

1. What is one of things, mentioned in the training, that you should do when you found out that one of your online accounts was compromised? *

- ☒ Change your password
- ☐ Pretend like nothing happened
- ☐ Try logging in from a different browser
- ☐ Reboot your computer

2. According to the training, what can you do to avoid the consequences of phishing email? *

- ☐ Don't click links
- ☐ Don't click attachments
- ☐ Navigate to the site directly and independently
- ☒ All of the above

3. What is something you can do that is more secure than sending data over a shared WiFi connection, like those found at coffee shops? *

- ☐ Wait until you get home and use your personal WiFi
- ☐ Disconnect from public WiFi and use cellular service
- ☐ If you must use your laptop, set up a hot spot on your cell phone
- ☒ All of the above

4. Which Type Malware holds your data hostage until you pay to have it unencrypted? *

- ☐ Trojan Horse
- ☒ Ransomware
- ☐ Worm
- ☐ Rootkit

5. What is the best defense we can have against email/cyber attackers? *

- ☒ Awareness
- ☐ Gmail
- ☐ Antivirus