Keeping Staff and Students Safe Online

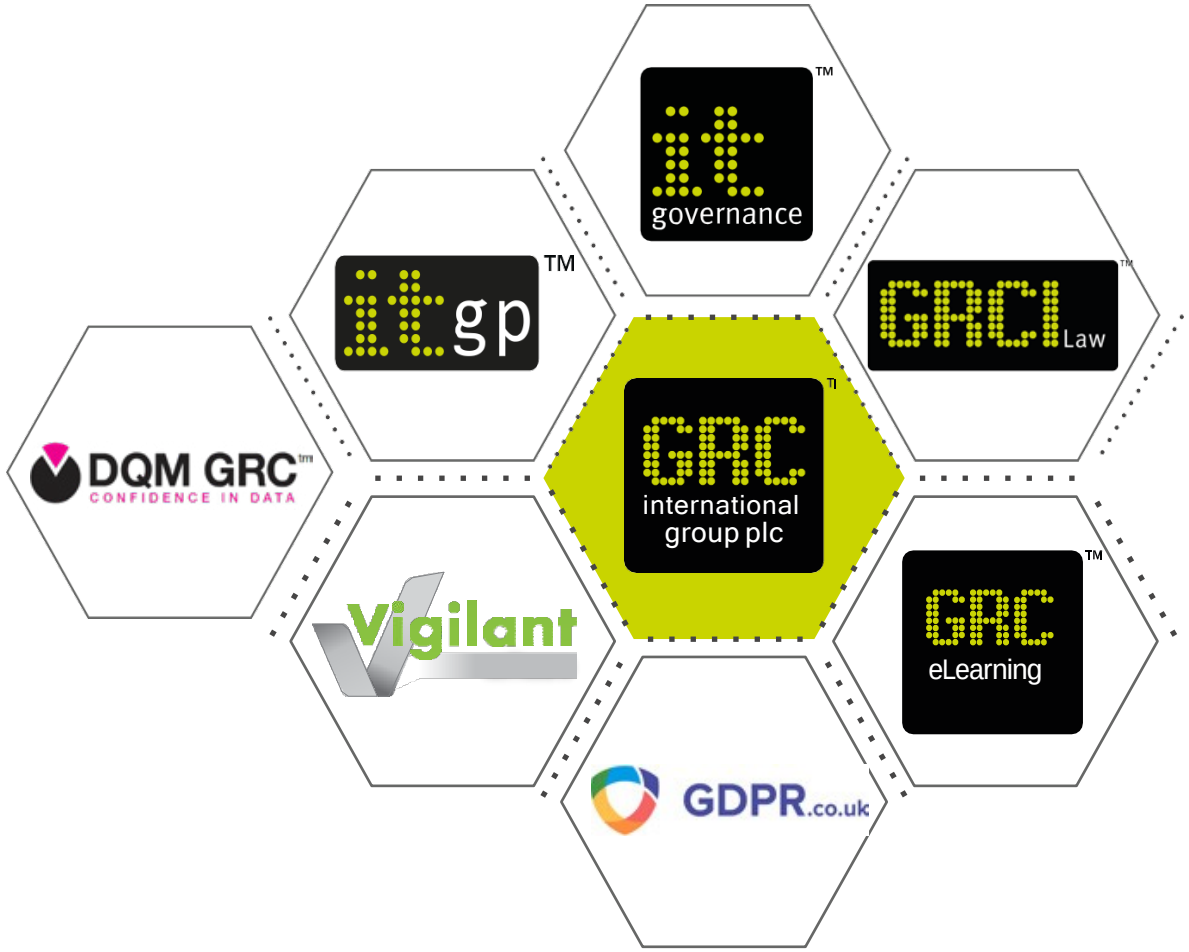
Geraint Williams - Chief Information Security Officer (CISO)

Claire Ashton – Sector Marketing Manager for Education

GRC International Limited

www.ascl.org.uk/pd

GRC International Group



Geraint Williams

Chief Information Security Officer (CISO)

Claire Ashton

Sector Marketing Manager for Education

Preferred Supplier ASCL Association of School and College Leaders

10% discount

Keeping Staff and Students Safe Online
Learning outcomes

1	2	3
Understand how to work from home more safely	Understand how to share data securely	Understand how to spot common cyber attacks such as phishing emails

