1. Why Cybersecurity defense is important?
2. Everyone can be a target of cyber-attacks.
3. Cyber-attacks is a security risk to individuals & company.
4. Technology is part of the daily lives and key to business.
5. All of the above.
6. What is Malware?
7. Malicious Hardware.
8. Malicious Software.
9. Both A and B.
10. None of the above.
11. What is Ransomware?
12. Computer equipment that criminals steals from you and won’t return until you pay them.
13. A form of cryptocurrency.
14. Software that infects computer networks and mobile devices to hold your data hostage.
15. Software used to protect your computer or mobile devices from harmful virus.
16. Phishing is a type of online scam where attackers impersonate legitimate organizations via email, text message, and advertisement in order to steal sensitive information. Which of the following scenario is a phishing attempt?
17. You received monthly bank statement via email which shows spending of the month.
18. You received an email from Human Resources Department ask you to provide personal information right away.
19. You received a message stating reminder for your appointment at the hospital.
20. You received a phone call from a close friend asking “how are you?”
21. Which statement is true about Spear Phishing?
22. Spear Phishing targets specific individual within an organization.
23. Attacker does research on the individual online.
24. Purporting to be a trusted individual.
25. All of the above.
26. What is Email Phishing?

A) Uses phone call to trick individual.

1. Malicious emails that infect victim device with malware attachment or malicious link.
2. Uses SMS to trick individuals.
3. Targeting only working organization.
4. You get a text message from a vendor with a link attached asking you to renew your password via the link. You should:
5. Reply to the text message you have received to confirm that you have renew your password.
6. Click on the link to see if it redirect you to the vendor website.
7. Verify by calling the vendor using the number that is known to be correct.
8. Verify by calling the same number that send you the text message.

8. You received an email stating that it is from someone in your company and you have to reply them your email and email password to verify that you are a legitimate employee. What should you do?

1. Reply to the email with your information.
2. Verify by replying to the email.
3. Report it to the IT department and delete the email.
4. Click on the link if provided.
5. When browsing and surfing different websites, what should you look out for before entering your login information upon requested?
6. The Website Content.
7. The Website Design.
8. The Website URL.
9. The Website contact details.
10. Which one of the following scenario is not a cyber-threat?
11. You receive an email from a stranger informing that your computer has a virus.
12. You contact the number provided on the pop up.
13. You giving remote access to online stranger who you just met.
14. You inform the organization/ company IT department to check for any virus on your computer.
15. If you fall for a phishing scam, what should you do?
16. Delete the phishing email / message and alarm colleagues about the phishing email.
17. Inform higher authorities such as IT department.
18. Change any compromised passwords.
19. All of the above.
20. Which one of the following is the best practice when surfing online?
21. Use unique password for each account.
22. Avoid posting personal information online.
23. Verify with a reputable and trusted source (like Google) when in doubt.
24. All of the above.
25. You found a USB drive that is lying around near the coffee machine at the pantry, what should you do?
26. Plug in and check the USB drive.
27. Give the USB drive to someone else.
28. Report and give the USB Drive to IT department for them to dispose.​
29. Do not touch the USB drive.
30. How often should you change your password?
31. Every week.
32. Every single day.
33. Once a year or when password is compromised.
34. Not required to change.
35. When typing your new password, what should you observe?
36. People looking over your shoulder.
37. Password must not be written down anywhere.
38. Password must not be used before.
39. All of the above.
40. What is the basic of mobile device security?
41. Lock your phone with password and fingerprint.
42. Install 3rd party applications from unknown source.
43. Give out your OTP when requested.
44. Doing work related operations on free/public Wi-Fi.
45. If you fall for a phishing scam, what should you do to limit the damage?
46. Change any compromised passwords
47. Switch off the computer. This will get rid of any malware.
48. Reply the phishing email for help.
49. Ignore and do not do anything.
50. Which of these best describe on how cybercriminal start their attack?
51. Sending phishing email with links or attachment that put your data and network at risk.
52. Using infected websites known as pop-up phishing to download malicious software.
53. Gathering information through social engineering.
54. Sending customized message.
55. Cyber attacker/criminals only target large companies. True or False?

Answer is False

1. Which is the best answer for which people in a business organization should be responsible for cybersecurity?
2. Business owners. They run the business, so they need to know cybersecurity basics and put them in practice to reduce the risk of cyber-attacks.
3. IT Security department, because they are the best position to know about and promote cybersecurity within a business.
4. Managers, because they are responsible for making sure that staff members are following the right practices.
5. Every staff member should know some cybersecurity basics to reduce the risk of cyber-attacks.