**Exploring Cybersecurity: Learning and Troubleshooting**

In the vast expanse of the internet, a treasure trove of information awaits those seeking clarity or eager to delve into advanced subjects. As we embark on our cybersecurity journey, let’s explore some valuable resources:

* Basics: [Ubuntu: Creating Folders and Files](https://ubuntu.com/tutorials/command-line-for-beginners#4-creating-folders-and-files)
* Advanced: [Unbuntu: Superusers](https://ubuntu.com/tutorials/command-line-for-beginners#7-the-command-line-and-the-superuser) and [Hidden Files](https://ubuntu.com/tutorials/command-line-for-beginners#8-hidden-files)
* Extra Practice: [Command Line Challenge](https://cmdchallenge.com/)

**Troubleshooting Unleashed:**

* Troubleshooting is our trusty companion throughout this course. Whether we’re tinkering with scripts, configuring Azure Lab setups, or navigating access controls, it’s a vital skill.
* While it lacks the glamour of hacking or defending systems, troubleshooting is equally crucial.
* As a penetration tester, system administrator, SOC analyst, network admin, or IT help desk associate, you’ll frequently troubleshoot technology.
* Embrace trial and error, consult Google, or seek help from peers—it’s all part of the process.
* Remember that every search query expands our knowledge. Googling is second nature for IT professionals, providing quick insights into unfamiliar tasks or issues.
* The more challenges you tackle, the stronger your problem-solving prowess becomes. Hiring managers value this mindset.

#### **The Split-Half Search Method**

One specific methodology to apply when troubleshooting is the [Split-Half Search](https://www.peachpit.com/articles/article.aspx?p=420908&seqNum=3). It is an effective tool that can be applied to *any* technical issue to find a solution quickly.

Follow these steps:

* Begin by removing half of the variables that could be causing the problem.
* Retest the system.
* If the issue is resolved, focus on the variables you removed.
* If the problem persists, investigate the variables you didn’t remove.
* Repeat this process, narrowing down the problematic variables until you find the solution.

#### **Stack OverFlow**

* [StackOverFlow](https://stackoverflow.com/questions) is an online community of developers and technologists where anyone can ask questions and provide answers. Think of Stack Overflow as an online hub for developers and technologists.
* It’s a place where you can ask questions and provide answers.
* The community up-votes helpful answers and down-votes less useful ones.
* Consider it like a reliable, extensive version of Yahoo! Answers, specifically tailored to technology-related queries.

## **Staying Informed in the Cyber-verse**

Staying up to date on the latest cybersecurity developments will be a useful habit far beyond your 24 weeks of this boot camp. It will help you relate what you learn in class to what is happening in the real world, and reflect positively during job interviews when you are able to demonstrate your knowledge of the latest news and developments.

In this section, you will explore a few methods you can use to stay up to date and informed.

### **Set Up Google Alerts**

Google will send you email alerts when new results for selected terms appear in their search engine. For example, you can set up an alert to email you once a week for new "ransomware attack" search results.

* [Google: Create an Alert](https://support.google.com/websearch/answer/4815696?hl=en)

### **Read blogs:**

Check out different blogs:

* [Krebs on Security](https://krebsonsecurity.com/)
* [Dan Miessler](https://danielmiessler.com/)
* [WiCyS](https://www.wicys.org/news)

Google "cybersecurity blogs." Various lists should appear and you will be able to explore the various perspectives from a plethora of professionals.

### **More resources**

Beyond blogs, here are a few other resources you can check out in advance of the first days of class:

* [Podcasts](https://digitalguardian.com/blog/best-information-security-podcasts)
* [Twitter Accounts](https://whatismyipaddress.com/twitter-cybersecurity-experts)
* [YouTube Channels](https://kruptos2.co.uk/blog/the-best-cyber-security-youtube-channels-in-2019/)

These aggregated lists are by no means the definitive ranking of resources. You are encouraged to search on your own. Find the voices and perspectives that you find most interesting, informative, and compelling.