Develop a Basic Network Scanner with Python: Source 3 highlights that knowing how to build tools and automate repetitive tasks with languages like Python empowers you to become a more efficient analyst and that Python ranks among the most prevalent languages in cybersecurity and is relatively easy to learn. Source 3 also mentions that you can start scripting with Python in as little as one month. Furthermore, source 10 specifically suggests that in "phase two," you should challenge yourself to build some kind of thing, a project, and provides the idea to build a simple network scanner, scan your network and look for open ports using Python. This project will give you hands-on experience with Python, a key technical skill, and introduce you to network concepts. You can focus on using libraries like `socket` or `nmap` to scan for active hosts and open ports on your local network.

2.

Simulate a Phishing Awareness Campaign: Source 3 suggests that if you're new to cybersecurity, you can create mock projects to demonstrate your skills. For example, simulate a phishing attack scenario. This project involves creating a realistic-looking phishing email and a corresponding landing page (for educational purposes only, without attempting to capture real credentials). You can then create a brief educational document or presentation explaining what phishing is, how to identify phishing emails, and the potential consequences. This project will help you understand social engineering tactics from an attacker's perspective and allow you to practice communication skills by explaining the risks and mitigation strategies. Understanding attack vectors like phishing is also a core security concept.

3.

Set Up a Basic Home Lab with Virtualization to Explore Operating System Security: Source 7 suggests setting up a home lab using virtual machines to practice security concepts. Source 3 emphasizes the importance of operating systems knowledge, including MacOS, Windows, Linux, as well as their command-line interfaces. For this project, you can use free virtualization software like VirtualBox or VMware Player to install a couple of different operating systems (e.g., a Linux distribution and a Windows evaluation version). Within this isolated environment, you can experiment with basic security configurations like firewall settings, user account controls, and explore command-line tools for system monitoring. Source 10 also recommends getting your own Linux server & secure it, spin up a cloud vm, and starting with the basics of IT and cyber skills. This hands-on experience will build your familiarity with different operating systems and their security mechanisms.