Cyber threats explained

UK EDUCATION SECTOR

Contains promotional material

ecclesiastical

Cyber threats

Introduction

The explosion in technology and internet use has also seen a significant rise in those looking to exploit the technology for financial gain or to cause damage and interruption to systems and services. In addition, a school's own staff could also cause significant damage either through intent or by accident.

Many cyber attacks use indiscriminate scatter-gun approaches to target victims. If you're a school, you are just as likely to be a victim of these scatter-gun attacks as a large organisation. Attackers may not know (or care) who you are until they get into your system.

According to a survey by the Ponemon Institute, **72%** of hackers are opportunistic and **69%** of hackers would quit an attack if a organisation's defences were discovered to be strong.[1]

The Ecclesiastical Education Tracking Survey found that **1 in 5 schools** had been subject to a cyber attack.[2]

A cyber security breach can damage a school in many ways ranging from disruption and data loss, damage through loss of intellectual property, denial of access to websites and services, physical loss or damage through viruses, ransomware and other forms of malicious software, reputational impact through damaged brand image and impaired relations with parents.

In addition, legislation such as the Data Protection Act 1998, and the European General Data Protection Regulation (GDPR) which came into force in May 2018, can impose penalties on organisations for not taking appropriate steps to secure or prevent access to data about individuals.

Cyber Crime

Cyber crime has now overtaken physical crimes such as burglary or robbery. Cyber criminals are highly organised and are finding a myriad of new and more sophisticated techniques to access data and information for the purpose of financial gain and to commit fraud. This can result in money being taken from a bank account or credit arrangements (such as loans or overdrafts) being arranged in your school's name for the benefit of a fraudster. There is also an increasing risk of the use of 'ransomware' where an attempt is made to extort money from you by preventing access to your computer system or files until a ransom is paid.

In the event that someone attempts to extort money from you, or hold your data or systems to ransom it's important that you do not pay the ransom demand without first seeking specialist advice. Paying even a small sum can result in an increased risk of you being targeted again in the future, as criminals share this information and in many cases, despite payment, access to the locked computer or files is not always restored.

Hackers will use any means available to find technical, procedural or physical vulnerabilities which they can attempt to exploit. They will use open source information such as LinkedIn and Facebook, and other social media to exploit user naivety and goodwill to elicit further, less openly available information, which they can then use to access your computer systems.

1. 2017 Cost of Data Breach Study, sponsored by IBM Security, conducted by Ponemon Institute Research Report, June 2017 (https://www.ibm.com/downloads/cas/ZYKLN2E3)

2. FWD Education Annual Tracking Survey 2017

Threat sources

Cyber criminals

Career cyber criminals are professionals who "work" in the digital shadows, and may well have made the jump from traditional crime into cyber-enabled fraud, using technology instead to lower the chances of getting caught.

The cyber criminal is motivated by one thing: money – and the more of it they can get their hands on, the better.

Cybercrime as a Service (CaaS), is the creation and sale of tools of cyber crime by third parties to criminals and has boomed over the last few years. There are also well established marketplaces that provide specialist cyber crime skills for organised criminals.

Right now, cyber criminals are all about mass phishing campaigns. They are low cost, easy to pull off, and promise a good return on investment. Spear phishing is still a big concern, and it's much harder to defend against, but for value nothing beats a good mass phish. Phishing is explained later in the guide.

Typically these campaigns are used to deliver malware payloads (often ransomware), and the emails usually include a strong social engineering component.

Hacktivists

Wikipedia defines hacktivism as "the use of computers and computer networks to promote political ends, chiefly free speech, human rights, and information ethics". As with hacking, hacktivism can also be a force for good or evil.

With the use of social media, hacktivists can now spread the word and recruit across the globe with a single tweet or a Facebook post to carry out their agenda driven attack.

Hacktivist groups have been known to target Higher Education establishments that are involved in Government defence or scientific projects.

Hacktivists overwhelmingly favour attacking websites. Since websites are often the most publicly facing aspect of an organisation, this makes perfect sense. Their methods may include **distributed denial of service (DDoS)** attacks, **website defacement, viruses** and **worms** that spread protest messages; taking over social media accounts, and stealing and disclosing sensitive data. These methods are explained later in the guide.

