Beaming

CYBER SECURITY FOR SCHOOLS

How to protect your school and students in a connected world

Introduction

In March 2021 the National Cyber Security Centre issued an alert to schools, colleges and universities warning of an increase in malware attacks – in particular ransomware - targeting education establishments.

What do schools have that cyber criminals want?

In short, data and money. In a ransomware attack, malware infects the school, college or university's network and cuts off access to vital systems and data until a ransom is paid. Disruption to students' learning can't be tolerated for long, so in the eyes of cyber criminals, education establishments are a good target for this kind of attack.

Safeguarding students from online harms

In addition to the threat of cyber attacks, schools have the responsibility of protecting students from harmful and inappropriate online material.
We've divided this guide into two sections. One is for teaching, admin & support staff, to help them understand the simple measures we can all take to help protect against cyber attacks. The second focuses on considerations for management and IT staff when it comes to both the protection of the school's systems and the safeguarding of students.

Contents

TEACHING, ADMIN & SUPPORT STAFF

Our easy-to-follow guidance helps school staff play their part in protecting data and networks.

>

Seven simple ways to improve cyber security

*** PASSWORDS

Your log in credentials give access to school systems, your own private data and confidential student data, so they must not be easy to guess. Bear in mind that the "guesser" here is not human – you're up against sophisticated computers with databases full of common and previously breached passwords. **Ensure passwords are unique, long and strong by following our guidance >**

MULTI FACTOR AUTHENTICATION

Try to enable multi-factor authentication (MFA) on any accounts that make this possible. This means that even if your password is breached, an attacker couldn't gain access to your account without meeting at least one other requirement such as entering a PIN sent to your mobile, details from memorable information you've provided, or even biometric data such as your thumbprint.

BEWARE PHISHING

Phishing emails can be used to trick you into installing malware on your computer (and in turn, the whole network) or sharing sensitive data, usually by clicking a link or downloading an attachment. These attacks have become increasingly sophisticated and while many take a "scattergun" approach by sending out mass emails to try and hook your attention, others may be extremely targeted to you and the organisation you work for. **Here's more advice on spotting & dealing with phishing attacks >**

RUN UPDATES

It can be annoying to run updates when you have work to get on with, but operating system and software updates often fix bugs you're unaware of which could otherwise be exploited. Allow updates to run as soon as they become available.

USB USE

Your school may restrict your use of USB memory sticks, but if you do use them, be very wary of plugging anything in to a USB port unless you know exactly where it's come from. Instead of storing sensitive data on portable memory devices, which are easily lost, try to use secure cloud storage or even better, when you need to access network files from a remote location, use a VPN.

PHYSICAL SECURITY

Don't forget physical security – a cyber attack could be initiated by someone with unauthorised physical access to a computer on the network, so be wary of allowing access to your computer unless they're a recognised member of the IT team. If you work using a laptop or tablet on public transport, consider using a privacy screen to ensure no prying eyes can see confidential information over your shoulder.

PROTECT MOBILE DEVICES

Protect laptops and tablets with automatic screen locks and multi-factor authentication, and activate remote data wiping so that if it were to be lost or stolen, others would not be able to access data or the network.

Good password practice

Your password is the key to a wealth of data on your school systems, from confidential emails to sensitive student data. If it's easy to guess or you re-use the same password (or even the same one with slight variations each time), cyber criminals may already have it in a database and could use it in an automated attack to gain access to the network.

How to choose a strong password & keep it safe

1. Avoid easy to guess passwords (birthdates, sports teams, pets name etc).
2. Use a combination of 3 random words to make a strong but memorable password.
3. Use completely different passwords for work and personal accounts.
4. Ideally, you'd have a separate password for every log in, but at the very least ensure that you keep your most important accounts (access to student records, your email) secure with a totally unique password.
5. Don't share your passwords with anyone.
6. Use multi-factor authentication for added security where available.
7. Consider using a password manager, which makes it easier to create & use unique passwords without having to remember them all.