Outline of the webinar

- Outlining the cyber threat
- Cyber security basics
- Dos and don’ts when using video conferencing
- Data protection tips
- Worst case scenario

Useful definitions

Cyber security

Cyber security focuses on protecting computer systems from unauthorised access or being otherwise damaged or made inaccessible

Cyber attack

An attempt by criminals to damage or destroy a computer network or system or an attempt to steal data

Phishing

A type of social engineering often used to steal data, including log in details and credit card numbers or infect computers with malware

Social engineering

Techniques designed to lure unsuspecting people into giving away personal details or perform an action that helps the attacker

Malware

Malicious software designed to disrupt, damage, or gain unauthorised access to a computer system.

Includes: viruses; worms; trojan horse; spyware; and ransomware

Ransomware

Malicious software designed to block access to a computer system or data until a sum of money is paid

In your organisation

Has your organisation been hit by a cyber attack?

- Yes
- No
- Unsure

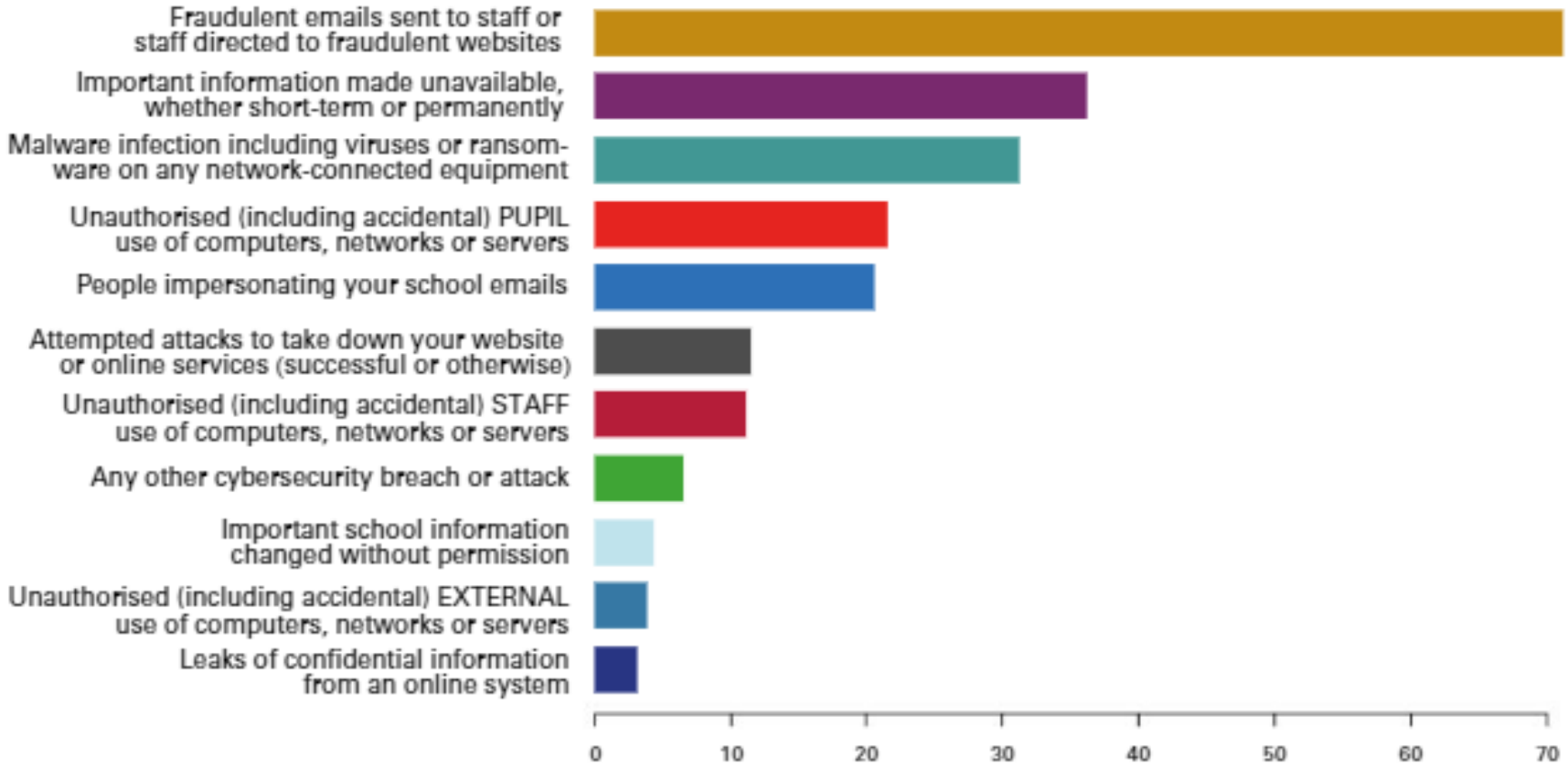
In your organisation

- Who has specific responsibility for cyber security?
- A member of the senior leadership team
- The IT team
- We outsource it
- Someone else
- No one
- Unsure

If not now then when?

LGfL and NCSC joint cyber security audit of schools 2019

As far as you know, have you ever experienced the following?
(% of 432 schools answering yes)



Actual cases in schools

- Hackers use ransomware to encrypt files - losing students' GCSE coursework
  - Sir John Colfox Academy, Bridport, March 2019

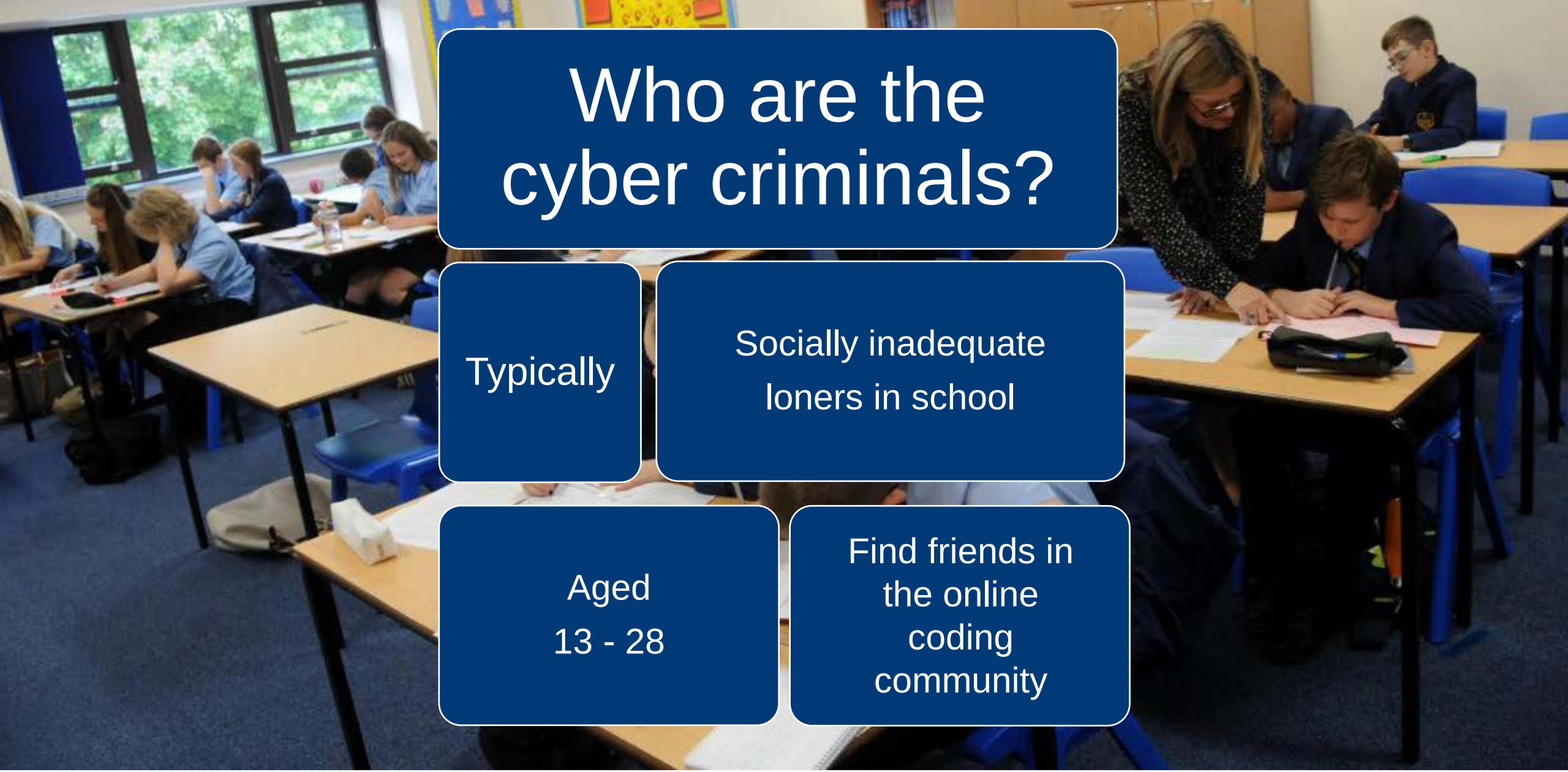
- Ransomware attack - 5000 password resets, multiday outage
  - Dundee and Angus College Feb 2020

