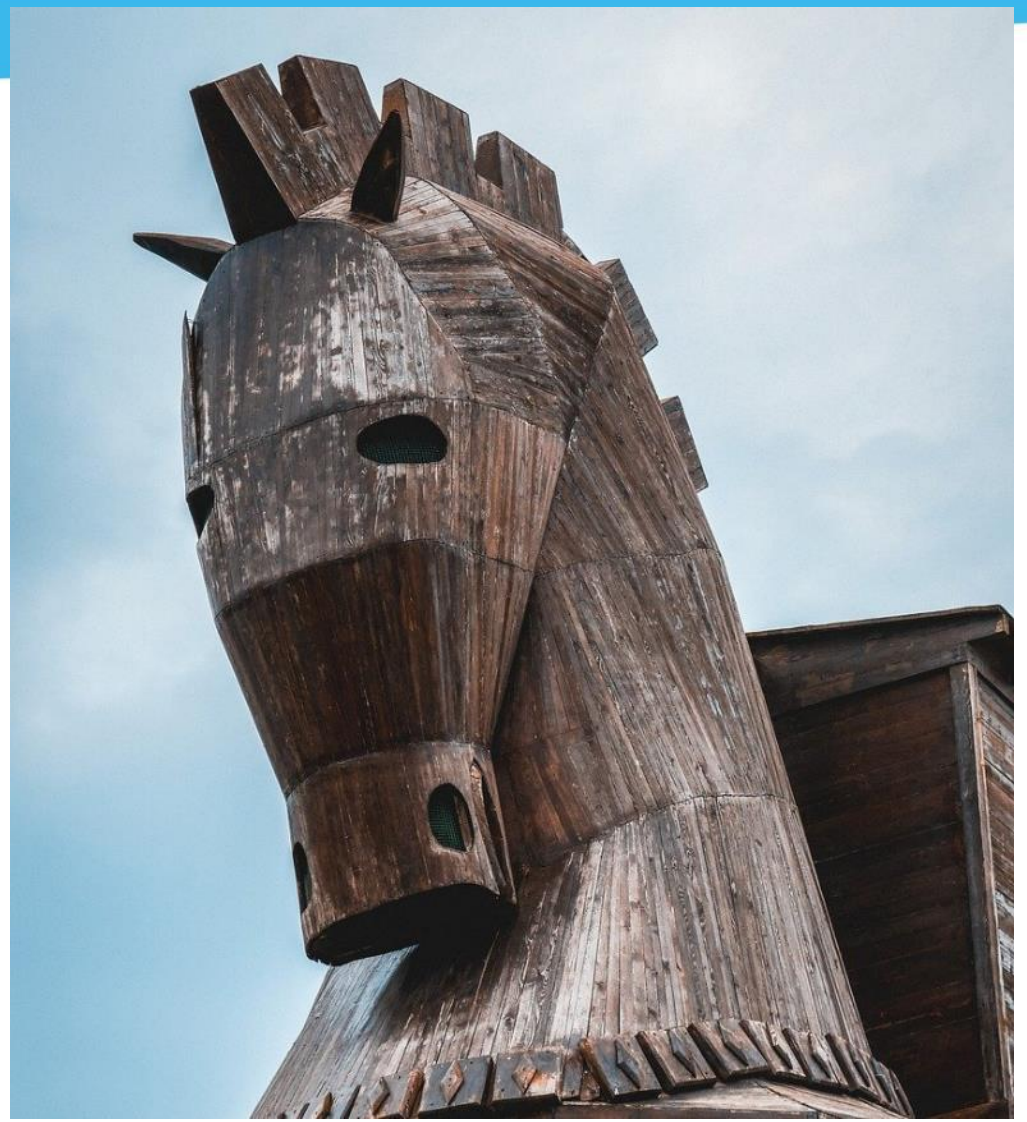

# What would you do?

The Police walk through the door…

CySecAware

They tell you that your school is infected…

…with a TROJAN



CySecAware

They are concerned because:

