**Cybersecurity Podcasts & Video Series:** *A Beginner’s Perspective*

As someone just starting out in cybersecurity, I’ve been looking for ways to make the concepts feel more real and less textbook-y. For this project, I explored two podcasts and two video series that break down security topics in ways that are actually engaging. I wanted to see how professionals talk about threats like phishing, social engineering, and data breaches, and whether these resources could help me connect the dots between what I’m learning in class and what’s happening in the real world.

**Podcast 1:** *Security Now (Steve Gibson & Leo Laporte)*

<https://twit.tv/shows/security-now/episodes/912>

This podcast is like sitting in on a conversation between two experts who genuinely care about explaining things clearly. In the episode I listened to, they talked about recent vulnerabilities in widely used software and how attackers exploit buffer overflows. Steve Gibson broke it down in a way that made sense, even the technical stuff didn’t feel overwhelming. I appreciated how they tied everything back to user impact and system security. It was definitely helpful for understanding how threats evolve and why patch management matters.

**Podcast 2:** *Darknet Diaries (Jack Rhysider)*

<https://darknetdiaries.com/episode/6/>

This one felt more like a true crime podcast, but for hackers. The episode I chose followed a real social engineering attack where someone tricked their way into accessing sensitive data. It was wild to hear how simple tactics like impersonation and emotional manipulation can bypass technical defenses. It reminded me that cybersecurity isn’t just about firewalls and encryption, it’s also about human behavior and awareness. I’d recommend this to anyone who wants to understand the psychology behind attacks.

**Video Series 1:** *Cybersecurity Awareness Training 2025*

<https://www.youtube.com/watch?v=PbqsOYSpyMw&themeRefresh=1>

This video was short but packed with practical info. It covered phishing techniques (including QR code scams, which I hadn’t thought about before), threat actors, and why multi-factor authentication is so important. I liked how it used real-world examples and kept things visual. It helped clarify some of the confusion I’ve had around phishing detection and why organizations need to train employees without overwhelming them.

**Video Series 2:** *Cybersecurity for Beginners: Basic Skills*

<https://www.youtube.com/watch?v=aRbKFCY4tjE>

This one focused on investigation techniques and spotting suspicious activity. It emphasized critical thinking and pattern recognition, skills I’m trying to build. The examples were simple but effective, and it made me realize how much of cybersecurity is about noticing what doesn’t look right. It also reinforced the idea that even basic knowledge can make a big difference in protecting systems.

**Final Thoughts**

All four resources helped me understand cybersecurity in a more relatable way. The podcasts gave me insight into how professionals think and talk about threats, while the videos helped me visualize key concepts like phishing and threat detection. They were accurate, beginner-friendly, and honestly made me feel more confident about what I’m learning. I’d recommend them to other students or anyone curious about how cybersecurity works in the real world.