Getting Your School Cyber Safe

0121 309 0126 | www.cybersecure.school

CONTENTS

WHY YOU SHOULD TAKE CYBER SECURITY SERIOUSLY

You may think that schools will not be attractive to cybercriminals, after all, there are far more lucrative targets out there. No doubt you have read stories of attacks on banks, big business and even government institutions. For example, at the start of 2021, a US fuel pipeline company paid a $5million ransom to cybercriminals to recover their data. However, since the start of the Covid 19 pandemic there has been a rapid rise in the number of cyberattacks on schools, so much so that the National Cyber Security Centre has urged schools to take urgent steps to better protect themselves from such threats.

But why schools?

Quite simply, cyber attackers see schools as easy targets. For one, schools keep sensitive data, essential to the smooth running of their schools which they are duty-bound to protect. Secondly, IT networks in the education sector is one of the least protected – a hacker simulation test carried out by a leading anti-virus software vendor was 100% successful in breaching 50 universities across the country. Lastly, education institutions are filled with hundreds or even thousands of users accessing the internet. It only takes one absent-minded person to click on a phishing email or bogus website to give cybercriminals access to a trove of sensitive data. Cybercriminals know that education providers will have little choice but to pay out to get their data back.

A third of schools that suffered a cyber-attack lost control of their systems, data, or money. For schools with already stretched budgets, being required to pay a ransom for the return of sensitive data would be a huge burden. Likewise, any system outage caused by a successful attack could prove detrimental to students' education not to mention the long-term effect of such a breach.

By Julian Brettle,
Cyber Solutions Manager, CYBERSECURE by Supreme Systems

TYPES OF CYBER ATTACKS AND HOW CYBERCRIMINALS ACCESS YOUR SYSTEM

There are two main types of cyberattacks on schools. The first is called a Distributed Denial of service attack or DDoS attack – which is when a cyber-attack shuts down the school's servers, website, or restricts its ability to access the internet. Hackers will disrupt a school's system by sending numerous access reports with the intention of overwhelming the network until it crashes.

The second (and most frequent type of attack) is called a Ransomware attack. This is where hackers prevent schools from accessing their systems or the data held on them. Typically, the data is encrypted, but it may also be deleted or stolen, or the computer itself may be made inaccessible.

Following a ransomware attack, cyber attackers will usually send a ransom note demanding payment to release the data. They will typically use an anonymous email address to make contact and will request payment in the form of cryptocurrency.

In recent incidents affecting the education sector, ransomware has led to the loss of student coursework, school financial records, as well as data relating to COVID-19 testing.

Cyber attackers can access a school's network through several ways:

1. Remote Access

Hackers can access a school's system via remote access systems such as remote desktop protocol (RDP) often used by staff to access school files remotely. The easiest networks to breach in this way will have weak passwords, a lack of multi-factor authentication (MFA), and unpatched software.

CONTINUED ON NEXT PAGE →

2. Phishing

Phishing is when an attacker tricks a user into believing an email or instant message is from a reputable person or entity. Attackers will use phishing emails to distribute malicious links or attachments that can perform a variety of functions. Some will extract login credentials or account information from victims.

Phishing is popular with cybercriminals, as it is far easier to trick someone into clicking a malicious link in a seemingly legitimate phishing email than it is to break through a computer's defences.

By Angela Hart,
Regional Director, CYBERSECURE by Supreme Systems

CHALLENGES FACING SCHOOLS AND TOP TIPS TO SECURE YOUR SCHOOL

Schools are faced with many challenges when it comes to protecting their networks from cybercriminals.

- Lack of resources and budget – There is typically a lack of finances to invest in cybersecurity, be it buying the right software or having the right IT staff.
- Cultural issues – 'Bring Your Own Device' culture is common in educational institutions, this can present difficulties in securing the wider network, particularly with IT staff already facing stretched resources.
- An absence of policy – Setting out IT policies for using the network and making sure those policies are adhered to is also a challenge for schools.
- Training – Many schools are unable to find appropriate cyber security training for their staff to help them spot cyber threats.
- School data can be spread across numerous platforms. This makes it difficult to restore their systems in a timely fashion following a cyber-attack.

