Londonwide LMCs
The professional voice of London general practice

Be safe! Take care of your cyber security

We know that the security of your practice IT systems is often out of your hands. However, we have put together some tips that may help you secure your systems following the ‘WannaCry’ attack on the NHS earlier this month.

Back up and update

Make sure you have effective backups of data on an external hard drive or cloud-based service and ensure all devices are regularly updated.

Beware of spam emails

Ransomware attacks usually rely on an end-user activating them, normally by opening an email attachment. Educate the practice team and ensure that they question who or where emails come from on a regular basis. Ensure this is covered in any staff inductions.

Make sure the team regularly change their passwords and using a mixture of upper and lower case letters, numbers and symbols.The National Cyber Security Centre has produced some helpful guidance on dealing with a ransomware attack.

Have a disaster recovery plan

You should have a disaster recovery plan in place which outlines what the team should do in the event of an attack. Also, ensure that cybersecurity is discussed at every practice team meeting. The plan should include details on how to disconnect infected devices from the network as well as how the practice may work whilst systems are restored.

Read the RCGP’s ‘advice for GP practices following cyber-attacks on their systems’ for further information.

Plan a response

Advice from Practice Index states:

“In the absence of IT specialists – which is the case for most practices – it’s up to ‘leaders’, which will usually be a practice manager, to determine an effective cause of action in the event of an attack, and educate staff to prepare for them.”What this means in essence is that the practice should have a strong cyber security response plan with clear definitions of how data can be recovered as well as roles and responsibilities within the practice team. Read the UK government’s 10 steps to cybersecurity for further advice.

Unfortunately, cybercrime is a fact of life today and it’s only a matter time before the next attack takes place.

These tips will hopefully help you to take a few simple steps towards making cybersecurity part of your practice culture so you can minimise the chances of any future attacks and the damage they may cause.