

Cyberspace: Information Security & Digital Forensics

Lesson Plan

Created By: Zipline Theory

- **Cyber Ethics [lesson 1]**
 - Staying safe online
 - Proper and ethical behavior online (Online interactions)
 - Important cyber values
 - CIA Triad
 - How to identify things like phishing and scams
- **Cybersecurity right now and it's future. [lesson 2]**
 - What is cybersecurity?
 - Small intro
 - Different types of cybersecurity
 - Preventative
 - Offensive
 - Incident Response
 - Digital Forensics
 - Cyber law and cyber crime
 - Networking and cyber systems
 - Jobs and careers in cyber security
 - (I suggest a talk with an actual industry professional)
- **Computer networking, internet protocols, and encoding [lesson 3]**
 - Networking
 - OSI Model
 - TCP/IP
 - IP addresses
 - TCP Protocol, flags(scanners)
 - How computers communicate with each other
 - Server and Client relationships
 - Internet protocols
 - HTTP/HTTPS
 - POST vs GET request
 - Construction of RESTful requests
 - APIs
 - How is HTML served to you on the browser
 - DNS
 - A records
 - CNAME
 - PTR record

- FTP
- SSH
 - Command Usage
 - Encryption (telnet no have encryption because telnet no have brain)
 - Example
 - How a typical page query looks like behind the scenes (DNS lookup, send TCP flags, back and forth communication)
- Encoding/how data is transferred
 - What is unicode
 - Transferring data with things like base64
 - Hex and binary data, data on a low level
- **Digital Forensics and Cryptography [lesson 4]**
 - Steganography/Data in image files
 - How files work, what are files?
 - Windows file artifacts
 - Autopsy
 - FTK Toolkit
 - Strings
 - Metadata
 - LSB data
 - Spectrograms
 - Forensic data
 - Autopsy
 - Collecting evidence
 - How files leave behind traces, computer memory
 - Wireshark
 - Review of networking
 - An interaction between a server and a client in action
 - Cryptography
 - Basic ciphers, block vs stream ciphers
 - How it's used in cybersecurity
 - SSL/TLS

