isams
By IRIS

[DATA PROTECTION]

Common cyber scams in schools and how to avoid them

Table of Contents

Common cyber scams in schools and how to avoid them

Computer technology and software have become inexorably linked with the day to day running of schools. From a parent sending an enquiry and having their child accepted, to teachers taking the register and students completing homework, technology touches almost every aspect of school life.

The benefits of all this technology include more convenient methods of working, faster communication and greater flexibility, but as technology develops, so too do the methods of criminals intent on exploiting it for financial gain.

In 2020, the Department for Digital, Culture, Media and Sport conducted a Cyber Security Breaches Survey with a section focused specifically on the education sector. Its findings made for perturbing reading.

The results of the survey showed that 41% of primary schools, 76% of secondary schools and 80% of further education institutions had identified at least one cyber-attack or security breach in the previous 12 months.

Hackers and cybercriminals appear to be increasingly turning away from larger organisations in favour of targeting smaller institutions – seen as low hanging fruit - that may be less well equipped to deal with a scam or hacking attempt. We explored some of the most common threats to schools and some best practice to keep your digital infrastructure safe...

Three common cyber threats

Of the many ways in which IT systems can be compromised, three common threats make up the majority of attacks on schools and often cause the most damage:

- Ransomware
- BEC (Business Email Compromise)
- Insider threats

What is ransomware?

Ransomware is one of the most prolific and lucrative forms of hacking for cybercriminals. It involves compromising an IT system in some way, gaining access to the data contained within the system and then encrypting this data to prevent you from accessing it. Once the hacker has encrypted your data, they will demand a ransom to decrypt the information.

Schools that choose not to negotiate and pay a ransom are often hit with a second, more insidious demand. Ransomware is usually coded not just to encrypt important data, but to send this information back to the hacker. This is used as leverage in circumstances when schools refuse to pay, as hackers may then threaten to release sensitive data on the internet.

One such attack occurred as recently as June 2021, forcing the closure of two schools after hackers broke into their servers, stealing data and encrypting student information. With staff unable to access emergency information for students, the schools were forced to close their doors while the matter was resolved, and parents were asked to contact their banks should their details have been compromised.

Needless to say, this kind of attack is incredibly effective, but how does ransomware infect your school network? There are three primary infection vectors to note:

- Phishing attacks
- Malicious downloads
- Compromised credentials

BEC: Business Email Compromise

BEC (Business Email Compromise), also known as CEO fraud, involves an email account or address within a school or business being compromised by way of an infection vector or spoofed by a hacker. The hacker will send an email that may appear as though it has been sent from someone within the school – often from senior management or the finance team – asking for money to be paid to an account. These attempts do yield some successes for scammers but are more speculative when compared with an email account that has been fully compromised.

In this case, the hacker accesses an email account – usually via phishing – and then observes the email account over time, waiting for the right time to send an email. This is usually an exchange between a school supplier and the school, or between the school and a parent. The hacker parades as a supplier or school staff member and provides a new address for money – such as school registration fees – to be paid to. This is a far more effective scam because the email originates from a trusted email address – often a colleague.

Hackers will often try to bypass typical due diligence by incorporating a sense of urgency to the email e.g., 'this must be done before the end of the day!' Once a payment has been made it is often irretrievable and nearly impossible to trace.

As previously mentioned, BEC hackers increasingly are going after the 'low hanging fruit' of smaller organisations or less protected staff with emails that are readily available online (this is often the case with schools where some staff contact details are available in order that parents can make direct contact).

Interestingly, more than 30% of BEC emails are sent on Monday mornings, suggesting that hackers have identified this busy time of the week as the time at which staff are least likely to scrutinise an email for authenticity.

Other techniques to add credibility involve manipulating email subjects to include RE: or FWD: as an attempt to convince the reader they are reading a pre-existing, legitimate email thread. Hackers have even gone as far as to create real email chains to validate their false requests in the minds of would-be victims.

Insider threats

Another growing trend in hacking conforms more closely to the stereotypical notion of the hacker that many of us hold in our mind's eye – the ingenious, hoody-wearing teenager bathed in the blue light of a computer screen. This is the insider threat – hacking attempts perpetrated by students of the school they attend.

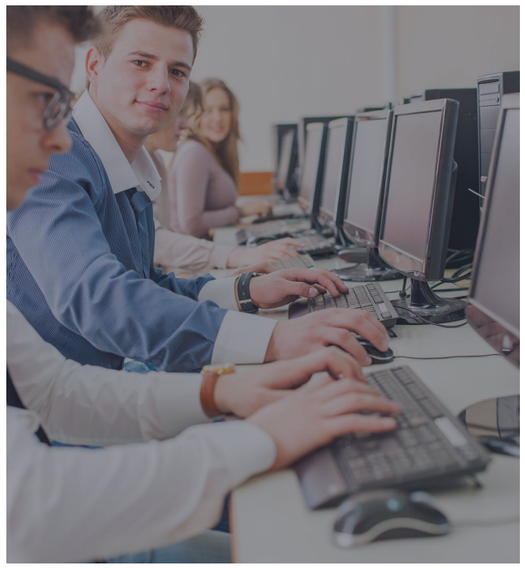
In 2011, a student managed to hack into the IT system of their school and expose the personal details of 20,000 people, including the medical information of more than 7,000 past and present students. In another similar case in 2014, 11 pupils hacked into their school's IT infrastructure and installed keylogger malware, a sophisticated programme that records every keystroke used on the computer whilst the malware is active, capturing usernames, passwords and messages sent.