Focus on phishing

Phishing emails use clever psychological tactics to trick the recipient into carrying out an action such as sharing personal or financial information, or downloading malware. The problem may not be immediately obvious, for example you may receive a (fake) request to reset your password and be taken to a website designed to capture your information. Those details will later be used to orchestrate an attack. Otherwise, you may be persuaded to download an attachment, which when opened allows ransomware to take over your computer and in turn the network.

Email users should follow these steps to help prevent becoming a victim:

1. Always check the email addresses

Look for deliberate mis-spellings in the email address designed to trick the eye or nonsense addresses full of random characters. When you reply, check where your email is being sent to as scammers can redirect your messages, giving them the opportunity to continue a conversation without raising alarm.

2. Look at how the email is written

There are certainly some clever scammers out there, so this is not a given, but some phishing emails contain poor grammar and spelling that would not pass the proof-reading or normal written style of the legitimate sender or organisation.

3. Don't automatically click

Be wary about clicking links or opening attachments in emails you hadn't expected, even if you (think you) know the sender. Store internal documents in a shared location instead of sending them to colleagues via email. When unsure, contact the sender via another means to validate their intent.

4. Use shift+delete

Delete suspicious emails straight away. Use shift+delete to make sure the email bypasses your recycling bin and is permanently deleted.

5. Be extra cautious on mobile devices

It may differ slightly from device to device, so make sure you know how to view the full email address of senders and how to check the full URL of any link you're directed to.

6. Don't overshare

As someone that works in education, your social media accounts are most likely private already. Be careful to remove any "friends" or "followers" you aren't certain you know in real life. Giving away personal information will make it much easier to scam you.

7. Being pressured should ring alarm bells

Think twice, especially if you are requested to carry out an action or share sensitive information. If you receive an email that asks you to click a link, download a file, share confidential information or divulge financial details, think before you act, especially if there's a sense of urgency.

8. Don't be scared to double check

If a request seems odd then always follow up verbally. You're demonstrating your commitment to data security so no one should be offended!

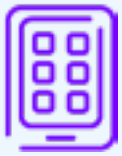
Working from home

When you have work to do at home, as teachers often do, it's just as important not to let your guard down and inadvertently allow cyber attackers to access the school's systems. Follow our guidance to keep data secure.

Stay up to date

Ensure that all of the software you are using when working from home is up-to-date. Use the latest version of your browser software and up-to-date antivirus that is actively blocking threats.

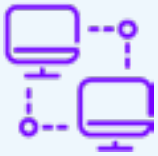
Please note that Windows 7 is now 'end of life', meaning Microsoft no longer offers patches and security updates. Some PC's running Windows 7 can still be upgraded for free to Windows 10.



Don't allow device sharing

Don't share access to work devices with family members.

All of the excellent work you've done to protect your school from the risks of cyber attacks can be undone in an instant if someone you live with accidentally downloads key-logging software or some other form of malware.



Secure data in motion with a VPN

You should be provided with a VPN or Virtual Private Network, which encrypts Internet traffic and makes the flow of data more secure.

This is the way to access documents containing confidential data – don't remove them from the school's systems.

Update your router & password

Secure your home broadband router. As well as ensuring that the firmware is up-to-date, change the default WiFi password within the router settings to something longer and more secure.

This will disconnect old devices (which is a reasonable security precaution in any case) and ensure new devices are accessing the network more securely.

IT TEAMS AND MANAGEMENT

Management and IT teams need to work closely to protect the school and students from online harms.

Your responsibilities

The Information Commissioner has previously advised schools to be particularly vigilant around information security. It has warned that unauthorised access to personal information would be particularly harmful to pupils; parents and staff; people with a right to seek compensation if the loss of their personal data caused them damage.

Educators need to think about the agility of their systems. If necessary, how quickly could they switch to a model where staff and students work from home without compromising on school cyber security policies? It's a serious consideration: If school resources were to be made inaccessible by a ransomware attack, learning and administration would become decidedly more difficult.

While the risks of malware and data theft are relevant to any organisation with personal data and computers, schools are particularly exposed to several other risks relating to online safety, including:

- Exposure to sexually explicit, racist, violent and extremist content
- Inappropriate contact from people who may wish to abuse, exploit or bully them
- Students themselves engaging in harmful online behaviour

Prioritising the physical and online safety of children continues to be a focus for schools' leadership teams and it's important that IT teams are able to review and implement changes to ensure their online safety.