Despite these challenges, schools must still secure their networks against unauthorised access and cyber-threats. The National Cyber Security Centre (NCSC) has recommended that schools take a "defence in depth" strategy to combat the growing threats. Put simply, this means that schools must deploy tools to protect their IT networks, educate their staff and have effective means to recover data.

With that in mind, here are our top tips for securing your school from cyber-attacks:

1. Have a robust anti-virus and anti-spam solution

Most viruses will enter an IT network via the internet and email. A good anti-virus and anti-spam solution will stop a good percentage of malicious emails from entering your system in the first place.

CONTINUED ON NEXT PAGE →

2. Use Strong Passwords, Check Your Access Policies

We cannot stress enough the importance of having strong passwords. Here's a tip – create your own policy for creating passwords. An example policy could be CityCAPSCarLOWColourSymbolSymbol. This password regimen will help you create a whole number of random passwords. Here's one I created earlier - LONDONvolvoRed!! Ensure staff do not use the same password on multiple accounts and that they are changing their passwords regularly.

Also, check who has access to what. There is no reason why all staff members should have access to all information on your school servers. Restrict staff access to drives and folders that contain the information required to do their job. Also, ensure you manage leavers effectively. Immediately change passwords when they leave and delete the account if no longer required.

3. Protect your portable devices with encryption

Schools use a lot of portable devices such as USB sticks. We recommend password protecting your USB devices as well as encrypting them so that if they do go missing the information on them will not be easily accessible.

4. Add An Extra Layer for Signing on

Two Factor Authentication is a security process where users provide two different authentication factors to verify themselves. This process is done to better protect both the user's credentials and the resources the user can access. When you log on to a website, for example, you may be asked to include a second method to confirm your identity – this is usually a text sent to your mobile phone, or an email sent to you to confirm that you are indeed the person trying to access the site.

5. Develop IT Policies

Policies will help schools set a uniform standard for their staff as to how they access IT systems. You can have policies that govern the use of passwords, the use of personal devices in schools and for accessing the internet. Schools should also create a cyber security incident plan that will outline what steps staff should take in the event of a cyber-attack.

CONTINUED ON NEXT PAGE →

6. Provide your staff with ongoing training

Providing basic training is essential to ensure all staff understand the basics of cyber security. This can be something as simple as sharing a handbook with staff and students including information about what to look out for, and tips for practising good cyber-security hygiene.

7. Get Certified

Cyber Essentials is a government-backed certification scheme that covers the essential actions every organisation should take to ensure its digital security and protection from cyberattacks. Getting certified can protect your school from 98.5% of the most common cybersecurity threats. It's also a great indicator of your school's commitment to security and data protection. Completing the Cyber Essentials certification also has a long-term benefit. By putting in place the measures needed to complete the assessment, you'll also create a culture of cyber safety – helping to protect your institution against future threats.

8. Get a good backup solution

We highly recommend having both onsite and offsite backups. Your backup solution should also allow you to recover your data, applications, and emails, quickly in the event of a cyber-attack.

By Tom Burnett,
Technical Lead, CYBERSECURE by Supreme Systems

WHAT YOU SHOULD DO IF YOU SUFFER A CYBER ATTACK

First thing don't panic, but you need to act fast! Your cyber incident response plan should include a step-by-step guide of what staff should do in such an eventuality. For instance, one of the most important guidance should be that if a user has accidentally clicked on a malicious link, they should immediately switch off their device and disconnect it from the mains. That way it is quarantined from the whole network.

Other Steps to Take After a Cyber Breach

1. Contain the Breach

Here are a few immediate things you can do to attempt to contain a data breach:

- Disconnect your internet.
- Disable remote access.
- Maintain your firewall settings.
- Install any pending security updates or patches.
- You should also change all affected or vulnerable passwords immediately. Create new, strong passwords for each account, and refrain from reusing the same passwords on multiple accounts. That way, if a data breach happens again in the future, the damage may be limited.

