Quizzes for Cybersecurity Fundamentals

**Threats**

1. Which of the following examples of potential malicious actors in cyberspace (select all that apply):
2. **Nation State Actors**
3. **Organized Crime**
4. **Political and Ideological Actors**
5. **Business Stakeholders**
6. **Hackers**
7. Choose examples of what an adversary may try to do after gaining access to your network (select all that apply).
	1. **Run malicious code**
	2. **Blackmail you or your organization**
	3. **Steal data**
	4. **Manipulate, interrupt, or destroy your systems and data.**

**Cybersecurity Basics**

1. Please select the most secure password of the options below:
	1. M1PA$$w0rd
	2. **T4ble font Phone $hoe**
	3. william1980
	4. MinistryOfCommunication2021
2. A website you are trying to access is blocked by your organization. You should (select all that apply)
	1. Try to access it on your personal device
	2. **Contact your IT administrator to determine next steps**
	3. Disable your VPN and try to access it again
	4. Turn your computer off and on and try to access it again
3. Which of the following are security considerations while using public Wi-Fi (select all that apply):
	1. **Threat actors collecting data from your device**
	2. **Threat actors capturing your credentials**
	3. **Threat actors taking control of your accounts**
	4. **Threat actors learning where you live**

**Online Safety**

1. Which of the following are ways to ensure that you are transacting with your legitimate financial institution online (select all that apply).
	1. The URL has the name of the financial institution in it
	2. **The URL begins with “HTTPS”**
	3. The URL begins with “HTTP”
	4. The URL ends in “.com”
2. Threat actors cannot view my online posts if I do not accept them as a “friend” online and have my privacy settings set to the most restrictive setting in my social media accounts
	1. **True**
	2. False
3. I can tell that news comes from a legitimate source if: (select all that apply)
	1. It comes from a relative
	2. It has a lot of “likes”
	3. **I have verified its accuracy using reliable sources**
	4. It is on television

**Protecting Government Information**

1. Anti-virus software intercepts malware.
	1. **True**
	2. False
2. I can download any software I want to my work device.
	1. True
	2. **False**
3. What are important things to keep in mind with printers or other networked devices? (select all that apply)
	1. **It is okay to use removable devices if they are approved by my IT department**
	2. It is okay to leave documents on the printer for a while if I am comfortable with the people that I work with
	3. **I should periodically review all of the networked systems connected to my computer to make sure that they are all current and necessary**
	4. **If I notice a new device or one I do not recognize connected to our network I should report it to my IT department**

**Mobile Device Security**

1. Which of the following tasks are your responsibility when it comes to maintaining mobile devices? (Select all that apply)
	1. **Allowing your systems to patch and install updates**
	2. **Powering off/rebooting your devices at regular intervals**
	3. **Installing only applications for which there is a business need**
	4. Downloading files for colleagues on your devices
2. Which of the below are not examples of practicing good cyber hygiene with your business mobile device?
	1. **Making your passcode to unlock your phone 1111 or another repeated number**
	2. Setting a lock timer on your device, so that is locks after a certain amount of idle time passes
	3. Using multi-factor authentication
	4. **Letting your family members play with your phone and/or download online games**
3. When traveling with your mobile device, it is best practice to: (select all that apply)
	1. **Backup your device before traveling**
	2. Store your mobile device in your checked luggage
	3. **Disallow your device to auto-connect to networks**
	4. Lend it to a colleague to check their personal email during the trip