In Beaming's experience, the most secure organisations use technology where appropriate, supported with clear policies and, most importantly, extensive user education. Our 12 steps to bettwer cyber security and safeguarding for schools are outlined on the following pages.

12 Steps to better cyber security and safeguarding

Schools should consider the following twelve pieces of advice when developing their own cyber security and online safety approaches.

1 Take ownership at senior level

The Government's statutory guidance requires that a member of the senior leadership team is made responsible for safeguarding in schools. Cybersecurity and online safety should be taken just as seriously. They should be discussed regularly with school governors and at leadership team meetings. Appropriate policies should be implemented and enforced by the senior leadership team.

2 Establish a strong online perimeter

Schools should establish strong boundary firewalls and internet gateways to protect school networks from cyber attacks, unauthorised access and malicious content. Cyber security controls should be monitored constantly and tested on a regular basis.

3 Update content filters, constantly

People are usually the weakest link in organisations. In schools there are many young internet users with curious minds that need extra protection. Content filtering systems need to be updated constantly as tech-savvy students are capable of creating new ways to circumnavigate filters with incredible speed.

4 Establish solid access control policies

Schools should establish effective processes for managing user privileges on their systems to minimise the risk of deliberate and accidental attacks. Users should be provided with the minimum level of access they need to do their job. When staff members leave the school, their access should be revoked promptly. All records should be kept up to date to prevent exploitation of old accounts.

5 Check third party providers thoroughly

Schools should ensure they vet thoroughly all third party platform providers used to ensure their approaches to security and safety are at least as stringent as their own. Access to students, parents and guardians should be granted by teachers themselves using email addresses provided in person.

6 Ensure secure configuration and patch management

Schools should know precisely what hardware and software is being used on their networks and ensure configuration changes are authorised, documented and implemented appropriately. Devices should be set up so that only approved users can make changes. Software updates and security patches should be implemented quickly when released by manufacturers.

7 Monitoring and incident management

Schools must monitor all of their systems continuously and analyse them for unusual activity that could indicate an attack. Criminal incidents should be reported to the police and other relevant authorities.

8 Invest in cyber sceurity and online safety education

The Department for Education requires that students are taught about online safety as part of safeguarding for schools. Leadership should ensure that members of staff understand the risks and their own security policies covering acceptable and secure use of systems. There should be regular sessions to ensure staff and students are aware of new phishing or spoof email attacks.

9 Don't forget about physical security

Planning should include the physical security of hard drives, internet routers, servers and other devices on which data can be stored. School equipment is targeted by thieves, especially in the school holidays, so any device holding sensitive data should be encrypted.

10 Consider personal devices

Schools should have clear policies around mobile technology and how it is used on their premises. Students should be taught about acceptable use of their personal devices, how they interact with each other on social media and where to turn for help. When staff are working from home, they should be provided with IT equipment that's for work use only and is not shared with others.

11 Use of VPN

When staff are working from home, VPNs should be used to ensure that data being sent back and forth to the school's network is encrypted, meaning that even if it were to be intercepted it would be indecipherable.

12 Staying in touch

For pupil safeguarding issues a voice conversation is often more suitable than speaking via email. However, staff calling pupils and their family members from their personal phones creates another issue in itself. Putting in place a cloud hosted telephone system can mitigate this problem. Call recording can also be a useful feature here, but call recordings must be treated as sensitive data.

How do young people get into cyber crime?

As cyber skills improve with each generation, some young people find themselves in possession of a skill set which is not fully understood by the authority figures in their lives and which they may not have the maturity to manage responsibly themselves. Without proper guidance, a talent for certain aspects of information technology can be used for negative means, rather than being channelled positively, resulting in a misguided venture into the world of cyber crime.

Cybercrime is an attractive choice for some, with potentially large returns. Young people can be particularly vulnerable targets; keen to make quick money and sometimes confronted with the expense of further education. In addition to this, the world of cybercrime represents a community to belong to and a way to feel powerful.