- Wakefield school forced to close due to cyber attack
  - St Thomas à Becket Catholic Secondary School, October 2019

- Ransomware attack at Plymouth school, some coursework lost
  - Hele's School, Plymouth, September 2019

Outlining the threat

- Cyber attacks on schools and colleges are happening now
- Educational settings are seen as easy targets with valuable data
- School staff are busy and well meaning
- Some students see bringing down networks as a challenge



Who are the cyber criminals?

Typically

Socially inadequate loners in school

Aged 13 - 28

Find friends in the online coding community

Threat Actors

- Script Kiddies / Newbies
- Recreational Hackers
- Malicious Insider
- Cyber Criminals
- Hacktivist
- Cyber Terrorist
- Corporate Espionage
- State Sponsored

National Cyber Security Centre

About NCSC | Information for... | Advice & guidance | Education & skills | P

Home » 11 - 19 year olds (CyberFirst)

Education & skills

11 - 19 year olds (CyberFirst) | Higher education | Professional skills & training | Working NCSC | academia

11 - 19 year olds (CyberFirst)

Developing the UK's next generation of cyber professionals through student bursaries, courses and competitions.

What is CyberFirst and who is it for?

Launched in May 2016, and inspired and led by the National Cyber Security Centre (NCSC), a part of GCHQ, CyberFirst began as a programme of opportunities helping young people explore their passion for tech by introducing them to the world of cyber security.

CyberFirst Girls competition

The NCSC are working hard to get more girls interested in a career in cyber security. The CyberFirst Girls Competition provides a fun but challenging environment to inspire the next generation of young women to consider a career in cyber security.

NCA National Crime Agency

Leading the UK's fight to cut serious and organised crime

Search ...

Who we are | What we do | News | Careers | Most Wanted | Contact us

Home > What we do > What we investigate > Cyber crime > Cyber Choices: Helping you choose the right and legal path

Share this page:

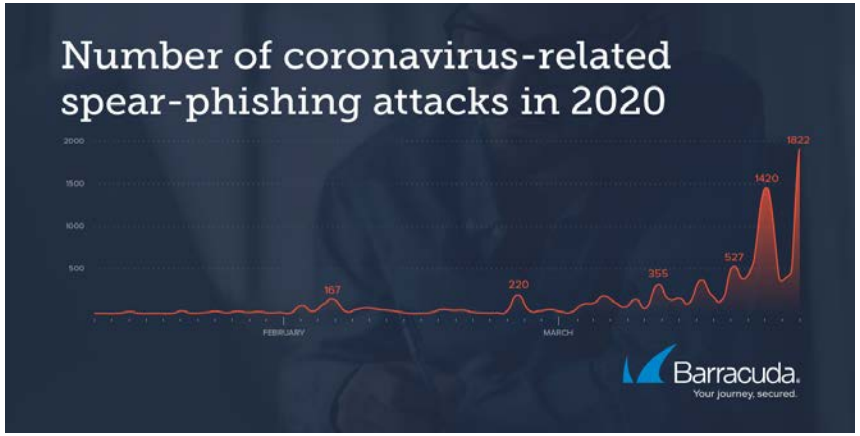
Cyber Choices: Helping you choose the right and legal path

