NCSC

NATIONAL CYBER SECURITY CENTRE

Quick Guide: Cyber Security for Schools

Background

Schools are now significantly more reliant on information technology systems to function. They also may manage large amounts of sensitive personal data, including data on staff, students/pupils, and parents. As a result, they have become potential targets for cyber criminals. A cyber-attack on a school can negatively impact its ability to function, its reputation and its legal obligations to keep sensitive personal data secure and confidential.

Good cyber security helps to protect schools from harmful cyber-attacks which can severely damage the ability of a school to function. It also helps to prevent unauthorised access to large amounts of sensitive personal data that is stored on a school's IT systems.

Cyber security must therefore be an important priority for schools with a reliance on information technology and online systems. School boards and their governing body should be aware of the cyber risks to their schools and the measures to consider to mitigate against these risks.

This quick guide has been produced by the NCSC to assist primary, post primary and special schools in particular to implement the key priority measures that can help to reduce the likelihood of a school becoming a victim of a cyber-attack or to reduce its impact.

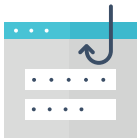
Who Might Want to Target Schools?

Online Criminals

Online criminals may attempt to steal and sell important sensitive personal data, or they could carry out a ransomware attack, encrypting files and preventing access to systems so they can hold a school to ransom.

Hackers

There may be individuals, for reasons beside financial motivation who wish to access a school's IT systems so that they can cause disruption or reputational damage to schools.



Human Errors

Staff and pupils who are using the devices and online systems may make mistakes or fall victim to phishing e-mail campaigns which allow sensitive information or credentials to fall into the wrong hands and possibly be exploited.

Malicious Insiders

Disgruntled staff or unhappy students/pupils may use their access to a school's IT systems to carry out malicious activity to cause disruption or reputational damage.

Untargeted Cyber Attack

These types of attacks don't care who the victim is and indiscriminately target as many devices, services, or users as possible. They do this using techniques such as phishing, water holing and port scanning. If a school has a low level of protection in place then these types of attacks could negatively affect the schools ability to function and store sensitive information securely.

Impact of Cyber Attacks

Encryption

The attacker will push out their encryption to as many devices as possible. The attacker will also focus on encrypting backups they can access in order to prevent recovery. The attacker will demand a ransom payment in return for a decryption key.

Data Theft

Before encrypting the system, the attacker will likely have stolen sensitive and personal data, in order to conduct 'double extortion' whereby they will demand a further ransom payment to prevent the data being leaked or sold.

Defacement

Hacking of school websites or social media accounts to deface them or publish damaging disinformation to cause reputational damage.

Guidance to Improve Cyber Security and Reduce the Risk of a Cyber Incident

Network Security

If not in place already, use a firewalled connection to prevent unauthorised access and malicious content to your networks. Monitor and test firewall controls so they are operating effectively.

User Awareness

Produce user security policies detailing the correct and secure use of devices and online systems. Include staff and pupils on regular up to date cyber security awareness training.

Malware Prevention

Produce appropriate policies on malware and install anti-virus protection on the school's devices, online systems, and IT infrastructure. Disable USB ports unless strictly necessary.

Account Security

Manage and limit user privileges as well as monitoring user activity. Create a password policy. Cultivate a habit of **strong and unique passwords** for accounts and services. Use a password manager to store passwords. Enable **multi-factor authentication (MFA)** on all accounts if possible.

Backups

Create backups regularly and consider a cloud solution to store these. Create a policy to control all access to removeable media, limit media types and scan media before importing onto the network. Apply patches and software updates regularly.

Prepare

Make an incident plan and involve staff. Carry out a test exercise to test preparedness. Document contact details of external people who can help during an incident. Monitor systems and network for unusual activity.

Reporting

If you experience a cybersecurity incident it should be reported to your local Garda station. You may also report incidents to the NCSC at certreport@decc.gov.ie

Further Information

To assist schools in developing approaches and policies in this area, further guidance on cyber security best practice and ransomware is available at the following resource:

NCSC Guidance

Glossary

Credentials - A user's authentication information used to verify identity - typically one, or more, of password, token, certificate.

Decryption - Decryption is taking encoded or encrypted text or other data and converting it back into text you or the computer can read and understand

Encryption - A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it.

Firewall - Hardware or software which uses a defined rule set to constrain network traffic to prevent unauthorised access to or from a network.

Multi-factor authentication - The use of two different components to verify a user's claimed identity.

Patching - Applying updates to firmware or software to improve security and/or enhance functionality.

Phishing - Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

Port scanning - A port scan is a common technique hackers use to discover open doors or weak points in a network.

Ransomware - Malicious software that makes data or systems unusable until the victim makes a payment.

Water-holing - Setting up a fake website (or compromising a real one) in order to exploit visiting users