Welcome to the March 2024 Scomis Online Safety Newsletter for Schools

Cyber Security

With the Easter break almost upon us, Scomis reminds our customers that Cyber Security is an extremely important consideration for the Senior Management Team, Governing bodies and Trustees of Academies and Multi Academy Trusts.

Robust **Network security** will prevent loss of vital data, accidental damage and malicious activity (cyber attacks). The DfE's guidance Cyber crime and cyber security: a guide for education providers - GOV.UK (www.gov.uk) reports the highest proportion of cyber-attacks reported to the DfE from the education sector are ***ransomware attacks***. Ransomware is a type of malware, this 'malware' is typically introduced to a network through sophisticated ***phishing/social engineering attacks***. Once in the school's network the attacker will seek out critical and valuable forms of data:

- financial systems
- personal identifiable data
- intellectual property
- student coursework
- staff personal records
- MIS/SIMS databases

Data is selected and encrypted, preventing the ***Data owner*** (the school) from accessing the data until payment of a ransom in exchange for decryption of the data.

Phishing

Phishing is a form of social engineering attack aimed to trick the user into giving their personal credentials or their identity information to an attacker:

- The email messages will appear authentic with corporate /official logos which the recipient believes to be genuine.
- Phishing emails often contain links to websites which will install malware without the user knowing or contain an attachment, which once downloaded or opened, will install the malware onto the system.
- The emails tend to ask for the recipient to confirm/ verify personal information, such as account numbers, passwords or date of birth.
- Unsuspecting victims who respond may suffer from stolen accounts, financial loss and identity theft.

All staff should be educated to 'Never click on links or download attachments from unexpected emails'.

Review the South West Grid for Learning's Cyber Security Checklist for Schools

Train your staff regularly!
Provide training around personal risks!
Keep training interesting!
Identify those who have access to sensitive information: Headteacher, DSL, Business/HR Manager ++

Review and consider the National Cyber Security Centre's resources designed to help board members govern cyber risk more effectively Board Toolkit

Or contact Scomis for impartial and objective advice on: Infrastructure Services; Network Solutions and Services; Remote Back-up

Scomis: **01392 385300 E: scomis@devon.gov.uk**

Ofcom's Media Use and Attitudes Report

Publication of Ofcom's **report for 2024** is imminent.

Last year's report published on 29th March 2023 highlights include:

- Ownership of mobile phones is increasing gradually by children up to 8 years of age, rate of ownership accelerates to levels that are near universal among children aged 12. The acceleration coincides with the move from primary to secondary school.
- Older children (12-17-year-olds) were most likely to use mobile phones (69%) to go online, while those aged 3-11 (64%) were most likely to use a tablet for this purpose. Ownership of mobile phones increases gradually up to age 8, when the rate of ownership accelerates to levels that are near-universal among children aged 12 and remains so into adulthood. This acceleration coincides with the move for many children from primary to secondary school.

Children aged 3-4 years:

- mainly watch videos online(92%)
- YouTube is by far their most-used app (87%),
- more likely to use YouTube Kids (51%)
- almost two-fifths of 3-4-year-olds (38%) had their own profile on YouTube

Check the online activities of 3-4 year-olds

Guidance on Mobile phones in schools

The Department for Education (DfE) published new guidance for schools in England on prohibiting the use of mobile phones by pupils. The guidance:

explains how to develop, implement and maintain a policy that prohibits the use of mobile phones and similar smart devices during the school day.

aims to help schools reduce distractions and disruption caused by mobile phone use, as well as reduce the risks of peer pressure and bullying.

Alongside the guidance, there are case studies, a toolkit and information on creating a mobile phone-free school environment.

Read the guidance: Mobile phones in schools

For more information contact
Scomis: 01392 385300
E: scomis@devon.gov.uk

Helpline for staff solely dedicated to supporting the children's workforce:
The Professionals Online Safety Helpline (POSH):
Website Tel: 0344 381 4772

Free Resources

Need free Online Safety Resources?
Internet Matters
NSPCC CEOPS
ThinkUKnow BBC UK
Safer Internet Centre

SCOMIS Your ICT Partner