Department for Education

Why we are contacting you?

The Department for Education and the National Cyber Security Centre (NCSC) has been made aware of an increasing number of cyber-attacks involving ransomware infection affecting the education sector at this time. The purpose of this letter is to make you aware of the threat and provide high-level information and advice to support your ongoing cyber security preparedness and mitigation work.

In all cases the NCSC has been working with the department and the affected providers to contain and support post-incident outcomes. However, these attacks and incidents have had a significant impact on the affected education provider's ability to operate effectively and deliver services.

These incidents appear to be financially driven but opportunistic, taking advantage of system weaknesses such as unpatched software, poor authentication systems or the susceptibility of users to misdirection.

Whilst I would urge you to ensure that your systems, processes and awareness training are up to date, I also want to make you aware of the steps you should take if your educational setting is affected.

What should I do if I am affected?

Please action the following:

1. Enact your incident management plan
2. Contact the NCSC, via https://report.ncsc.gov.uk
3. Contact your local law enforcement and Action Fraud,via https://www.actionfraud.police.uk/

4. Inform the Department for Education at this address: sector.securityenquiries@education.gov.uk

What do I need to do now?

It is vital that all education providers urgently review their existing defences and take the necessary steps to protect their networks from cyber-attacks.

Along with your defences, having the ability to restore the systems and recover data from backups is vital. You should ask your IT team or provider to confirm that:

- They are backing up the right data
- The backups are held offline
- They have tested that they can restore services and recover data from the backups

What do you need to do next?

The Department for Education would like to signpost guidance in developing defences as well as a number of free offers that the NCSC provide which can help notify you of possible malicious activity on your networks. These have been listed in the annex attached.

We will continue to monitor these situations and will revert with further information if there are further developments.

Yours sincerely,

Department for Education

ANNEX A – Ransomware

What is ransomware?

Ransomware is a type of malicious software (malware) that prevents you from accessing your computer (or the data that is stored on it). The system itself may become locked, or the data on it might be stolen, deleted or encrypted. Some ransomware will also try to spread to other machines on the network, such as the Wannacry malware that impacted the NHS in May 2017.

Normally you're asked to make a payment (often demanded in a cryptocurrency such as Bitcoin) in order to unlock your computer (or to access your data). However, even if you pay the ransom, there is no guarantee that you will get access to your computer, or your files. Occasionally malware is presented as ransomware, but after the ransom is paid the files are not decrypted. This is known as wiper malware. For these reasons, it's essential that you always have a recent offline backup of your most important files and data.

How does it impact education providers?

Ransomware is often used by criminals in a way that doesn't initially target specific organisations. Once the malicious software is on a network, the criminals can monitor and control the encryption of data. Their aim is to encrypt data that will have the most impact on the organisation's services. This can affect not just the organisation's computer networks but also services it operates, including telephony and websites. The data held by these services is also at significant risk, including personal information (student and staff details), financial transactions (staff salaries, payment of ESFA funds, ability to pay suppliers), details on vulnerable people (adult social care), and college and school data (admissions, at risk children).

Depending on the comprehensiveness of disaster / business continuity plans in place, normal service can take weeks, if not months to resume. In some cases, data will never be recovered.

Some ransomware groups have started to steal data from their victim organisation's networks before encrypting what is left. This means that even if the victim can recover from backups the criminals may try to extort money in exchange for not revealing the data online.

Should we pay ransomware?

The Department supports the National Crime Agency (NCA) recommendations. The NCA does not encourage, endorse, or condone the payment of ransom demands.

Payment of ransoms has no guarantee of restoring access or services and will likely result in repeat incidents to educational settings.

ANNEX B – Being prepared

Cover the basics

1. Have an incident plan and test it
2. Make sure your data is backed up offline and test the recovery of it
3. Regularly review your defences and controls

NCSC material and support

1. Ransomware advice and guidance for your IT teams to implement, available here:

https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

2. How to effectively detect, respond to and resolve cyber incidents, available here: https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes/developing-your-plan
3. Sign up to the Cyber Security Information Sharing Partnership (CiSP); a safe and secure environment that allows the NCSC to share threat information, available here: https://www.ncsc.gov.uk/section/keep-up-to-date/cisp
4. Enrol in the NCSC Early Warning service that helps the NCSC to rapidly notify organisations that might be affected by malicious software, available here: https://earlywarning.service.ncsc.gov.uk/
5. Test your incident response with an “Exercise in a Box”, available here: https://www.ncsc.gov.uk/information/exercise-in-a-box
6. Finally a data backup strategy and guidance is also available here: https://www.ncsc.gov.uk/collection/small-business-guide/backing-your-data

Further information

1. Back to school audit by NCSC and London Grid for Learning, available here: https://www.ncsc.gov.uk/blog-post/cyber-security-going-back-to-school
2. Questions for school governors by NCSC and DfE, available here: https://www.ncsc.gov.uk/information/school-governor-questions
3. NCSC practical tips for everyone working in education, available here: https://www.ncsc.gov.uk/information/resources-for-schools

4. NCSC cyber security risk management guidance, available here: https://www.ncsc.gov.uk/collection/risk-management-collection