Nation states

The nation state hacker has a very high degree of technical expertise and sit at the top of the tree. They work for governments to disrupt or compromise other target governments, organisations or individuals to gain access to valuable data or intelligence, and can create incidents that have international significance.

They might be part of a cyber army or hackers for hire for companies that are aligned to the aims of a government or dictatorship.

The nation state hacker knows exactly what they're getting into, and knows full well that the mayhem they are spreading overseas is tacitly supported by their state. They can work without fear of legal retribution and often have close links to the military, intelligence or state control apparatus of their country.

Script kiddies

A script kiddie or 'skiddie' are the most common breed of hacker. Essentially bored teenagers or younger, with possibly some programming skill who mainly use programs developed by other, more experienced, hackers. These amateur hackers attack for fun and seek recognition amongst their peers. They tend to be un-targeted in their approach, finding thrills in bringing down any system.

Script kiddies have youth on their side. If caught, they're unlikely to get more than a slap on the wrist for their actions.

Script kiddies are influenced by others such as organised crime gangs, who may manipulate or recruit them to do their dirty work. They can be used as a diversionary tactic by criminals, creating a smokescreen of small, obvious attacks to mislead or distract investigators.

The tools they use vary, with many freely available and downloaded from the internet that are either used indiscriminately or as part of sophisticated, targeted attacks aimed at achieving specific goals. Given the abundance of hacking tools online and easy access to information, script kiddies are the largest threat by number and growing.

Cyber terrorists

These hackers, generally motivated by religious or political beliefs, attempt to create fear and chaos by disrupting critical infrastructures. Whilst this group has big ambitions, to date, there have been no publicly reported cases of terrorists using the internet to carry out cyberattacks; what has been done that has been atrributed to cyberterrorism is more akin to hacktivism such as website defacement.

Insiders

The insider comes in both accidental and malicious forms: the disgruntled teacher or office staff, the well-meaning innocent, or the supplier with trusted access to the school network. The insider may conduct their activites on purpose, through carelessness, or through outside influence - falling for a scam or becoming the victim of blackmail, for example.

This makes the insider one of the hardest threats to anticipate and defend against. The insider's position within an organisation can mean they can do just as much damage as the most sophisticated piece of malware. Whatever their motivation, the insider possesses access to the school's systems, and the means to breach or bypass defences with ease.

Alternatively, insiders may simply be a well-meaning individual trying to help what they think is a parent, contractor, colleague or student out.

Tech-savvy students

Modern students are very tech-savvy, having been taught coding from an early age and like moths to a flame, curious students can often look to push the limits of what they are taught in class.

They have access to powerful computers, YouTube tutorials and chat forums detailing how to execute basic and advanced hacks, and time—and at younger and younger ages. They explore, tinker and express themselves. As a result, they can often be far more advanced in their technical knowledge than many of the adults at the school.

There have been several examples where spyware or keystroke logging hardware was used to discover passwords and gain access to protected areas on the school's computer network to change grades or access sensitive information on teachers and other pupils.

Example: In 2012 a student hacked the systems of an academy. Having cracked a staff member's password, he tried it across other administrative systems and found it worked – making him privy to 20,000 individuals' information, including medical information on 7,600 pupils.

What was once stored in locked cabinets in an office is now stored on a computer network designed to enable broad internal and external access.

Threat actions

The threat to the education sector is varied and ranges from high volume, automated and opportunistic attacks to highly sophisticated and targeted attacks involving bespoke malware.

Malware

Malicious soft**ware** or malware for short is software that can be used to compromise computer functions, steal data or otherwise cause harm to the a computer. Malware is a broad term that refers to a variety of malicious programs.

Most malware requires user error or in-action to make it onto a computer system. Usually, hackers will try a variety of tricks to get victims to download, install, and run malware on their computers or devices. Malware distribution is largely dependent on social engineering for this purpose.