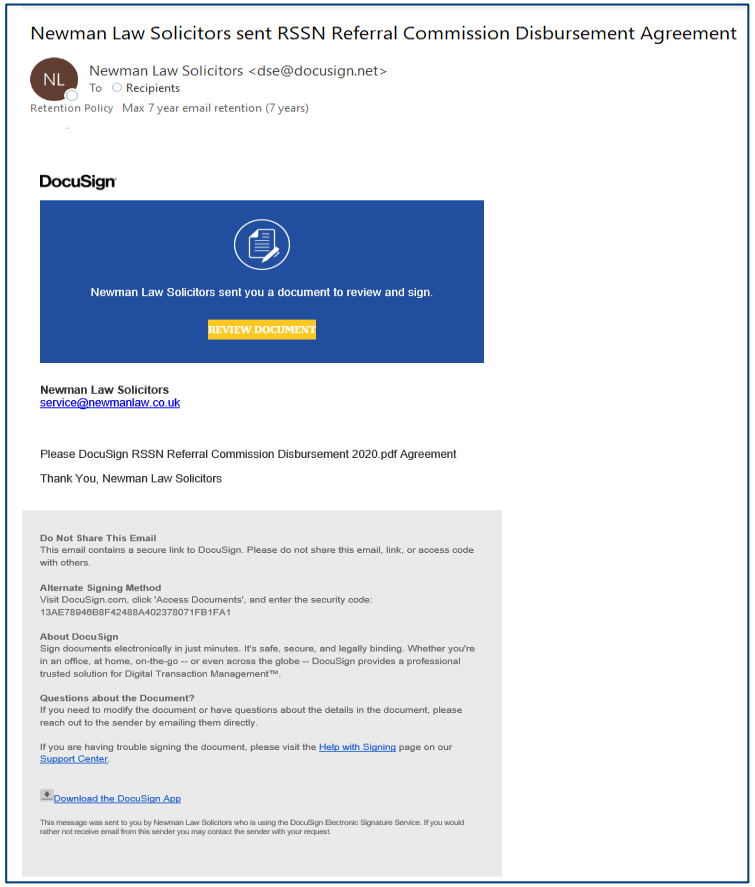
Help is available

https://www.ncsc.gov.uk/section/education-skills/11-19-year-olds

https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyberchoices

What's happening during Covid 19?





Cyber Security Basics

Leader

The magazine for school and college leaders

ASCL Association of School and College Leaders

ABOUT | LATEST EDITION | ARCHIVE | CONTACT

GO

FEATURES | NEWS AND GUIDANCE | THE KNOW ZONE

2020 Spring Term 2

FEATURES

Rebel with a cause
Lemn Sissay left behind a troubled childhood to find success as a poet, writer and broadcaster with work highlighting, in particular, the plight of children in care and inequality. He talks to Julie Nightingale. More »

Trees of diversity
Making school and college leadership more diverse will

Cyber security expert **Claire Ashton** says protecting your school or college from a cyber attack is vital in order to avoid serious consequences. Here, she shares top tips on how you can protect yourself.

Cyber secure?

If you have not been hit by a cyber attack, recent surveys and statistics suggest that you are lucky. A London Grid for Learning (LGfL) and National Cyber Security Centre (NCSC) study (http://bit.ly/ASCLITG4) found that 83% of schools had experienced a cyber security incident, 69% a phishing attack and 35% periods with no access to important information. The vast amounts of personal data, often low technical understanding and busy staff make schools and colleges an attractive target.

