Freedom of Information Request

Reference Number: Ref EPUT.FOI.18.652
Date Received: Date 12.07.2018

*Note to Applicant: As of 1 April 2017, North Essex Partnership University NHS Foundation Trust (NEP) and South Essex Partnership University NHS Foundation Trust (SEPT) merged to form one new organisation known as Essex Partnership University NHS Foundation Trust (EPUT).

Information Requested:

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: ________________ %

**EPUT does not track this information this is the responsibility of NHS Mail.**

**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

**EPUT does not track this information this is the responsibility of NHS Mail.**

**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): ____________________

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)

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

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

EPUT does not track this information this is the responsibility of NHS Mail.
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

EPUT does not track this information this is the responsibility of NHS Mail.

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: _______________

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

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

• 30 from both internal and third party suppliers as don’t differentiate between senders

Q. Do you provide a report button within your email system for end users to report phishing emails?

• Yes

• No

Q. Does your organisation have a SOC (Security Operations Centre) or IT security team?

• Yes

• No

Q. Do you have a secure email gateway?

• Yes

• No – NHS Mail is Responsible for this.

• Don’t know