April 2020

SYSTEMIT

CYBER SECURITY GUIDE *for Education*

Falling victim to cyber-crime can be devastating. Although the potential rewards in targeting schools are lower for cyber-criminals, the damage those with malicious intent could cause in terms of data compromise could have significant implications.

The National Cyber Security Centre (NCSC) have released guidance and taking these 5 steps will significantly increase your protection from the most common types of cyber-crime.

1. BACKING UP YOUR DATA

Take regular backups of your important data. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

- Identify what needs to be backed up. Make backing up part of your everyday work.
- Ensure the device containing your backup is not permanently connected to the device holding the original copy, or automatically accessible over a local network.
- Consider backing up to the cloud. This means your data is stored in a separate location away from your office/devices.

System IT can assist with full setup and daily monitoring of both onsite and cloud data backups. Give us a call on **01228 516555** or email info@system-it.co.uk to find out more.

2. PROTECT MOBILE DEVICES

Smartphones and tablets, which are used outside the safety of the school and home, need even more protection than ‘desktop’ equipment.

- Switch on PIN/password protection/fingerprint/facial recognition for mobile devices.
- Configure devices so they can be tracked, remotely wiped or remotely locked, if they are ever lost or stolen.
- Keep your devices, and all installed applications up to date. If available, look for the ‘automatically update’ option.
- When sending sensitive data, don’t connect to public Wi-Fi hotspots – use 3G or 4G connections, or use a VPN.
- Replace devices that are no longer supported by manufacturers, with an up-to-date alternative.

3. PREVENTING MALWARE

You can protect your school from the damage caused by ‘malware’ by adopting these simple and low-cost techniques:

- Use antivirus software on all computers and laptops. Only install approved software on tablets and smartphones and prevent users from downloading third party apps from unknown sources.
- Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. If available, look for the ‘automatically update’ option.
- Control access to removable media, such as USB sticks. Encourage staff to transfer files via email or cloud storage instead.

4. AVOIDING PHISHING

In phishing attacks, scammers send fake emails asking for sensitive information, such as bank details, or containing links to malicious websites.

- Ensure staff don't browse the web or check emails from an account with Administrative privileges. This will reduce the impact of successful phishing attacks.
- Scan for malware and change passwords as soon as possible if you suspect a successful attack has occurred. Don't punish staff if the get caught out, as it may discourage people from reporting in the future.
- Check for obvious signs of phishing, like poor spelling and grammar, or low-quality versions of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

5. USE PASSWORDS

Passwords, when implemented correctly, are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

- Make sure all devices use encryption products that require a password to boot. Switch on password/PIN protection or fingerprint/facial recognition for mobile devices.
- Use multi/two-factor authentication (MFA/2FA) for important websites like banking and email, if you're given the option.
- Avoid using predictable passwords. Think of 3 random words, and include numbers and symbols for added complexity, e.g. BikeLines+Stamp55
- If you forget your password, or you think somebody else knows it, change it, or contact System IT as soon as you can.
- Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.
- Provide secure storage so staff can write down passwords and keep them safe, but not with the device. Ensure staff can reset their own passwords, easily.
- Consider using a password manager. If you do use one, make sure that the 'master' password, that provides access to all your other passwords, is a strong one.

Watch the video below on **The Dos and Don'ts of Coronavirus (Covid-19)** and remember our tips for secure home working.

Working from Home - Tips and Pointers

- Do not click on links or download attachments from unknown sources
- Use a VPN (Virtual Private Network) for extra security
- Create strong passwords
- Ensure your antivirus is up to date
- Avoid the use of Public Wi-Fi
- Use Multi-Factor Authentication
- Secure your home router and Wi-Fi

For more information on any of the above, please get in touch with us today on **01228 516555** or email **info@system-it.co.uk.**

You can find more of our Newsletter's stored in Sharepoint Online, click the logo to view more