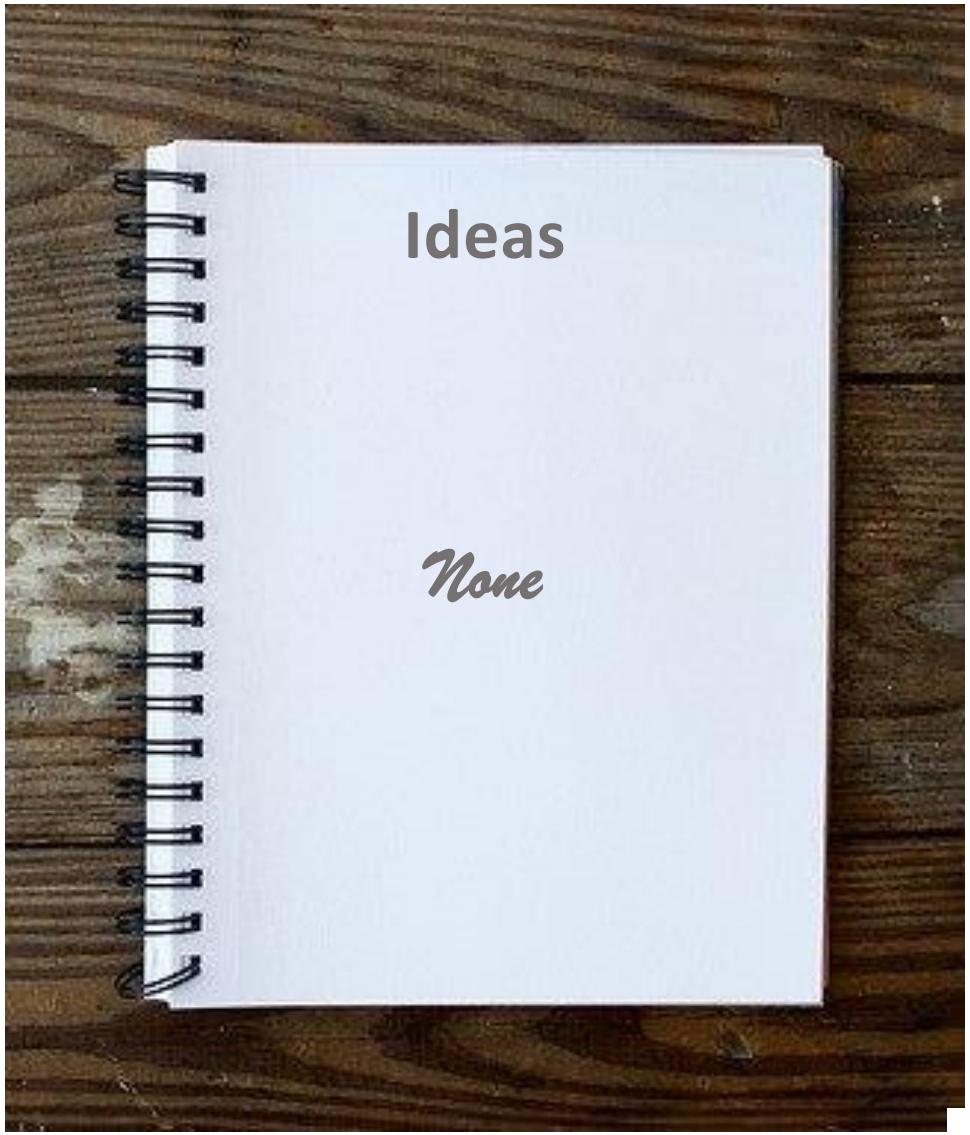
- Safeguarding data may be compromised
- This often leads to ransomware

They ask you to disconnect everything

CySecAware

You call your IT support

CySecAware




They have no idea of the impact of switching off the network…

To be honest, they just have no idea how to respond!