Article published in the Spring 2020 edition of Leader magazine

http://www.leadermagazine.co.uk/articles/cyber_secure1/

Free cyber security posters for schools

https://www.itgovernance.co.uk/cyber-security-posters-for-schools-and-colleges

Cyber Security Basics

Password management

Everyone knows this but…

In 2018, 23.2 million hacked accounts used the password ‘123456’

Patch management & secure configuration

Install updates as soon as available

Ideally automate updates

Shut down computers daily to ensure updates are identified

Avoid unsupported software

Microsoft ended support for Windows 7 in January

Customers warned of the risks of malware

System privileges

Allocate privileges based on role

Additional privileges may lead to unauthorised access to information

Accounts with higher levels of access are more appealing to criminal hackers

Account management

Forgotten software and network accounts are an easy target for cyber criminals

Former employees continuing to access systems is unlawful access to data

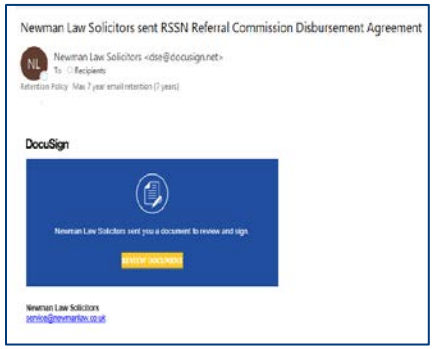
Secure remote working

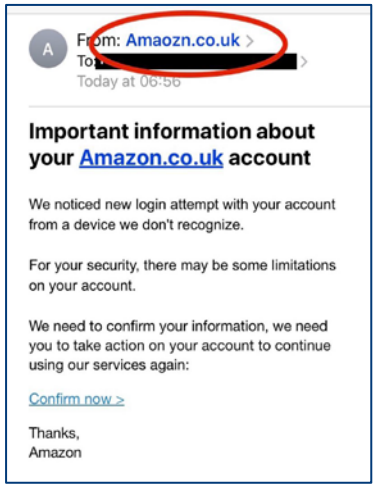
Encrypt laptops, mobile devices and removable media

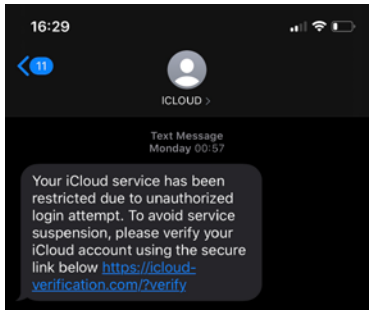
Introduce and enforce policies for accessing sensitive systems and taking sensitive documents home

