Liverpool Heart and Chest Hospital NHS
NHS Foundation Trust

Reference Number: FOI/2019/006
From: Private Individual

Date: 07 January 2019

Subject: Social Engineering

Q1 Does the organisation have training that covers:
1. Recognising and reporting Phishing emails
2. Recognising Tailgating and how to respond (challenging strangers, checking for ID etc)
3. Disposal of confidential information
4. Dangers of using USB sticks being given away or finding one that looks like it has been dropped

A1 Yes
1. Covered in corporate induction and via mandatory training
2. Regular staff awareness communications about tailgating and the importance of challenging individuals who do not wear name badges are issued
3. Regular staff awareness communications are issued about record retention and destruction
4. Covered in corporate induction and via mandatory training, supported by regular staff awareness communications

Q2 Does the organisation allow the use of USB sticks?

A2 Yes – however, only Trust-approved encrypted USB sticks

Q3 Does the organisation deliver specialised training to key staff (those staff that could be targeted as part of a phishing email campaign, i.e. finance, execs etc.)?

A3 No – training covers all staff

Q4 Does the organisation perform confidentiality audits as per the Data Security & Protection Toolkit?
Can you also answer relating to the audits:
1. Where the audits are undertaken would these be organised with the local team manager or the head of department i.e. the director etc.?
2. Would an audit ever be carried out unannounced?
3. Do you have a policy / procedure of how to conduct the audit? – if so can you supply a copy.
4. Do you record the results on a checklist / report and return the key contact? – if so can you supply a blank copy.

A4 Information not held – no audits have been carried out yet, audits form part of this year's work plan

Q5 Does the organisation have confidential waste receptacles placed through the entire organisation and are they regularly emptied?

A5 Yes

Q6 Does the organisations Exec board receive board level training relating to Cyber Awareness?

A6 Yes

Q7 How does the organisation provide Data Security & Protection Training to staff, does the organisation use (please select all the options that are applicable):

a. Third party application package ☐
b. Third party Trainer / class room ☐
c. eLearning for Health Data Security Awareness ☐
d. In house developed package ☐
e. Combination of any of the above ☐

A7 c. e-learning - Data Security Awareness Level 1 developed by NHS Digital and Health Education England