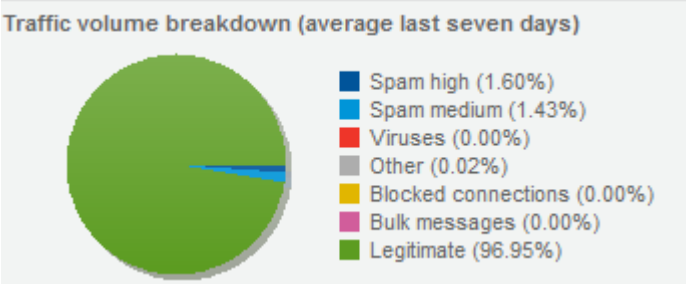
NHS Bolton NHS Foundation Trust

2018-412 - FOI Request - IT Security

Q. What percentage of emails that your organisation receives are fraudulent – i.e. phishing messages, BEC (business email compromise) attacks, CEO Fraud, malware laden, etc.	
• Please indicate as a percentage	This does not specify the time period to be looking at this over. We have layered security and this doesn't distinguish between emails and general traffic at the first layer for reporting purposes. Or emails specifically see below. 
• Don't Track	
Q. What is the most common type of fraudulent email/cyber-attack that your organisation receives?	
• CEO fraud – this is when someone sends an email impersonating a senior company executive asking an employee to make payments for goods or services into a fraudulent bank account • Fraudulent transaction requests – fraudsters send invoices for payment of goods or services as if from a legitimate organisation • Credential theft – fraudsters send messages trying to get users to divulge their username and password or other sensitive information • Ransomware • Other • Don't Track	Our reporting would not break down to these questions.
Q. Has your organisation suffered financial loss in the last 12 months as a direct result of a faked email message being received that tricked an employee into sending money via wire transfer	
● Yes ● No If yes, please state how much was lost (if fallen victim more than once, please provide total amount given to scammers):	No
Q. Has your organisation had a device/system infected by	

ransomware in the last 12 months that was delivered via email:	
• Yes – once • Yes – more than once • We were infected by ransomware but the source wasn't traced • Never NB: If you have answered yes, please answer the following questions for each separate ransomware infection (if numerous devices were infected at the same time, this counts as one incident)	No
How long were systems affected:_____ Did you pay the ransom: • Yes • No If yes, how much was paid:_____ Did the criminals provide the information/program needed to restore systems: • Yes • No	N/A
Q. Do you use the domain-based message authentication, reporting and conformance protocol (DMARC) to block fake emails being spoofed to appear as if they have been sent by your company/organisation:	
• Yes • No • Don't know	Yes
Q. Are you aware if your organisation/brand has ever been 'spoofed' and used by scammers to send emails trying to trick people	
• Yes – before we started using DMARC • Yes – after we started using DMARC • Yes – but not sure if it was before or after using DMARC • Never • Don't Track If yes, please state how many separate incidents of your organisation/brand being spoofed that you know of: before we started using DMARC:_____ after we started using DMARC: _____	Yes, but none successful
Q. Do you publicise externally how a member of the public can check an email communication with your organisation to determine if	

it is fake?	
● Yes ● No If yes, how many reports have you received in the last 6 months of fake/phishing messages: ● _____ ● Don't Track	No
Q. Do you publicise internally how a member of your workforce (including third party suppliers) can check an email communication with your IT/Security team to determine if it is fake?	
● Yes ● No If yes, how many reports have you received in the last 6 months of fake/phishing messages: ●_____ from internal workforce ●_____ from third party suppliers ●_____ from both internal and third party suppliers as don't differentiate between senders ● Don't Track	Yes Our service desk does not provide the requested breakdown.
Q. Do you provide a report button within your email system for end users to report phishing emails?	
● Yes ● No	Users contact the service desk and can forward SPAM emails to a mailbox which will improve our rule base.
Q. Does your organisation have a SOC (Security Operations Centre) or IT security team? ● Yes ● No	Yes
Q. Do you have a secure email gateway? ● Yes ● No ● Don't know	Yes