**Cyber Awareness Training Final Test**

1. What is the recommended minimum length of a password?
   1. 12 characters
   2. 4 characters
   3. **8 characters**
   4. 10 characters
2. What is NOT a password best practice?
   1. Do not include personal information
   2. Do not use words from dictionary
   3. Should include uppercase, lowercase, numbers, and special characters
   4. **None of these**
3. Password managers are recommended to keep track of passwords
   1. **True**
   2. False
4. What is the purpose of a phishing attack?
   1. **Steal sensitive information**
   2. Used to exploit a computer
   3. Show unwanted ads to users
   4. None of these
5. What is a phishing attack against a specific group of individuals?
   1. Targeted Phishing
   2. Whaling
   3. **Spear Phishing**
   4. None of these
6. How to prevent phishing attacks
   1. Be careful of attachments sent
   2. Be careful of links you click
   3. Look carefully at who sent the email
   4. **All of these**
7. What does removeable media include?
   1. CDs/DVDs
   2. External Hard drive
   3. USB Drives
   4. **All of these**
8. What attacks can be orchestrated with removeable media?
   1. **Ransomware**
   2. Phishing
   3. Buffer Overflow
   4. All of these
9. What should you do when you find a USB?
   1. Plug it in
   2. **Do not plug in/Report to IT**
   3. Leave it
   4. None of these
10. What is NOT a common scam?
    1. Someone calling pretending to be the IRS
    2. Someone pretending to be Tech Support
    3. **Your bank calling to verify a purchase**
    4. None of these
11. What is a way to protect yourself from scams?
    1. Give out your personal information to anyone
    2. Click on every link sent to you
    3. Trust that emails come from who they say they come from
    4. **None of these**
12. It is not critical to maintain security on your mobile devices
    1. True
    2. **False**
13. What are the dangers of not protecting your mobile devices?
    1. Nothing
    2. Could steal personal information
    3. Could install malware
    4. **Both B & C**
14. What is NOT a way to protect your mobile devices?
    1. **Do not install updates**
    2. Install updates when they come out
    3. Use a passcode
    4. Keep personal information secure
15. What is physical security NOT responsible for?
    1. The facilities
    2. The physical IT equipment
    3. **The software**
    4. All the above
16. What are physical measures that can be taken?
    1. Access Control
    2. Applying Principle of Least Privilege
    3. Using MFA
    4. **All the Above**
17. What is shoulder surfing?
    1. Sniffing network packets
    2. **Looking at someone’s screen to get information**
    3. To ask someone for sensitive information
    4. None of these
18. Shoulder surfing is dangerous as an attacker could steal sensitive information
    1. **True**
    2. False
19. How to protect yourself from shoulder surfing?
    1. There is nothing you can do
    2. Don’t use your computer in public
    3. Get a Privacy Screen
    4. Avoid using public Wifi
20. Social engineering is using technical means to trick people into giving sensitive information
    1. True
    2. **False**
21. What is NOT a danger of social engineering?
    1. Theft of personal information
    2. Stolen Passwords
    3. **Nothing**
    4. All of these
22. What is the best way to protect against social engineering?
    1. There is nothing you can do
    2. Awareness
    3. **Enable MFA**
    4. None of these