

## Assessment Blueprint – Cybersecurity for Home-based workers

Status: Final

Date: 4<sup>th</sup> June 2020

Approved by: Questionmark Legal Team and Assessment Experts

### General information

Purpose of assessment	To measure whether the employee has a grasp on critical cybersecurity 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.  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 cybersecurity practices when working at home.  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 cybersecurity practices when working at home.  Feedback on questions that the participant got wrong is given to help improve knowledge.

Language	<p>Test is presented in US written English.</p> <p>Participants can be native English speakers or should have at least B2 level of English if not a native speaker.</p>
Format	Online test presented in Questionmark software, automatically scored
Accessibility	No use of graphics/images/media.
Time limit	<p>45 minutes</p> <p>(Based on evidence from the pilot where over 95% of people took 45 minutes or less to answer the assessment)</p>
Number of questions	Participant to be presented with 25 questions (with random selection from 43). 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	<p>Participant to be given at end of test:</p> <ul style="list-style-type: none"> <li>- Overall score</li> <li>- Helpful question level feedback for wrong answers, giving the correct answer</li> </ul>
Editing the test	We recommend that you consider using the test unchanged, as the questions have been validated and the pass score set using a defensible method. But if your organization needs to change questions or settings, you are permitted to do so. However, the test is copyright Questionmark Computing Limited, and you may not move the test outside of the platform provided by Questionmark.

### **Detailed topic 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  
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 Wi-Fi networks**

Safe setup and use of home Wi-Fi

### **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 2020. All rights reserved