How are they recruited?

Vulnerable young people can be recruited into criminal networks through social media sites like Reddit and even Instagram. They're told that there are financial benefits and are taught related skills (if they don't already have them). Often, they act as the "fall guy" for a larger group of criminals. For example, in transactional fraud, the fraudster will offer money in exchange for the victim's PayPal account.

The criminal then uses this account, along with stolen credit card details to perform fraudulent chargebacks. Since the account is registered in the name of the young person they may be held responsible and prosecuted.

Others take a more active role in cybercrime, learning the skills to hack from online tutorials and message boards. They can then exploit the security systems of companies and take confidential information. This information is used to create fake identities or can be sold on. In some cases, this is done just to prove that it can be, with hackers vying for kudos.

The perceived anonymity of infiltrating a business from the comfort of home – as opposed to donning a balaclava and breaking in physically – means that young people may not fully comprehend the severity of their actions and the resulting consequences.

> "The cyber security industry is well known to be suffering from a skills shortage and the threat of cybercriminals has created a demand for people who understand how hackers think, can test a company's systems and provide security solutions.

How could these skills be put to good use?

The key to preventing teens and young people from committing this kind of crime lies in giving them the option to use their skills for good and letting them know that this can still be lucrative but without the risk of a prison sentence.

The cyber security industry is well known to be suffering from a skills shortage and the threat of cybercriminals has created a demand for people who understand how hackers think, can test a company's systems and provide security solutions. Young people should consider doing an apprenticeship or a degree to transition their skill set to work within an official organisation, creating positive outcomes.

Case study: Sabden Multi Academy Trust

The Sabden Multi Academy Trust had six educational sites to unite and needed to improve their network's security.

Challenges

When Beaming came on board, none of the Trust's six sites were linked and they had varying levels of connectivity. It was a frustrating situation; to operate efficiently and achieve best practice, the schools desperately needed to share resources. Security was another area of concern. The management of firewalls by another outsourced provider was unsatisfactory to say the least – with changes taking weeks to implement. The Sabden Multi Academy Trust's in-house IT team needed help fast.

Solution

Beaming had previously delivered 100Mbps fibre connectivity to one of the Trust's schools. Seeing the instant benefits of this upgrade, they asked us to continue the good work and overhaul the connectivity of the entire Sabden estate. We did this by developing a secure network built on a PWAN core, linking each of the six sites using Ethernet fibre connections. We've also taken over the firewall management, offering a fully responsive change control service. Further resilience is ensured by employing Layer 3 switches to control routing, providing automatic failover for the network.

> "We love dealing with a service provider that speaks our language! We were so used to long change request times but with Beaming, we now feel we can really communicate quickly and effectively with our ISP.
>
> **Phil Ridley, ICT Systems/Network Manager, Sabden Multi Academy Trust**

Results

The new network enabled the different schools to operate as an efficiently functioning collective, helping management, staff and pupils alike. It meets their specific security requirements and allows staff unprecedented working flexibility.

The Trust's IT team love working with a service provider that speaks their language. Having been so used to waiting a long time for firewall changes to be made, they know they can now communicate quickly and effectively with their ISP.

About Beaming - www.beaming.co.uk

If you want support with keeping your school safe, call Beaming. We are an Internet Service Provider (ISP) that works with primary, secondary and multi-academy organisations and unlike most providers, we own our network, which has been built for top-quality performance. We supply thousands of organisations across the UK with fast, reliable, and secure voice and data connectivity and managed services including content filtering and firewall management.

Cyber security is at the forefront of everything we do, and we are ISO27001 certified - the gold standard in data safeguarding. We can help you increase your resilience cyber-attacks.

Our teams are handpicked, not only for their great technical capabilities but their great people skills too. Our customers never end up talking to robotic sounding call centre operations.

Follow Beaming online and on Twitter to get regular updates on cyber threat analysis and new cyber security insights.

How to get in touch

Speak to our experts:
Call 0800 082 2868
Or email hello@beaming.co.uk
Or visit www.beaming.co.uk

Certificate Number 9849
ISO 9001, ISO 27001