CySecAware

You close the school because:

- No Safeguarding information
- No next of kin data
- Door locks fail
- CCTV not working
- Fire alarm not working

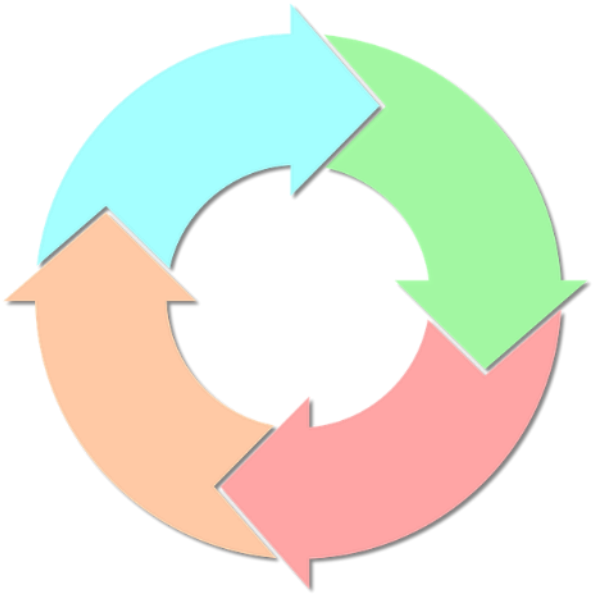

CySecAware

After the Police perform Digital Forensic analysis, IT begin to rebuild…

CySecAware

Rebuild

