Cyber Security Guidance for School Staff

As you will be aware, Cyber security attacks are increasing of late in education. Schools that use LGFL are very well protected with LGfL firewalls and web filtering along with Sophos Antivirus. Schools not using LGFL will have in place their own firewalls and Anti-Virus software, which is also often Sophos. It is absolutely vital to your school that both your filtering is regularly maintained and that your Anti-Virus is also regularly updated. But that is only half the story, a large part of your protection comes through the actions performed by your staff when receiving unsolicited and unexpected emails.

The number one cause of most hacks is due to staff downloading or opening an attachment from unknown or sometimes known sources if the email address has been spoofed and so does not actually come from that source.

Even with up-to-date antivirus in place, hackers are creating new ways to get past your defences which is why your antivirus is constantly updating in order to add extra protection with the new ways hackers develop as soon as they are detected.

Vigilance is key for all your staff who use your email system. Anyone can unintentionally trigger a potential breach in your security, just by clicking on an inappropriate icon or link in an email. Below are some helpful suggestions to make navigating this new landscape a little easier and safer.

The basic advice is: Don't trust any email you receive that contains any of the following:

- Unexpected email / content from someone you know.
- An email from someone you don't know.
- An email that has mistakes in the spelling of the name or the email address.
    - i.e., NorTon (instead of Norton).
    - A slightly amended email address name such as yourschool.net, rather than yourschool.co.uk for instance.
- An email which has poor grammar and spelling in the content.
    - I.e., the email doesn't read well, plural words are used incorrectly or not used when they should be.
- Any email that asks you to send money or your personal details for any reason via any methods to anyone.
    - No legitimate business will ask you for these via email for any reason, only criminals do this.
- The email has no subject and / or no content, just an attachment.
    - I.e., The attachment and maybe subject looks like an invoice or similar document.
- The senders email address appears to be a random jumble of letters and numbers.
- The senders email address is from a different country,
    - I.e., New Zealand (.NZ), etc

t. 0345 222 1551 **f.** 01908 410063 **e.** hello@schoolbusinessservices.co.uk
www.schoolbusinessservices.co.uk
Head office: Poole | Suite 22, Discovery Court, Wallisdown Road, Poole, Dorset, BH12 5AG
Registered in England No. 06443524

If you receive a suspicious email…

DO:

- Contact your ICT Support Company, forwarding a copy of the suspicious email.
    - Action can then be taken to investigate the potential threat and block if necessary.
- Delete the email.
- Contact the alleged sender to verify the email content, but not by replying to the email, not by clicking any links in the email and not by calling any telephone numbers shown in the email. All can be false.
    - Look up online the advised sender and use the telephone number listed on their website (not from a link in the email).
    - As above for any email contact details (don't reply to the email).
- For Personal Devices, especially Android: If your email supports the function, you can 'Report' the email and that will automatically delete it and block from your device.

DON'T:

- Click on any links within the email.
    - If you do, you will likely be taken to a website containing malicious code that may look like a legitimate website.
    - It is quite possible that you will enable a criminal to access all of your contacts and documents, etc.
    - It is quite possible that all of your identity and bank details will be accessed and used that your device has access to.
    - You may well have your email address spoofed to enable it to be used in a Denial-of-Service attack, whereby criminals use your email, mailbox, and system to send out 1000's of spam emails to everyone in your contact list as well as everyone else that has clicked on the link and their contacts.
- Open any attachments in the email.
    - If you do, you will activate whatever malicious package is stored in the attachment.
    - It is quite possible that you will enable a criminal to access all of your contacts and documents, etc. as well as everything else that can happen for clicking on links above.
- Reply to the email.
    - This will flag that the email account (yours) is legitimate, and therefore a target for further attacks.
- Forward the email to anyone other than your ICT Support Company
    - If you do, you increase the possibility of someone else activating the malicious content.
    - You could, unwittingly spread malicious code/fraudulent activity.

There is a free webinar from LGFL below (with limited spaces) which we recommend a few of your staff sign up to, to become more aware of cyber-attacks: https://booking.lgfl.net/book/add/p/33
Further information regarding Cyber security and LGfL can also be found here:
https://national.lgfl.net/security/protectionlayers

t. 0345 222 1551 **f.** 01908 410063 **e.** hello@schoolbusinessservices.co.uk
www.schoolbusinessservices.co.uk
Head office: Poole | Suite 22, Discovery Court, Wallisdown Road, Poole, Dorset, BH12 5AG
Registered in England No. 06443524