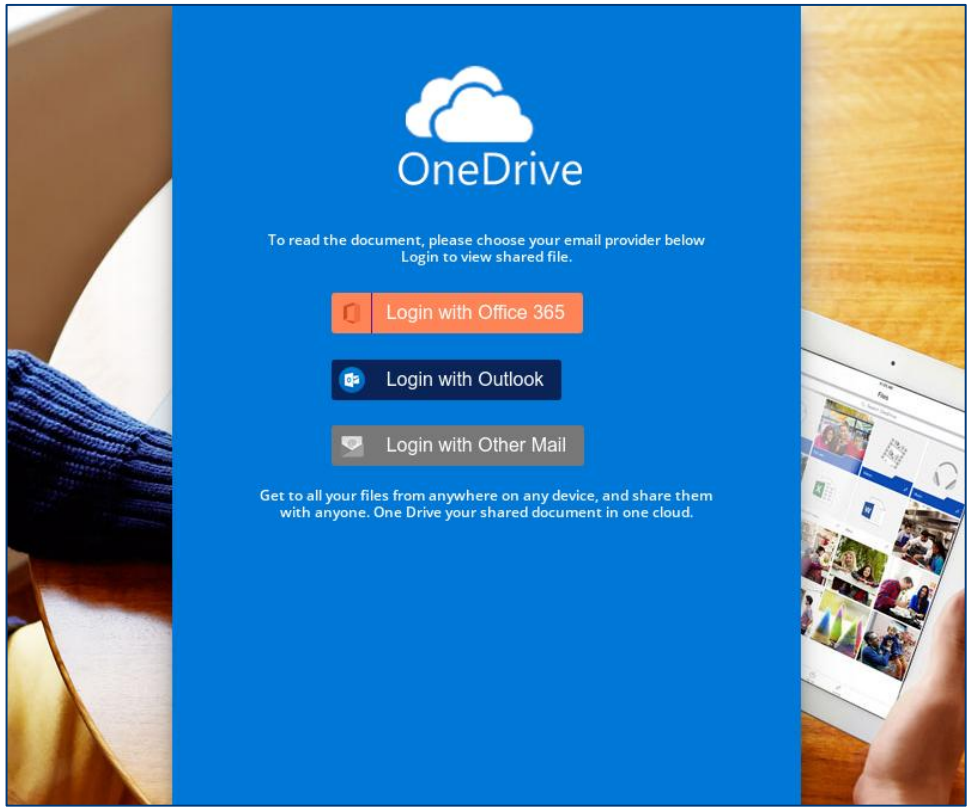
Understanding Phishing

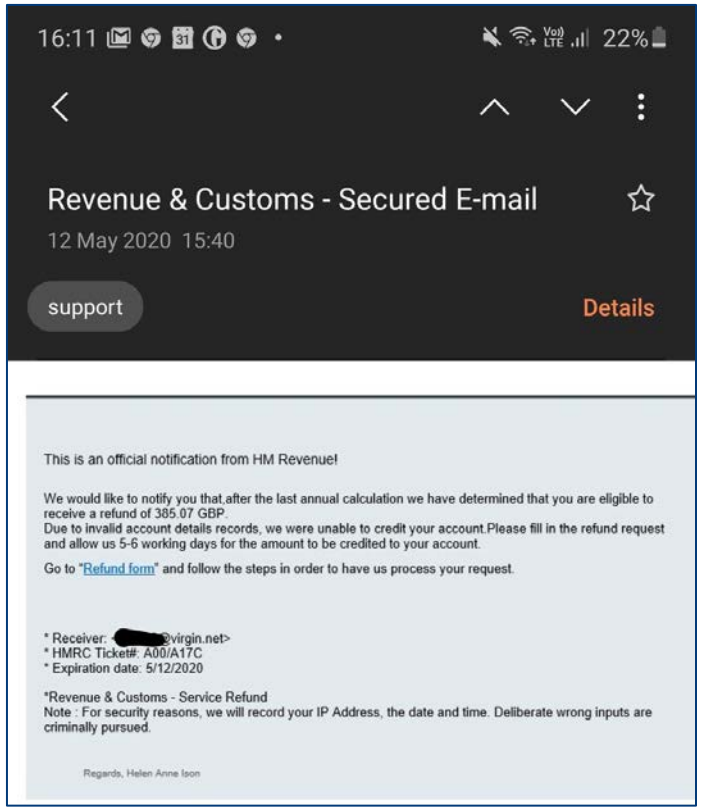
Your staff and students could be the gateway into your organisation











Ways to spot a phishing email

- ✓ Be suspicious of requests for information that the sender should already have
- ✓ Look out for typos and grammatical errors
- ✓ Hover over email addresses and links to reveal their true content
- ✓ Always double-check requests are genuine, check their website or call them – not using details on the email
- ✓ Only visit legitimate websites
- ✓ Report anything suspicious
- ✓ Always double-check bank accounts before making payments be very cautious of changes – call to check before making payment

- x Do not click onto email links or attachments from unverified sources
- x Never give away sensitive information such as log in details, passwords, card numbers etc
- x Do not be pressurised into doing something – be wary of messages with a sense of urgency

If it sounds too good to be true, it probably is.

Never be rushed into anything on an email, take a break and look at it again, ask a colleague and check again!

Dos and don’ts when using video conferencing

Remember your cyber security basics when using all software

- Stick to well known brands, e.g. Microsoft and GoToWebinar
  They prioritise cyber security and have the budgets to do it properly
- Do not share meeting or webinar log in details publicly
  This allows access to non-invited attendees
- Do not automatically choose the easiest to use tools
  Think security first
- Keep all software up-to-date
  Ensure you are using the latest versions as these include security updates

Two separate attacks have targeted as many as 50,000 different Teams users, with the goal of phishing Office 365 logins.

A convincing cyberattack that impersonates notifications from Microsoft Teams in order to steal the Office 365 credentials of employees is making the rounds, according to researchers. Two separate attacks have targeted as many as 50,000 different Teams users, according to findings from Abnormal Security.