Common types of malware - There are over **10million** new types of malware discovered each month and in 2018 the total of Windows-based malware exceeded **850million** types (only **47million** in 2010).[3]

Virus

Just like a biological virus a computer **virus** has similar traits. Viruses pass from one computer to another. Like biological viruses, they can't reproduce on their own and need a host i.e. a program or document. Viruses must be activated by the user in order to cause trouble.

Trojan Horse

A **Trojan Horse** or **Trojan**, takes its name from the famous wooden horse and operates in a similar way. **Trojans** are installed on a victims machine through deception and would appear to be a file or document. They then spring into action and can delete files, destroy information or allow outsiders to access the computer.

Spyware

Spyware includes any type of program that spies on a person's computer actvities. It may gather personal information such as usernames and password or account numbers. It may also track any websites that you might visit or emails you send and receive.

Worms

Worms are standalone programs that are often disguised as an attachment and are installed once it's opened. The worm can spread in many ways and can travel from one computer to another without any human interaction. Once activated, worms can open up remote access for hackers or enable the computer to be used in a Denial of Service attack (DoS).

3. AV test, april 2019 https://www.av-test.org/en/statistics/malware/

Ransomware

Ransomware is an aggressive form of computer malware that is designed for direct revenue generation. The most common type today is crypto-ransomware, which aims to encrypt data and files. The other, known as locker ransomware, is designed to lock the computer, preventing victims from using it and it then demands a ransom for its release.

The technology driving ransomware is increasingly advanced and uses 'zero day' flaws that may not be in the public domain, so can be difficult to detect by many anti-virus programs currently in use today. The criminals either go for volume to infect as many victims as possible or they zero in on the human element, relying on tricking staff into interacting with an innocuous looking email, file or web link. Even with regular training, it only takes a single momentary lapse in judgement from a user to result in an infection.

Example: UK schools were targeted in 2017 by attackers posing as a 'Department of Education' official requesting the personal email of the headteacher in order to forward some forms. An email was then sent to the Head with a zip file attachment that was infected by ransomware. Once the attachment had been downloaded the ransomware locked and encrypted computer files and asked for a ransom of up to £8,000 to regain access.

Some newer forms of ransomware, rather than just encrypt files also threaten to leak them online. Given the volume of sensitive data that schools hold relating to children and their very strong reliance on data, ransomware represents a significant threat.

Research from the cyber security company Symantec shows that ransomware attacks worldwide increased by 36% in 2017 — with more than 100 new malware families introduced by hackers.[4]

Example: In March 2019, hackers used ransomware to infect an Academy's systems and encrypted GCSE coursework that had been submitted by pupils. The email containing the ransomware had been 'spoofed' or made to look like it came from a nearby school and was mistakenly opened by a member of staff.

4. Symantec Internet Security Threat Report, Vol 22. April 2017 (https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf)

How is malware distributed?

Email attachments

Malware is often disguised as innocent email attachments in phishing emails. Users are tricked into downloading software that poses as an invoice, form, image, or other document. Once on the user's computer, the malware either unpacks itself or waits for the user to attempt to open it before executing its code.

Microsoft Office formats such as Word, PowerPoint and Excel make up the most prevalent group of malicious file extensions. According to the 2018 Symantec Internet Security Threat Report **71%** of all **targeted** attacks started with **spear phishing**.[5] Further information on spear phishing can be found later in the guide.

Web links

Other techniques include directing victims to web sites under the pretence of a threat e.g. **"suspicious activity has been detected on this account"**. These links typically lead to malicious sites that host 'Exploit Kits' which download malware onto computer when the page is loaded.

Storage devices

Some hackers leave malware-infected USB flash drives or other storage devices in public locations where they're likely to be discovered. When someone plugs the storage device into a computer to determine its contents, malware in the device can transfer itself to the computer and infect it.

Denial-of-Service (DoS) attacks

"Denial of service" or "DoS" describes the aim of this class of cyber attack that's designed to render a service inaccessible. The common type of DoS attack is those that are launched against websites. When a website suffers a DoS attack, the apparent effect will depend on its use. For the average user, it appears that the site has simply stopped displaying content. For others, it could mean that the online systems they depend upon has ceased to respond.