One final case for consideration highlights the importance of diligence in password management. A school staff member left a post-it note stuck to their school computer, detailing their username and password for their school MIS (Management Information System) account. A student used the credentials to log in to the school's MIS and several other systems (for which the passwords were the same), exposing more than 20,000 records. This breach led to the school being disciplined by the ICO (Information Commissioner's Office).

DDOS (Distributed Denial of Service) Attack

A common form of Insider Threat is a DDOS (Distributed Denial of Service) attack – one of the best-known cyber-attacks because they happen regularly, often to very large companies and institutions. DDOS attacks utilise a network of computers or smart devices – often thousands at a time - to make data requests in unison, effectively drowning a system with more requests than it is capable of handling.

In April of 2021, Bradford Council's online learning network was hit with a series of DDOS attacks which caused chaos for teachers and students trying to continue teaching and learning throughout the pandemic. DDOS attacks are rarely used for financial gain, but rather to wreak havoc on a given system.



Best practice for defending against cyber scams and attacks

- Use a password manager to safely store machine-generated passwords – never write them down.
- Use 2FA or multi-factor authentication.
- Continually update software on your mobile and computer devices to protect against vulnerabilities.
- Train staff to spot phishing emails.
- Do not use personal devices – school-issued laptops and phones should all be set to the same security standards.
- If you suspect a system or email account has been compromised report it immediately.

How does iSAMS protect its client schools?

Enabling 2FA

As part of our ongoing attempts at iSAMS to combat cyber-attacks and scams, last year we implemented compulsory 2FA, having previously offered this as opt-in functionality. Schools must therefore enable 2FA as a minimum. iSAMS can act as the 2FA provider or use third party services such as Office 365 or Google and supports the Pwned Passwords check (Pwned Passwords are 613,584,246 real world passwords previously exposed in data breaches) to help school staff to identify a compromised password.

Protecting fee payments

Finance teams sending out invoices via email can be the perfect opportunity for a BEC scam. If the Bursar or a member of the admissions team at a school have their password compromised, scammers can then log in to their email, manipulate invoices and request payment from parents. Enabling 2FA restricts this scam by preventing hackers from accessing your staff email.

It's also possible to add another layer of protection by removing the ability for parents to pay via bank transfers.

We offer two methods to replace bank transfers with more secure methods for both domestic and international payments. The first involves migrating to a direct debit process, whereby parents do not have to send any money as the fee is requested directly from the bank. Our Fee Billing module has a dedicated Direct Debit module to automate this process.

We will also shortly be launching iSAMS Payments, which will sit within the Admissions Portal and Parent Portal. For domestic payments, parents will receive a notification to let them know there is an outstanding invoice, and they can log in to the portal, view the bill and pay it online using a debit or credit card. For international payments, parents have the choice to pay via one of our approved third-party integration partners, who manage the payment in multiple currencies in a secure manner.

Moving to the cloud

The final way we are looking to protect schools from cyber-attacks is by offering our schools a secure cloud hosted solution that moves them away from having on-premise servers, as without proper safeguarding technologies and protocols, servers become a target for cybercriminals.

We have invested heavily in several sophisticated protection services which are likely to be unaffordable to individual schools. Our servers – held in secure locations by Rackspace - are protected by Cloudflare. Cloudflare is a sophisticated performance and security service that – along with Rackspace - supplies protection against Distributed Denial of Service (DDoS) attacks. Cloudflare also features a Web Application Firewall that automatically prevents hacking attempts, flagging anything suspicious for our inspection.

We also provides 'Server Hardening' to Microsoft's recommended standards. This is a collection of techniques used to mitigate any vulnerabilities in our server infrastructure.

Another layer of protection is provided through Enterprise Managed Detection and Response (MDR), managed by a company called eSentire. eSentire delivers a managed detection and response service, which is deployed across the entire iSAMS server network, protecting your data from all forms of attack. This service is managed by a team of experts at their Security Operations Centre, who continually pull data from servers and scan it for threats and attacks.

Finally, schools on our hosted solution receive free server maintenance, saving schools time and money that could be better spent elsewhere. This goes for backing up your data too. Our servers are backed up every hour of every day, 52 weeks a year, with backups stored onsite and offsite for an added layer of security. This means you're unlikely to lose large amounts of important information in case of a hacking attempt.

Summary: top tips to protect your School

Technology

- Use a password manager to safely store machine-generated passwords.
- Always use 2FA or multi-factor authentication.
- Continually update software on your mobile and computer devices to protect against vulnerabilities.
- Ensure all school devices are set to the same security standards.
- Move to cloud hosting for your school servers.
- Avoid using bank transfers as a payment method for school fees.
- Deploy anti-virus and anti-malware software throughout your IT infrastructure.

Culture

- Train staff to spot phishing emails
- Do not use personal devices – school-issued laptops and phones should all be set to the same security standards.
- If you suspect a system or email account has been compromised report it immediately.
- Always check the email address you're receiving mail from to ensure it is genuine.
- Never download an email attachment from an unrecognised email address.
- Never open a suspicious email. Contact somebody within your organisation to check its validity.
- Never write down your passwords.

isams
By IRIS

9 Talavera Courwt, Darnell Way
Moulton Park, Northampton,
NN3 6RW, United Kingdom

T +44 (0) 1604 659100
E sales@isams.com
W www.isams.com