Royal College of General Practitioners

Advice for GP practices following 'cyber attack' on IT systems

Immediate steps that you may wish to take:

- Print out appointment systems records for the next week
- Print out Encounter records (paper forms – template attached) for use during potential further computer system failures
- Put up notices in the practice entrance informing patients - a template is provided for you to customise
- Check with your Clinical Commissioning Group (CCG) for regular updates
- Ensure all staff receive up-to-date communication, including regular bulletins on staff noticeboards and individual workstations
- Avoid opening any attachments in emails and social media
- Stop any use of USB sticks to load software
- If possible, ensure regular backups of everything

What to do if a computer is infected:

- Disconnect the computer from the network immediately
- Turn off any practice Wi-Fi
- Contact the relevant member of practice staff and seek immediate technical support from your CCG IT supplier

When and where possible, you may also want to:

- Check with your CCG and Commissioning Support Unit for latest advice on 'patching' and software updating
- Ensure anti-virus software is up to date on the server and all individual computers
- Meet to review the practice IT contingency plan
- Establish a task group to establish roles and responsibilities to manage control, conflict, communication, cohesion and consensus
- Ensure all staff are aware of the practice IT policy and contingency plan and that all new staff receive an IT induction
- Talk to your neighbouring practices about their experience and how they are managing /have managed the situation