Infection



Infection

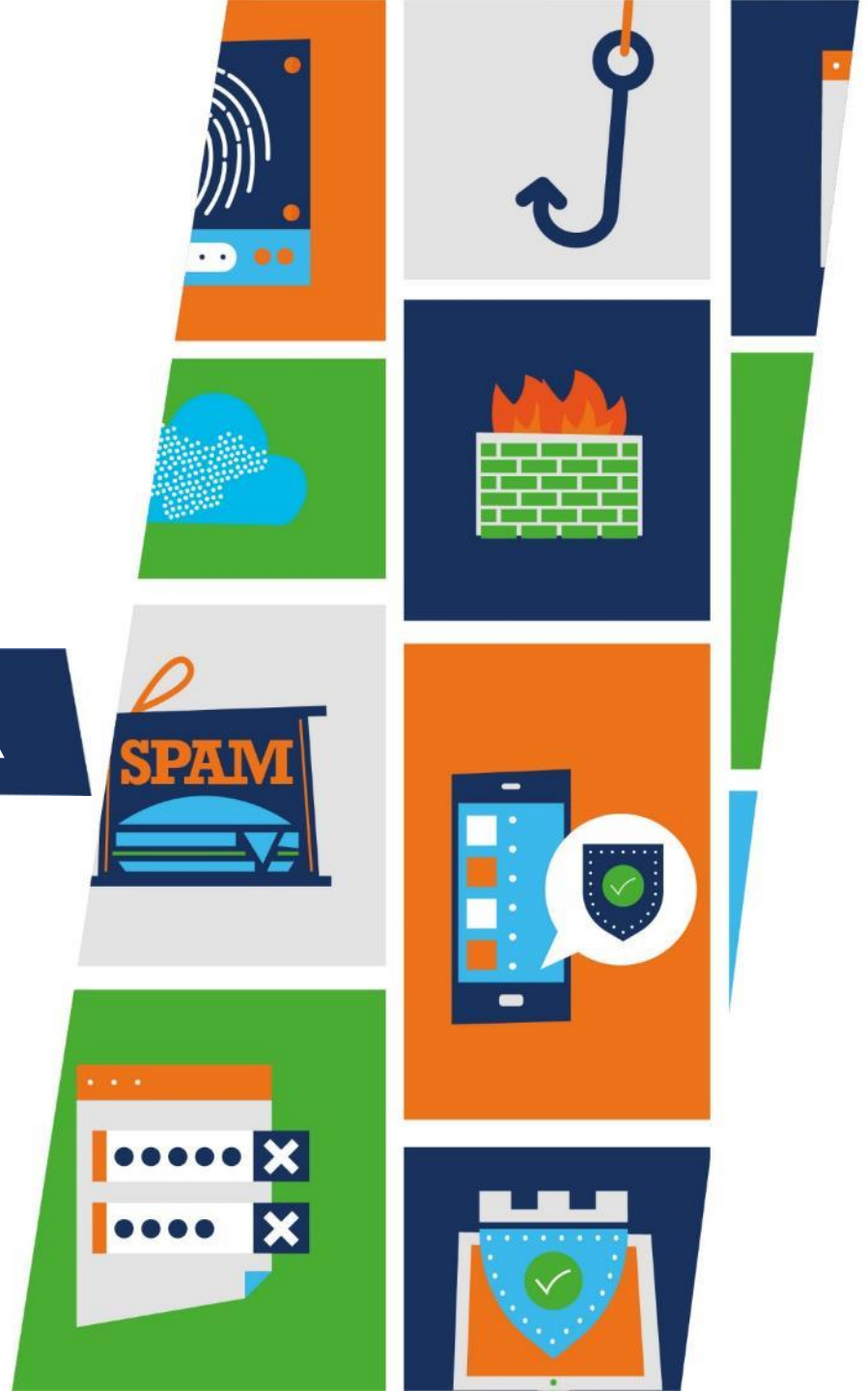
Rebuild

CySecAware


Finally you re-open a week later!

CySecAware

# TWO MONTHS LATER




CySecAware


The Police walk through the door!

CySecAware

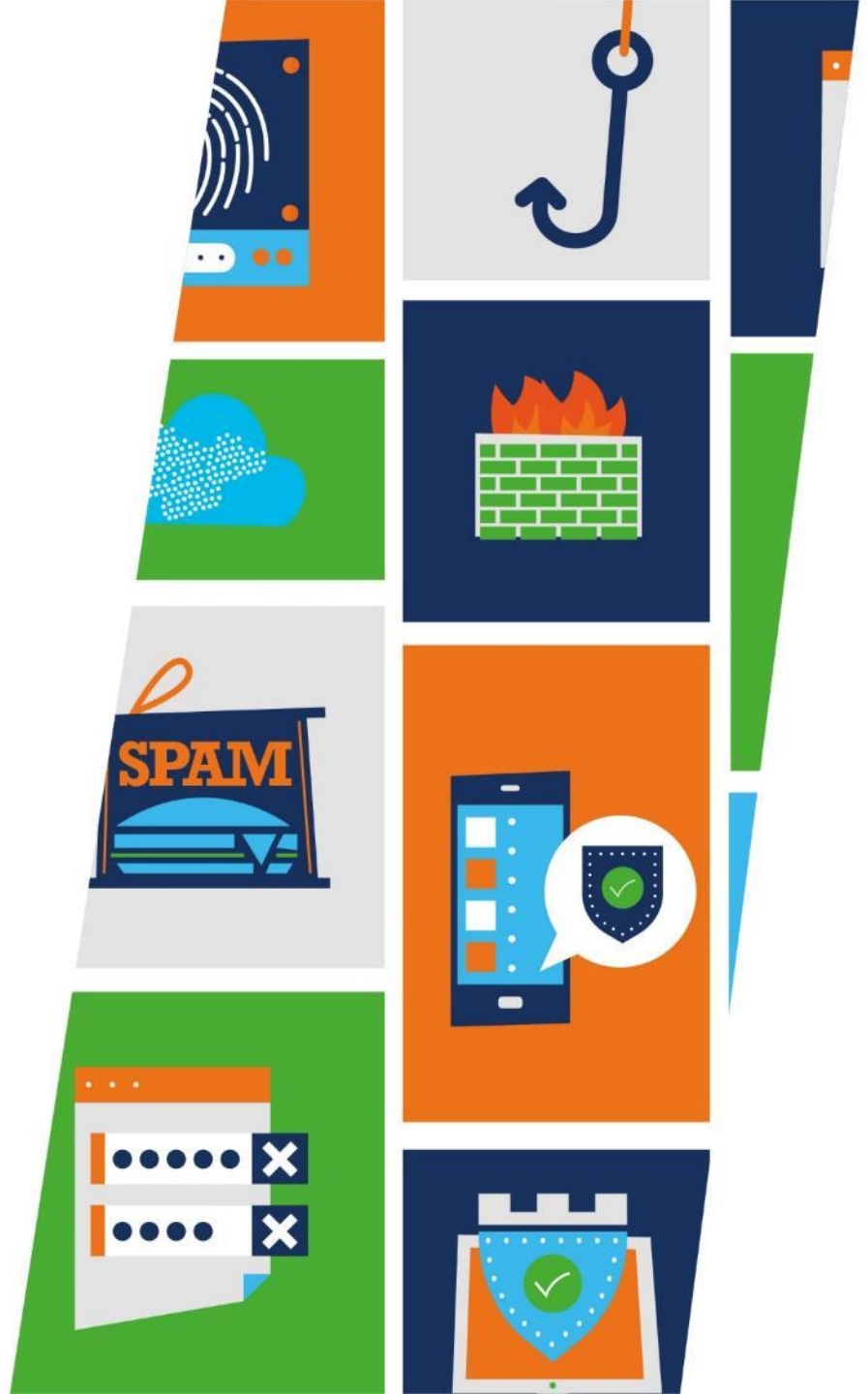
Data is flowing everywhere…
gigabytes of it

