Focus Group Topic Guide

Welcome
- Introduction of research
- Information sheet, consent forms to be signed and demographics form to be completed

Start timer and recording device

Topic 1: Groups technology capability/frequency of use
- Where do you use technology, at work / at home?
- How people engage with information technology, and whether they use it at work
  - E.g. phone, laptop, desktop, Alexa, smart meters, internet connections on door locks, fit bits - do they have connected devices
- Where they use technology at work, in their studies or home, or all of these

Topic 2: Behaviours
Ask about behaviours
- 'Next I am going to ask you about your own security behaviours'
- 'Your knowledge is as valuable as mine / you're the experts' – build up the confidence
  - Email behaviour
    - 'Does security come in to the way you think about email?'
    - 'What security measures do you take?'
    - 'Do you find you get emails that would be considered phishing?'
    - 'What do you do when/of you get phishing emails?'
  - Password behaviour – strong passwords, different for different sites
    - 'How do you construct your passwords?'
    - 'how do you come up with them?'
    - 'how safe do you think these passwords are?'
    - 'Have you heard of two-factor authentication? And can someone tell us what it is?'
    - 'Does anyone share passwords with family members or partners?'
    - Where is password and log-in information stored
  - Software – do they have security software on laptops / do they download the latest versions – at home and work (based on whether the group use technology at work) – 'do you always update your devices to the latest versions?'
  - Social media behaviour
  - Do they use secure Wifi

Topic 3: Threats
- How to they conceptualise the world of information security threat?
- Ask participants to brainstorm what threats they believe to be out there
- 'I want to spend 5-10 mins asking you to think all of the different information security threats relevant to people in the home and work environment'
- Or… with the previous devices mentioned, what do you see as the top threats?
  - If none are mentioned can prompt (depending on industries):
    - Ransomware
    - Phishing

- ▪ Viruses and worms
- ▪ Social engineering
- ▪ Unpatched vulnerabilities
- ▪ DDoS
- Are these threats relevant for yourself, or your employer?

Fear Based Questions
- Are these threats frightening? (see if any evidence of denial or other fear control processes)
  - o Or which ones (if any) are the most 'frightening'? Or 'what do 'you think others might find frightening
  - o Why?
  - o If so… how is this fear dealt with?
    - ▪ With frightening threats, do you know what to do to reduce them? – for example if a threat is phishing, do you take care to look for phishing signs when looking at emails
    - ▪ Is it ignored? Is the threat too hard to deal with?
    - ▪ Or third person approach: 'some people have told us that they don't bother with security software because they think if they're going to get hacked they're going to get hacked'
    - ▪ Is it not worrying? -
- And… are there any personal/real examples of threats/incidents. If so…
  - o Ask about personal reaction to incident
  - o Any response from organisation?
  - o Would this experience make you more likely to try and avoid such an incident in the future?
  - o What would others in the group do if that incident happened to them?
- Who is responsible when such incidents happen?
  - o The organisation or the individual

Does this fear/threat, or anything else, motivate you to take precautions?

Enquire about self-efficacy
- Do they know how to protect themselves from the threat, and do they feel they can do this? Or how others can?
- Do they feel they benefit from staying safe?
- Why so/why not?

Topic 4: Sources of information
- Do they feel their workplace provides them with information on how to be safe? / Do they know where to look for personal information security safety information?
- Are they ever used as a source of information for others?
- Do they think of anyone / any organisation as an authority? – 'if you wanted to find out any information about cyber threats and how to deal with them, where would you turn?'
  - o Family members
  - o Have they heard of the NCSC?
- Normative influences

  o Do friends/ family / work colleagues / influence information security behaviours or decisions – 'do you think work colleagues influence each other's security behaviours'?

Enquire about response efficacy
- Do they feel the information, or strategies given to them (by any of the sources of information) are capable of reducing the threats mentions?
- Is this related to confidence with technology?

Topic 5: information security communications – this is the materials section
- Show posters two at a time
- Then bring all posters back out to start discussion
  - o Do you think this is targeted and relevant to people like you?
  - o Do any catch your eye?
  - o Would any of the posters change the way you see or do things?
  - o If they don't feel engaged – what would work? What would connect to them and work for them?
  - o Are some more persuasive than others?
  - o How else could these threats be communicated effectively?
  - o Any other mediums that would be useful?

Concluding remarks
- Summarise discussion
- Is there anything important relevant to this that has not been mentioned?
- Summarise my own interpretation of the discussion and check this – if there has been any ambiguity
- Hand out debrief forms