

## Assessment Blueprint

### Cyber Security for Home based workers

Date: 05 May 2022

#### General information

|                                     |  |
|-------------------------------------|--|
| Purpose of assessment               | To measure whether the employee has a grasp on critical cyber security issues for safety when working at home.   |
| Level of skill                      | Basic, some computer literacy is assumed but only a modicum of security knowledge  |
| Target audience                     | Employees who work at home for an organization who is concerned about the security of their data.<br><br>The test is technology neutral.   |
| Topic coverage                      | There are 25 questions on the test, see below for the areas covered.   |
| What does it mean to pass the test? | The participant has demonstrated understanding of good cyber security practices when working at home.<br><br>Feedback on questions that the participant got wrong is given to help improve knowledge.            |
| What does it mean to fail the test? | The participant has gaps or weaknesses in their knowledge of good cyber security practices when working at home.<br><br>Feedback on questions that the participant got wrong is given to help improve knowledge. |

|                                 |  |
|---------------------------------|--|
| Language                        | Test is presented in US written English.<br><br>Participants can be native English speakers or should have at least B2 level of English if not a native speaker.   |
| Blooms taxonomy cognitive level | Our target is that at least half of the questions are comprehension/application or higher.   |
| Format                          | Online test presented in Questionmark software, automatically scored   |
| Accessibility                   | No use of graphics/images/media.   |
| Time limit                      | 45 minutes<br>(Based on evidence from the pilot where over 95% of people took 45 minutes or less to answer the assessment)   |
| Number of questions             | Participant to be presented with 25 questions (with random selection from 40 to 50). This means that a second attempt can be scheduled with mostly different questions.  |
| Question types to be used       | Combination of multiple choice, multiple response  |
| Feedback                        | Participant to be given at end of test: <ul style="list-style-type: none"> <li>- Overall score</li> <li>- Helpful question level feedback for wrong answers, giving the correct answer</li> <li>- Link to a coaching report</li> </ul> |

### **Detailed coverage:**

#### **Browser security**

- Advantages of MFA
- Password security
- Use of HTTPS

#### **Looking after a device**

- Save/backup data to a corporate location
- Use of shared devices (individual logins etc)
- Encrypting device
- Enabling local firewalls
- Lock device when unattended



www.questionmark.com

#### **USA**

333 W 39th Street, Suite 1003,  
New York, New York 10018  
+1 (203) 425 2400  
(800) 863 3950

#### **UK**

New Kings Beam House, 22  
Upper Ground, South Bank,  
London, SE1 9PD  
+44 (0) 20 7263 7575  
0800 731 5895

#### **Germany**

Hopfenstr. 8,  
80335, Munich  
+49 (0) 89 220 61272

- Ensuring devices are up to date (patches, browsers, updates)
- Malware

### **Social engineering risks**

- Phishing and how to detect/avoid it
- Shoulder surfing
- Use of social media
- Safe browsing online (e.g. malicious adverts)
- Validating who you are dealing with

### **Connection to wifi networks**

- Safe setup and use of home wifi

### **Disposal**

- Secure disposal of documents
- Secure disposal of electronic media

### **Other**

- Using unknown removable media (USB stick)
- How to safely communicate passwords and other key codes
- Reporting possible security breaches

If you have any questions, please ask your Questionmark account manager or reach out to [content@questionmark.com](mailto:content@questionmark.com).

Copyright (c) Questionmark Computing Limited 2022. All rights reserved.