CySecAware

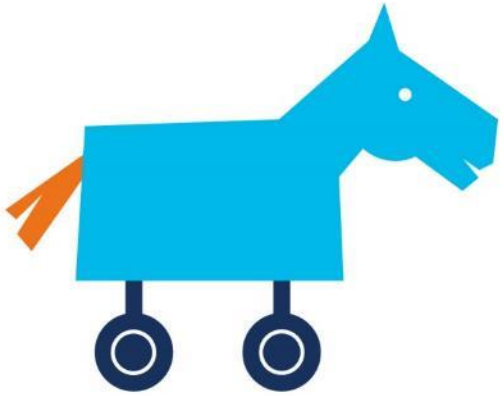
This was the culprit…

CySecAware

# Lessons learned




CySecAware



CySecAware

- Cyber security is not an IT function
- This is risk management
- Ownership should be in SLT
- Understand your network + assets
- Plan for an incident: reduce response time, minimise impact

CySecAware

Jez Rogers

Andy Rawlinson


**Information Security Training**

Designed to help you raise awareness of security and reduce risk in your organisation

SWGfL

Safe, Secure, Online

# Q&A

Ask your questions,
we're here for you!

With thanks to Bitdefender
for supporting us

Bitdefender
BUILT FOR RESILIENCE

GFCE Global Forum on Cyber Expertise | University of Kent | Institute of Cyber Security for Society (ICSS)

PHOENIX

SWGfL
Safe. Secure. Online

CySecAware

# Links

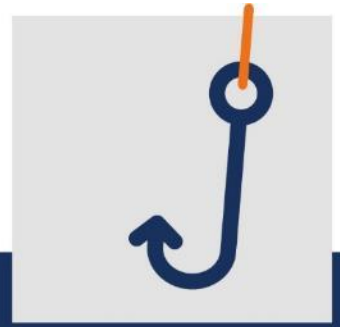
## NCSC
## Advice for Schools

http://tiny.cc/
NCSCSchools

https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools

## SWGfL
## Security Solutions

http://swgfl.org.uk
/security



## Cyber Survey

http://tiny.cc/
CSSurvey

# Goodbye & thank you for watching

# Links

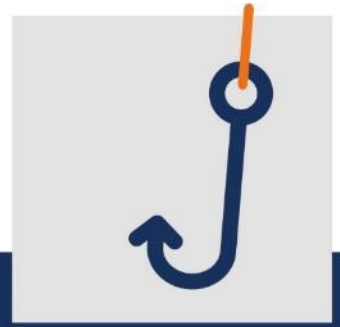
## NCSC
## Advice for Schools

http://tiny.cc/
NCSCSchools

https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools

## SWGfL
## Security Solutions

http://swgfl.org.uk
/security



## Cyber Survey

http://tiny.cc/
CSSurvey