Securing Microsoft Teams meetings

- Keep invitations secure
- Do not allow anonymous users to join a meeting
- Make all users join via the lobby
- Limit those who can present

Securing Zoom meetings

- Do not use personal meeting IDs for public meetings
- Do not publicly share meeting credentials
- Require a password to join
- Enable the waiting room
- Control screen sharing
- Turn off annotation
- Once all attendees have joined, lock the meeting

Working from home securely

Develop organisation policies and remember the cyber security basics

- Train people how to spot phishing and other malicious emails
- Secure devices
  Implement encryption, keep software up-to-date, shut down PCs and laptops daily, use firewalls
- Replace outdated software
- Allow secure access to data – we'll talk more about this
- Be aware of others in the home and the sharing of devices
- Consider safeguarding, e.g. when video calling
- Avoid using public and conference WIFI – post lockdown!

Sharing data securely

Avoid sharing data - where possible

Enable online secure access to data

Restrict data downloads

Standardise file sharing

Use a standard programme for secure file sharing across the organisation

Beware of sharing data via email

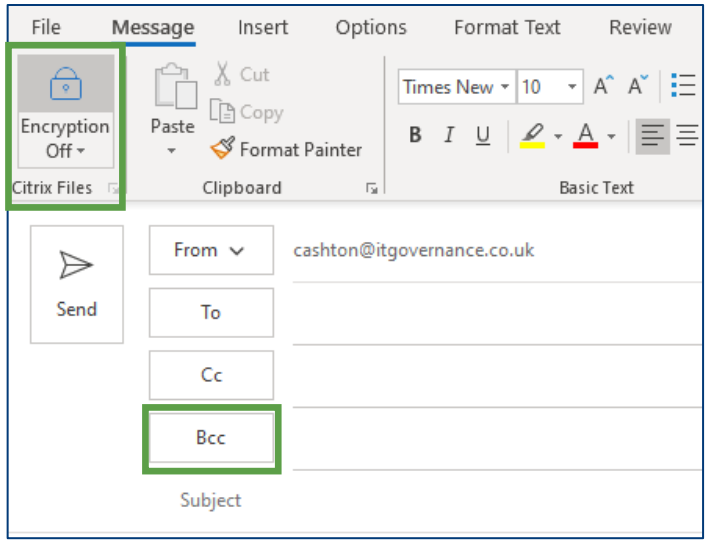
Try to avoid emailing data

Use the BCC field

Encrypt emails

Consider data retention and subject access requests (where is the personal data?)

Beware auto-completion of email addresses



Emailing personal data to the wrong person is a data breach

Keeping personal data from previous jobs – e.g. on email or USB sticks is unlawful processing of data

What to do in the worst case scenario

Ensure staff and students feel confident to identify and report a cyber attack

Never pay ransoms

Cyber criminals are criminals

Paying ransoms does not guarantee they will release your data or systems

Contact the police

Report the cyber attack to the police as soon as possible – this is criminal activity

Seek professional help

Contact IT professionals or your IT support team, LA or trust for guidance

Speak to your DPO and/or the ICO

Not being able to access personal data or someone else accessing personal data might need reporting to the ICO within 72 hours of discovery

Change log in details

If relevant, change log in details

Plan for all eventualities

Business continuity management - the process of understanding how to operate when systems are no longer available

Disaster recovery – how to recover quickly

Further advice and guidance

UK Government's Cyber Essentials scheme

www.itgovernance.co.uk/cyber-essentials-scheme

Understanding business continuity management

www.itgovernance.co.uk/bc_dr

Useful blogs

www.itgovernance.co.uk/blog

Twitter

@ClaireAshton

@ITGovernance

Thank you for listening

Would you like to hear more from us?

Let us know which topics you would like covering on future webinars

- Data protection and the GDPR
- More on cyber security
- Managing IT teams
- Business continuity management
- Other – please add to the comments

ASCL Professional Development

events
www.ascl.org.uk/calendar

join
www.ascl.org.uk/join

consultancy
www.ascl.org.uk/consultancy

follow ASCL

ASCLUK | ASCL_UK | ASCL_UK | ASCLUK | ASCL | ASCLUK

Whilst the information provided at this event was correct to the best of the knowledge of the presenters and organisers, neither ASCL nor Professional Development can accept liability if at a later date this should prove not to be the case. Nor can they be held responsible for any errors or any consequences resulting from its use.

Please also see the ASCL website for details of our copyright statement.

www.ascl.org.uk/pd

ASCL Professional Development

www.ascl.org.uk/pd

LEADING ON