Cybersecurity Merit Badge Requirements

1. Safety. Do the following:

(a) View the Personal Safety Awareness 'Digital Safety' video (with your parent or guardian's permission).

(b) Explain to your counselor how to protect your digital footprint, such as while using social media, mobile device apps, and online gaming. Show how to set privacy settings to protect your personal information, including photos of yourself or your location.

(c) Discuss first aid and prevention for potential injuries, such as eye strain, repetitive injuries, and handling electronics devices, that could occur during repeated use. Discuss how to keep yourself physically safe while using a mobile device (for example while walking or biking).

2. Ethics. Do the following:

(a) Relate three points of the Scout Law to things people do on the internet or with computers, phones, and other connected electronic devices.

(b) Discuss with your counselor examples of ethical and unethical behavior in cyberspace. Include how to act responsibly when you encounter situations such as: coming across an unattended or unlocked computer or mobile device; observing someone type their password or seeing it written down near a computer; or discovering a website that is not properly secured. Explain why these situations require good judgement, and how the Scout Law and personal values should guide your actions.

3. Fundamentals. Do the following and discuss each with your counselor:

(a) Describe three types of computer systems that need protecting and explain why.

(b) Explain the 'C.I.A. Triad'—Confidentiality, Integrity, and Availability—and why these three principles are fundamental to cybersecurity.

4. Cyber Threats, Vulnerabilities, and Attacks. Do the following and discuss each with your counselor:

(a) Define the terms vulnerability, threat, and exploit, and give an example of each that might apply to a website or software product you use.

(b) Pick one type of malware (such as virus, worm, Trojan, backdoor, spyware, or ransomware) and find out how it works. Explain what it does and the harm it can cause.

(c) Identify two risks of using public Wi-Fi and describe how to reduce or avoid those risks.

(d) Describe what spoofing and phishing are, and how to recognize a message or website that might be trying to trick you. Explain what steps you should take to protect yourself and others if you come across one.

(e) Current Events. Do ONE of the following:

(1) Read an article or news report about a recent cybersecurity incident. Explain how the incident happened and what the consequences were.

(2) Watch a movie or read a book in which cybersecurity plays a role. Discuss how realistic it was.

(f) Create a list of what is part of your cyber attack surface including all the ways someone could try to access your personal information or devices—such as online accounts, apps, or home networks.

5. Cyber Defenses. Do the following:

(a) Describe three technologies used to defend a computer or network, such as access controls, antivirus software, firewall, intrusion detection/prevention systems, and Virtual Private Network.

(b) Installing updates. Do the following:

(1) Explain the importance of installing the latest updates on your computer.

(2) Demonstrate how to check for, download, and install updates on a device.

(c) System security. With permission, do THREE of the following:

(1) Describe what makes a good password and why.
(2) Describe multi-factor authentication (MFA) and demonstrate it.
(3) Install and set up a password manager.
(4) Run a virus scan.
(5) View running processes on your computer and discuss the results.
(6) Use a command line to view open network connections.
(7) Demonstrate how to back up data.
(8) Create a checklist of FIVE things your family can do to stay secure.
(9) Identify and fix a vulnerability on a permitted computer or network.

6. Cryptography. Do the following:

(a) Research and explain to your counselor three situations where encryption is used in cybersecurity.
(b) Show how you can know if your connection to a website is encrypted.
(c) Do ONE of the following:
(1) Create your own encryption code, such as a substitution cipher, and demonstrate encrypting/decrypting a message.
(2) Set up an app that uses end-to-end encryption and explain how it works.
(3) Use a hashing tool to demonstrate file integrity checking.
(4) Create your own PGP email key and send an encrypted message.

7. Connected Devices and Internet of Things (IoT).

Describe four electronic devices you encounter that could be connected to the internet, why this is useful, what risks exist, and how they could be protected.

8. Cybersecurity Activities. Do ONE of the following:

(a) Learn about a cybersecurity competition, camp, or activity you could participate in. Share what you learned with your counselor.
(b) Participate in a cybersecurity competition with members of your troop or school group.
(c) Give a presentation to your patrol, troop, or another group on a cybersecurity topic of your choice.

9. Careers. Do ONE of the following:

(a) Identify three career opportunities in cybersecurity. Research one and share your findings about training, certifications, job prospects, and why it interests you.
(b) Visit a business or organization that works in cybersecurity and share what you learned about the roles and skills needed.