Cybersecurity Awareness

In this section we look at areas including malware, phishing, ransomware, as well as other key areas that need to be considered by schools.

Cybersecurity, Awareness and Reflection

A major cyberattack on your school would likely be the single most disruptive event in your school year. It would seriously impact all digital technology related and online school activities for all staff and students/pupils, including teaching, learning, assessment and administration activities. Following such an attack, the time, effort and resources required for the school to recover from such an attack would be directly proportional to the level of cybersecurity 'readiness' that the school had in place before the attack took place. The 'recovery time' for the school could be days, weeks, months or longer. The purpose of implementing proactive cybersecurity is to minimise the impact of cyberattacks on your school and school community.

What do we mean by Cybersecurity?

Having a cybersecurity policy and associated processes in place will empower schools to protect their digital and online systems from harmful cyberattacks. These attacks can severely damage a schools ability to function. A proactive cybersecurity policy therefore needs to be a high priority for schools who need to first understand the risks, and then put in place a robust policy to protect against these risks.

Schools are highly reliant on digital and online systems, as they manage large amounts of critical data, including personal data on staff and students/pupils. The shift to using digital and online learning has significantly increased the risk, as schools increasingly rely on a range of digital and online tools. As a result, schools have become more 'attractive' targets for cybercriminals.

Facts on Cybercrime

Cybercrime is a very profitable business, generating approx' $9.5 trillion in 2024, and growing yearly.

- If measured as the GDP of a country cybercrime would be the 3rd largest economy in the world after the USA and China.
- Cyber criminals who carry out the attacks are highly skilled professionals who use the latest techniques and technologies, including Artificial Intelligence (AI) and automation to attack organisations including schools.

Reasons for growing number of cyberattacks on schools:

- Data relating to individuals is valuable and is bought and sold for profit by cybercriminals as a commodity on the 'dark web'.
- Schools don't see themselves as profitable and attractive targets, however research clearly shows that cyberattacks on schools are rapidly increasing.
- It's no longer a matter of 'if' a school will be attacked, it's just a matter of 'when' and 'how'.
- Schools have significant quantities of 'potentially profitable' data on staff and students/pupils.
- Many users have the same or similar login details to access different school and non-school services. In such cases if an attacker gains access to just one user personal or school account they could then easily gain access to other accounts of that user.
- While cyberattacks are generally perceived as being from external parties, they can also be initiated by an internal school staff member or student/pupil.

- Schools generally lack the necessary expertise and resources to implement effective cybersecurity measures, leaving them exposed to increasingly sophisticated attacks from cybercriminals.

Cyberattacks often use a combination of malware and phishing. While malware is the actual software that has been designed to damage users or systems, phishing is often 'how' the malware is delivered to the victims computer systems.

Malware:
Malware is a general term for '**mal**icious soft**ware**', including software that is designed to damage, disrupt, or gain unauthorised access to a computer system or network. Malware includes viruses, worms, trojans, ransomware, spyware, and other harmful software. Malware can be used, without the knowledge or consent of a user, to take control of devices, steal sensitive information, cause data loss, or in the case of ransomware it can disable systems and demand a ransom to be paid. It can spread by various means, such as email attachments, infected websites, and malicious downloads.

4 ways in which malware can infiltrate a school

1. **On infected USB sticks**: Malware can be introduced into a school network by plugging a malware infected USB stick into a computer used in the school.
2. **Phishing Scams**: Attackers use a combination of deceptive emails or websites to deceive staff or students/pupils into revealing their login details.
3. **Ransomware Attack**: Cybercriminals can use downloaded malware to encrypt school files, disable systems and demand that a ransom be paid.
4. **Data Breach**: Following a data breach involving a login details, attackers could have unauthorised access to school data or systems, with damaging consequences.

Phishing:
Phishing is a type of cyberattack where an attacker tries to deceive individuals into unknowingly revealing sensitive information, such as usernames, passwords, or credit card details. Phishing uses a technique referred to as 'social engineering'. This is typically carried out using deceptive emails, messages, or websites that look trustworthy, but are actually infected with malware and designed to steal users data. Phishing could have serious consequences for a school, both in terms of data loss and reputational damage.

Example of Phishing
Imagine a phishing email sent to school staff, disguised as a message from the schools IT technical support company. The email requests recipients to click on a link and log onto a seemingly trustworthy website to 'update their account'. If a user enters their login details, the attacker could gain access to personal or school data. The attacker could then use this data for 'identity theft' or to launch further attacks, such as ransomware, which could lock school systems and demand a ransom payment for their release.

3 key points on Social Engineering and Phishing:

- **Deceptive Communication**: Phishing often relies on creating a sense of urgency through deceptive emails, phone calls, or messages that appear to come from 'trustworthy' sources, such as the school bank, or the school delivery company.

- **Exploiting Human Behaviour**: Attackers often use a combination of human psychology and social engineering techniques, such as curiosity, and gaining false trust, to deceive victims into taking actions without being cognisant of the consequences.

- **Infected Websites and Links**: Phishing often involves directing victims to infected websites using malicious links, from where they can then install malware or steal login details.

2 examples of phishing attacks on schools:

- **Email from software provider**: Cybercriminals could impersonate a schools software supplier, sending an email claiming the recipient's account has been compromised and that their password needs to be updated. The email contains a link to an infected login page, designed to steal login details.

- **Urgent email regarding licence expiry**: An attacker sends an email pretending to be from a well known company such as Microsoft or Google, informing the school that school licences for their product need to be updated to prevent expiry. Again the email directs recipients to a fraudulent website login page, designed to steal login details.

Schools Leadership Teams are encouraged to review other resources and supports in this section including the section on 'Assess Your School Cybersecurity Readiness'

If the School Cybersecurity team have any related questions on this area they can email Oide Technology in Education at ictadvice@oide.ie