DoS attacks can range in duration and may target more than one site at a time. An attack becomes a Distributed Denial of Service', referred to as "DDoS", when it comes from multiple computers instead of just one.

Sequel injection attack

A sequel injection also known as SQL injection or SQLi refers to a weakness that may allow hackers to steal or tamper with a database sitting behind a web application. This is achieved by sending malicious SQL commands to the database server, typically by inputting code into forms – like login or registration pages. A SQL injection is the most common form of web site attack, often common web forms are not coded properly and the hacking tools used to find weaknesses and take advantage of them are commonly available to be downloaded online.

5. Symantec Internet Security Threat Report, Vol 23. March 2018
https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

Phone fraud

Phone or PBX fraud (Private Branch Exchange is a private telephone network) entails external hackers taking over control of the school telephone system, routing international or premium calls through it. The losses involved can be high, especially when they are made during times that a school may be closed, for example the summer holidays. During this period it is likely that the fraudulent calls will go un-noticed until the telephone bill arrives.

Example: Figures from the National Fraud Intelligence Bureau show that between September 2017 and March 2018, 48 schools reported incidents. Of those, 12 lost £145,124 between them and one lost £19,150. Action Fraud has also known of schools returning from holidays to a £100,000 bill.[6]

Internet of Things (IOT) attacks

By 2025, it is estimated that there will be approximately 75billion connected devices around the world.[7] With more IoT devices – from cameras to alarms appearing in schools, cybercriminals are keen to leverage them in attacks. This heightened interest is due to the vulnerabilities in many IoT devices, not to mention their ability to connect to each other, which can form an 'botnet'.

In a botnet scenario, a network of internet-connected devices is infected with malware and controlled without the schools' knowledge, in order to launch ransomware and DDoS (Distributed Denial-of-Service) attacks.

Example: There were several incidents in 2018 which involved hackers who were able to break into and take control of connected CCTV cameras and stream footage of pupils live on the internet.

Personal Bring Your Own Device (BYOD) and school devices

There are an abundance of actual physical devices that students could bring to school, they include devices such as laptops, notebooks, mobile phones, tablets, phablets and the list goes on. BYOD is an attractive prospect for schools. It can help free up already restricted budgets, diminish the digital divide, increase the computer-to-student ratio, and improve engagement and motivation.

Schools are vulnerable to data theft, especially if staff or students are using unsecure mobile devices to share or access school data. As more small schools make use of BYOD technology, internal networks could be at risk from unsecured devices carrying malicious applications which could bypass security and access the network from within the school.

Phishing and spear phishing attacks (social engineering)

Phishing is an exploit that uses a disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they need or want. It is the simplest kind of cyber attack and, at the same time, the most dangerous and effective. Spear phishing is a targeted attack unlike traditional phishing which is indiscriminate.

