GDPR CYBER SECURITY

YOU CANNOT SAFEGUARD AGAINST EVERY POSSIBILITY BUT IT IS IMPORTANT TO BE VIGILANT AS SOME ATTACKS ARE PREVENTABLE. NETWORK USERS ARE NORMALLY YOUR BIGGEST THREAT. HERE ARE 16 TOP TIPS TO MINIMISE THE IMPACT OF CYBER SECURITY THREATS:

JUDICIUM EDUCATION

Call 020 7336 8403

1 THINK BEFORE YOU OPEN

Don't get hooked in by emails providing unexpected promises. If it seems too good to be true, it probably is. Viruses, malware and data fraud can all arise from opening contaminated links.

2 DON'T OPEN LINKS

Unless you can be 100% satisfied of the source. Consider whether it may be better to type the link out into your browser if you are unsure.

3 BEWARE OF URGENT EMAILS

Attackers target vulnerability usually with the threat of financial implications if you don't act. Don't forget the attacker wants you to think you have done wrong and act without thinking.

4 VERIFY

If you are not sure where an email has come from, take steps to verify their credentials before opening. Try googling the web address or calling the company.

5 INVESTIGATE

Phishing emails are getting more and more effective at finding ways to catch you out - but they can leave clues, such as bad spelling, new account details for payments and strangely titled attachments and links.

6 UPDATE

Patches and software updates should be installed immediately. People are finding new ways to test networks and so delaying an update can make your machine and the data you hold at risk.

7 PASSWORDS

Passwords should have a complexity requirement (a certain number of characters as well as a mixture of numbers, letters and special characters). Having a strong password makes it more difficult for an attacker to access.

8 AUTHENTICATION

Using two-factor authentication to log into accounts and sensitive areas can help validate individuals. This can also mean you are less likely to lose data due to phishing.

9 BACK UPS

Ensure back-ups are in place and that the time period between back-ups is short. There should also be procedures to recover data from back-ups in case of incident. If you are not sure check with your provider before an incident occurs.

10 CRISIS MANAGEMENT

Do you have plans should the worst-case scenario happen? How will you communicate incidents to staff and recover data? This will be a big task to manage so it's important to be prepared to act quickly.

11 ANTI-VIRUS

Ensure you have anti-virus programmes in place. Picking the right tool is important as it can help block attacks, stop attacks from spreading and help protect the system from infection.

12 APPROVED DEVICES

Avoid plugging in your own memory stick or hard drive onto the school network as these can be sources of risk. If you really need to use your own device, seek approval from your IT team.

13 APPROVED SOFTWARE

Only use software provided by your IT department. Never attempt to install software downloaded from the internet yourself.

14 ENCRYPTION

Protect devices you issue to staff and students. If laptops are taken off-site it is best that they are encrypted or ensure that users have to remotely log into servers so they don't save data directly onto devices.

15 SCREEN LOCK

Whenever you leave your computer, even for a short time, always apply the screen-lock.

16 SHUT DOWN

Always shut down your computer at the end of the day as it allows the system to install important updates.

ANY QUESTIONS IN THE MEANTIME DO EMAIL US AT DATASERVICES@JUDICIUM.COM OR CALL US AT 0203 326 9174.

0203 326 9174

DATASERVICES@JUDICIUM.COM

WWW.JUDICIUMEDUCATION.CO.UK