CYBER SECURITY

virtue TECHNOLOGIES

Understanding the DfE's Recent Cyber Security Advice

Department for Education

Benefit from our years of experience, with this free guide.

The Department for Education, in partnership with the National Cyber Security Centre (part of GCHQ) recently issued an important circular to schools to make them aware of the increased number of cyber security threats. The email you will have received focused on Ransomware as a key issue. It also highlighted a number of steps schools should consider to minimise the risk of an attack and the reduce the harm caused by one.

What Is A Ransomware Attack?

Ransomware is a focused cyber-attack that's designed to extort its victims by encrypting critical files and systems, and holding them to ransom. This style of attack has become extremely popular among cyber criminals, due to the opportunities for a high return on investment, and the relative ease at which Ransomware can be spread. In 2019, over 1,000 US schools were identified as Ransomware victims.

What Do Schools Need To Do Now?

The DfE have made some specific recommendations that your school should consider acting upon.

They recommend that schools:

- Have an incident management plan to deal with an attack
- Take all the necessary steps to secure their network
- Are backing up the right data
- Have backups held offline
- Have tested they can restore services and recover data from their backups

Based on DfE guidance, Virtue Technologies recommend that schools ensure these measures are in place to secure their network:

- Review your firewall rules. Ensure they're relevant and the school's not exposed in any way. Pay particular attention to your rules around the publishing of internal services to the internet.
- Ensure a leading end-point security solution is deployed on all computers that access your network (clients and servers), along with Anti-Ransomware technologies.
- Ensure that all your servers, desktops, laptops and other computing equipment are running on the latest operating systems, making sure they've got the latest security patches and updates installed.

Virtue Technologies Installed Services

For our customers that have the following services installed and maintained by us, we're able to provide some helpful reassurance:

- **Internet and Firewalls:** Our Internet services use Sophos SG/XG as firewalls. Our installations are secure and meet the requirements of all DfE guidelines (including PREVENT). Our engineers are all Sophos Accredited Engineers and are experts in configuring and maintaining firewalls in schools.
- **Remote Desktop Services:** There are many ways to install and configure remote access to a school's environment. For our customers who've got a Virtue installed service, we can reassure you that our installation is secure and does not have 'direct access' to your internal services. It uses a dedicated 'Session Host Server' to provide an extra level of security for you.

How We Can Offer Further Help

Firstly, collectively the team at Virtue Technologies have a wealth of experience working with schools to provide a secure and safe environment for teaching and learning. The DfE, with NCSC, have provided this valuable information to help you keep your school(s) secure. We fully support this step to maintain the safe and secure running of schools, especially at a time when the number of attacks has increased.

We're able to support customers with any and all of points raised by the DfE communication. Whether you'd like to get some reassurance about your current set-up or you need a more detailed investigation and/or recommendations, we're here to help.

To discuss your IT Security further, or any other aspect of your IT products and solutions, please contact your **Account Manger** directly or through our main office on 01695 731 233.