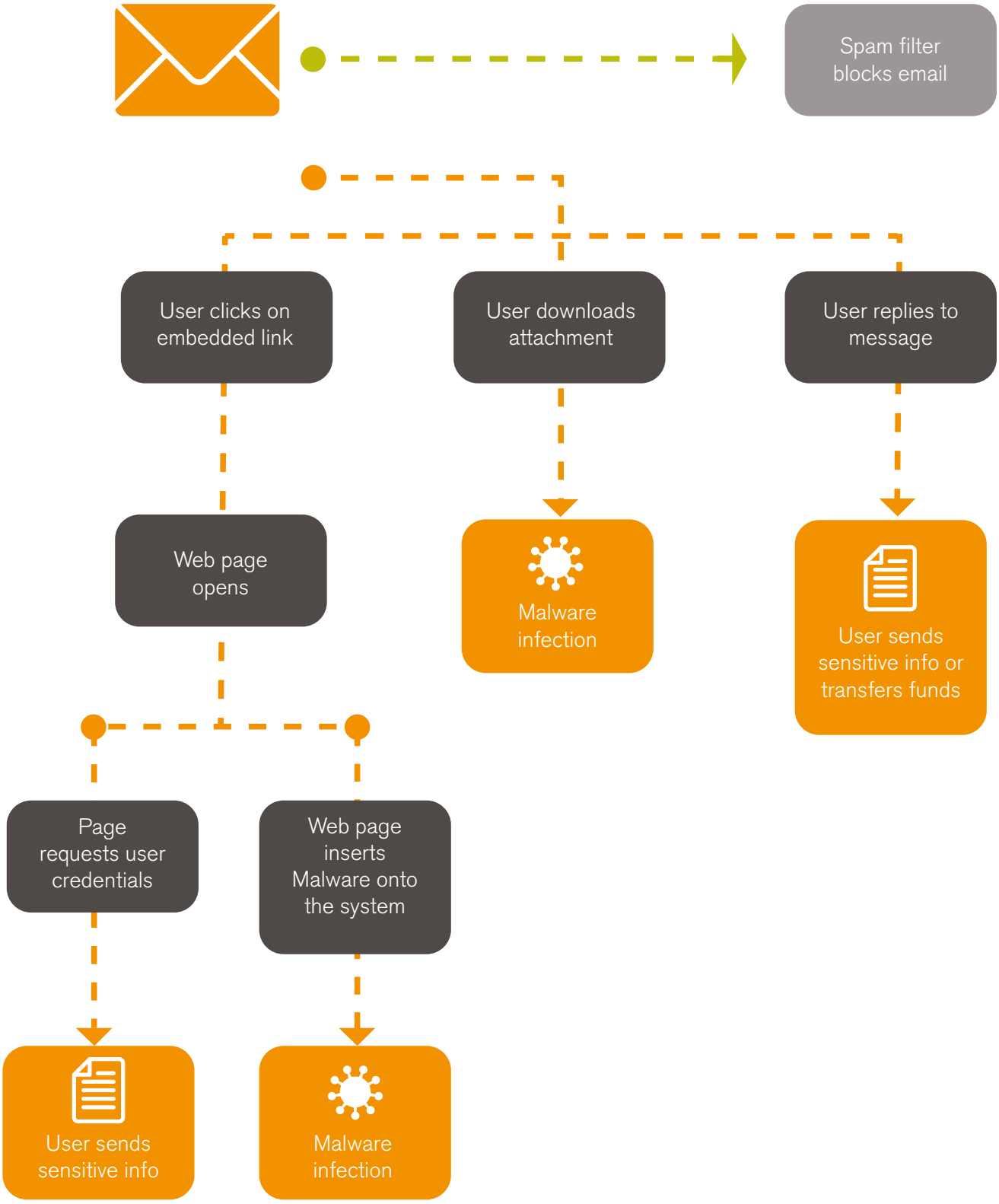
Invoice scams are a serious threat to schools of all sizes and represent one of the fastest growing, lowest cost, highest return cyber crime operations. A cyber criminal will impersonate a trusted person and attempt to coerce a staff member to transfer funds to the phisher's account or divulge sensitive information.

6. National Fraud Intelligence research 2017/18 https://schoolsweek.co.uk/schools-lose-145k-to-fraudsters-posing-as-heads-in-new-scam/

7. The Statistics Portal Statistics and Studies from more than 22,500 Sources. Internet of Things (IoT) connected devices installed baseworldwide from 2015 to 2025 (in billions) https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

For example, a school undergoing refurbishment or undertaking works may be contacted by someone pretending to be their contractor. They might suggest that there's been a change in bank details or promise a discount for early payment.

How a phishing attack works



Example: Fraudsters impersonating headteachers have also been able to defraud schools across the country out of tens of thousands of pounds. The scam involves a fraudster creating an email address that's similar to a particular headteacher's and using it to contact members of staff with responsibility for authorising financial transfers. The criminal, pretending to be the headteacher, then asks for an urgent one-off bank transfer, with the amounts requested ranging between £8,000 and £10,000. One school lost £19,150 in one go, while the average loss was £3,023.

Similarly parents with children at fee paying schools have also been targeted by criminals impersonating the school. Term fees of between £4,000 and £10,000 are an attractive target for criminals and it's often the case that the school was tricked by spear phishing attack into releasing their contact lists.

