Faq Sheet

Cyber Security/Malware

Between September 2016 - December 2017, has your university been targeted via a cyber-attack?	Yes. They were: Phishing attacks Spear phishing attacks Ransomware attacks SQL injection attacks Rootkit attacks
The number of cyber- attacks the university encountered during this time	Greater than 200 attacks
The number of phishing attacks the university encountered during this time	Greater than 400 attacks
Victims most affected from the attacks	Students Lecturers We do not have accurate data to enable us to quantify this
The number of targeted spear phishing attacks the university has encountered	50-75 attacks
The number of ransomware attacks the university has encountered between Sept 2016 – Dec 2017	Under 25 attacks
Time taken to resolve a ransomware attack	Between 1-2 days
The number of SQL injection attacks encountered	Under 100 attacks
The number of rootkit attacks encountered	Under 5 attacks
Content blocked or filtered	Security or Malware The university do not moderate content by type
Statistics relating to the requests blocked or filtered	We do not keep precise statistics or categorise, but block on average 20 links per day.
Monitoring requirements we have for ours users	We maintain network and system logs, which track system, rather than user activity. This can be used to identify specific user activity where required under policy or law.
Sources for penetration testing	Internal Resource
Currently document security or digital rights management tool	Documentum
Prevent action plan or any document that outlines your institution's Prevent policy in line with your obligations under the Counter Terrorism and Security Act 2015	We do not have a Prevent action plan or document that exactly covers this