2. Assess the Breach

If you are one victim of a broader attack that's affected multiple schools, follow updates from trusted sources such as the NCSC who will be monitoring the situation to make sure you know what to do next.

You'll also need to find out who may have been affected by the breach, as it may have affected people outside of school too – for example, suppliers or even parents. If you have suffered a data breach, assess how severe the data breach was by determining what information was accessed or targeted, such as birthdays, mailing addresses, email accounts and credit card numbers.

CONTINUED ON NEXT PAGE →

3. Inform People

You will need to notify people that the breach has happened. Inform your IT department, senior leadership team, governors, staff members, etc. Also, inform parents and other third parties too if the breach may affect them.

If you have cyber liability insurance, inform your provider immediately.

You can also report cyber incidents to Action Fraud - the National Fraud and Cyber Crime Reporting Centre (actionfraud.police.uk). If the incident involved a data breach, we would need to report it to the Information Commissioner's Office (ICO) under GDPR guidelines.

By Aidan Doyle,
Client Services Manager, CYBERSECURE by Supreme Systems

HOW SECURE IS YOUR SCHOOL?
Book Your Cyber Security Audit to Find Out

Let us help you pinpoint weaknesses and gaps in your IT infrastructure as well as any gaps in staff knowledge. We will review your current cybersecurity safeguards to see if they are robust enough to withstand a cyber-attack.

> The team at Supreme worked closely with us providing constructive advice, in a format and language we could understand, that gave us the confidence to entrust the works to them. They managed the process seamlessly from start to finish, and provided an excellent level of service throughout.
>
> **Nick Coley, Fitzgerald Civil Engineering Contractors**

We allow a full day for our audits as we will review:

- Router and Firewall
- Antivirus and endpoint security
- User account security
- Access Controls
- Password Management
- Remote access
- IT Policies
- Wi-Fi security
- Endpoint and server patching
- Email and collaboration tools security
- Cloud application security
- 15-minute knowledge assessment interview with five staff members
- Plus, if you do decide to apply to get Cyber Essentials, we will carry out your assessment for free – you will only have to pay the fees applicable to the certification itself.

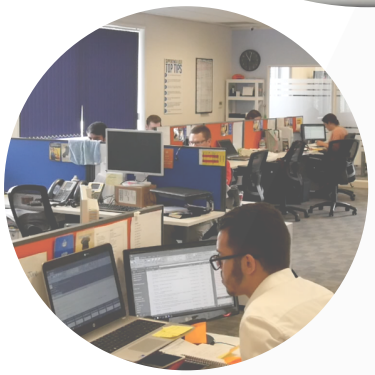
Our cyber security audit is just £999 plus VAT. Get 20% off with offer code GETSECURE

Call Julian Brettle, our Cyber Solutions Manager on **0121 309 0126** to arrange your audit, or send him an email to **julian@supremesystems.co.uk**

ABOUT SUPREME SYSTEMS

Supreme Systems, founded in 2008 is an ICT company based in Birmingham. We are one of the first ICT Companies in the West Midlands to achieve Cyber Essentials Plus, the highest accreditation for Cyber Essentials, the Government-backed scheme that helps organisations protect themselves against the growing threat of cyber-attacks. Since certification, we have helped hundreds of organisations achieve certification, with every single one passing first time.

We also help businesses secure their IT networks from cyber threats, by recommending and implementing robust ICT solutions to tackle those threats. No solution is 100% guaranteed but we are pleased to report that since launching our cybersecurity arm in 2015, we have had only one customer suffer a serious cyber-attack due to employee error. Luckily, no data was lost or compromised because of the disaster recovery solutions we put in place.



Your school is in safe hands with Supreme Systems. Watch our video to find out how we help schools like yours, read our staff profiles and customer testimonials to get a feel for how we work, then contact us to discuss your needs.

National Cyber Security Centre

Department for Education

CYBER ESSENTIALS

Barracuda

eset ENJOY SAFER TECHNOLOGY™

Contact Us

To find out more about CYBERSECURE and how we help schools get cyber safe, visit our website at **www.cybersecure.school**

CYBERSECURE
by Supreme Systems