In the three months after the introduction of the GDPR, the ICO, who are the regulator received an average of 500 calls a week to their breach reporting line. Collected data has identified that 50% of these related to phishing attacks. Malware (10%) and ransomware (6%) were also other notable causes of breaches reported.[8]

This is not the first time schools have been preyed on by cyber criminals. In March 2018 Ofsted was forced to issue a warning after phishing emails purporting to be from the organisation were sent to schools apparently asking for fees to be paid via PayPal. Also, back in February 2016, schools faced a different sort of challenge after a prankster who called himself "Uncle Rafool" called up more than 150 and impersonated an Ofsted inspector, telling staff they had lost their jobs before uploading the recordings to YouTube.

Password attacks

Password attacks refer to various measures used to discover computer passwords. This is usually accomplished by recovering passwords from data stored in, or transported from, a computer system. Password attacks are performed is several different ways and some of the most common are as follows:

- Brute force attack
  If a school publishes staff names, then a hacker can easily guess usernames and they can guess passwords locally or remotely using either a manual or automated approach. Password guessing isn't always as difficult as you'd expect. Most networks aren't configured to require long and complex passwords, and an attacker needs to find only one weak password to gain access to a school network.

- Dictionary attack
  A hacker uses a program or script to try to login by cycling through combinations of common words. In contrast with a brute force attack, where a large proportion of key space is searched systematically, a dictionary attack tries only those possibilities which are most likely to succeed, typically derived from a list of words for example a dictionary (hence the phrase dictionary attack). Generally, dictionary attacks succeed because many people have a tendency to choose passwords which are short (7characters or fewer), such as single words found in dictionaries or simple, easily predicted variations on words, such as changing a digit at the end.

Even common desktop computers are capable of running several billion passwords per second.

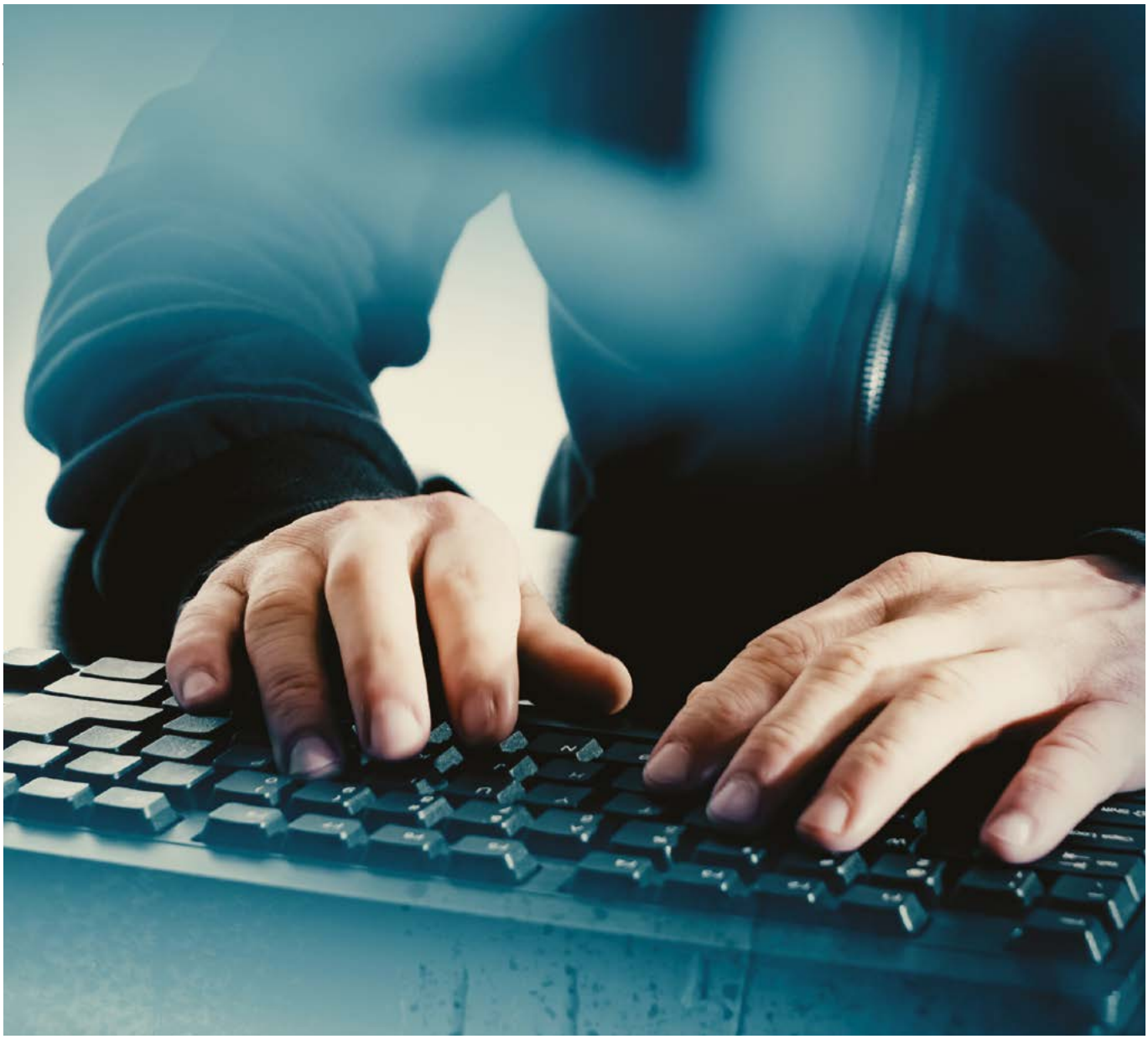
8. CBI Cyber Security: business Insight Conference 12 September 2018
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/cbi-cyber-security-business-insight-conference/

- Key logger attack

  Many attackers capture passwords simply by installing a keyboard-sniffing Trojan horse or one of the many physical keyboard-logging hardware devices for sale on the Internet. Symantec reports that **82%** of the most commonly used malware programs steal confidential information.[10] Most steal passwords. For £50, anyone can buy a keyboard keystroke logger that can log more than 2million keystrokes. Physical keyboard logging devices less than an inch long can easily be slipped between the keyboard cord and the computer's keyboard port. It's even possible to sniff passwords from wireless keyboards even from outside the boundary of the school.

There have been examples in education establishments in both the UK and US of students using key loggers to access the school network to change test scores.

10. Symantec Internet Security Threat Report, Vol 23. March 2018 https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf



Ecclesiastical's 2017 Education Annual Tracking Study

Phishing and password attacks appear in the top five incidents reported by schools, indicating human error remains a key vulnerability.

Notes

Notes

More than just insurance

With over 55 years spent securing the future of educational establishments, our education product and specialist service is tailored to give you peace of mind.

- A tailored insurance product that provides protection for staff, pupils, buildings, contents and business interruption.
- Access to helplines to support with PR and crisis management, legal advice and counselling.
- A bespoke risk management assessment, followed up with a risk tracker report, providing a before and after picture of risk improvements. Plus a unique view of where you sit in relation to your education establishment peer group.
- Access to our risk advice line providing quality support over the phone, helping you to manage your changing risks.
- Support from an award winning claims team[1] should the worst happen.
- Online advice via our "Education Hub". Here you will find useful information ranging from staff training and health and safety advice, to easy to use forms and templates and market insights.
- A 25% discount for EduCare, a leading provider of online duty of care and safeguarding training[2].

Visit **www.ecclesiastical.com** for further information on education insurance from Ecclesiastical.

[1] Winner at the Insurance Times Claims Excellence Awards and the Post Claims awards 2018.

[2] To claim the 25% discount you must have an active education policy with Ecclesiastical Insurance Office plc on the date of purchase. This discount cannot be used in conjunction with any other offer.

ecclesiastical

Ecclesiastical Insurance Office plc (EIO) Reg. No. 24869. Registered in England at Benefact House, 2000 Pioneer Avenue, Gloucester Business Park, Brockworth, Gloucester, GL3 4AW, United Kingdom. EIO is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Firm Reference Number 113848.

PD3174 1 03/21