Slide 1:
Hey everyone, I hope you're having a great day.

Today I'm going to be discussing this week's topic of Communications, Networking and Security.

Hope you enjoy.

Slide 2:

This is basically every point that I'm going to discuss in this slideshow, which you can read at your own leisure.
—————————————————————

Analog to Digital:

First we have analog vs. digital signals.

Analog signals take data line by line and record it with linear bumps, while digital signals convert analog media into a computer's interpreted language.
———————————————————————

Though many analog signals are outdated, there are still several benefits to them. Analog signals, for example, are easier to process, synchronize, and can store an infinite amount of values.

While analog signals can technically still be used modern-day, it's clear that using devices with digital signals will give you the upper hand.

With digital signals, media can be easily edited, copied, shared or played back at any point. Digital signals are also said to last longer than analog signals.
———————————————————————————————————

Networking:

The next topic I'm going to discuss is networking.

I'll first start by explaining what a modem is and what it does.

To put it simply, a modem connects several devices to the Internet by converting analog and digital signals to each other.
—————————————————————————————————————

The modulation process can best be broken down into 5 different steps.

Data generation is the starting point, and is where the computer generates the data in binary form.

The modem converts the signals to analog in order for the information to travel via the Internet.

The data then transmits over a communication line.

Finally, demodulation occurs and the data is converted back to digital and sent to the computer.

The demodulated data is then stored on the device for future usage.
____

Now let’s discuss networks.

To put it simply, a computer network is a system of different devices and systems connected to each other.

Its several components include a switch, bridge, gateway, backbone and a router.

Examples of network topology can be seen in the next slide.
____

This image shows the different forms of network topology, which includes the bus, ring, mesh, star, tree and hybrid.

Using a computer network comes with advantages and disadvantages.

Computer networks allow for the sharing of several different forms of data and software, as well as hardware.

It’s an efficient way to collaborate and communicate with others, quickly access web databases and offer increased security.

One example of this can be cloud storage and the option on many popular web browsers to save passwords.

However, there’s a ton of malicious activity and malware accessible through networks as well as the presence of phishing accounts.

It can pose distractions in a formal environment due to access to different content and media through a source like the internet.

A good network also requires daily maintenance and can become pretty costly, depending on the size of the network.
———————————————————————

Now let’s talk about different types of networks.

Taken from one of this week’s readings, a Wide Area Network spread across a wide geographical area such as an entire country or region. A great example of this is the Internet.

The Metropolitan Area Network covers a specific city or neighborhood. Some examples of this are cell phone systems.

Local Area Networks cover a small area or space such as an office, a building or a coffee shop.

A WLAN, or Wireless LAN, is just a wireless version of a Local Area Network, using radio frequencies instead of physical wiring. An example of this is a home area network that links all digital household devices.

And finally, A Virtual Private Network, or VPN, is used for the sole purpose of connecting to a different location or region. This involves using another IP address, for example.
——————————————————————————————————————

Next, a network’s architecture refers to a network’s structure. Some of its components include the following:

Topology, which is the layout of the network,
A **client**, which is, quoted from splunk.com, “requests and receives services from a server”,
A **switch**, which is a device that connects devices together,
Protocols, or regulations for data exchange over networks,
And **transmission media**, which is how data is transmitted.

This can be analog or digital.
——

Here are the types of network architecture.

Peer to peer, according to information on Splunk, involves “each node [acting] as a client and server simultaneously”. It’s best for the simple distribution of resources and communication.

The client-server model is similar to the peer to peer model, except this time, one computer acts as a server while the other nodes act as clients and receive processed requests from the server.

Hybrid networks combine elements of both previously mentioned models and both devices can act as both clients or servers.

Cloud based networks are used to access resources through cloud-based services.

The front-end side of the server is where the users interact with the services, and the back-end side provides the services with needed resources.
——————————————————————————————

The OSI Model describes how computers interact with each other within a network, and includes 7 main layers.

I’ve also included 2 helpful videos into this slide for additional info.
——————————————————————————————

The layers are broken up into different sections:

The Hardware Section (which includes the physical, data link and network layers),

The “Heart of the OSI”, which just contains the transport layer,

And the software portion, containing the session, presentation and application layer.

These layers all work together to send data from the user to the network and back.

This also provides a great visualization for how the model actually works.
—————————————————————————————

The difference between wired and wireless communication should be a bit obvious from their names.

As written, wired communication relies on physical wiring to connect devices to a network, while wireless communication uses radio waves instead.
Examples of devices that use a wireless network connection are TV censor bars, antennas and video game controllers.

I’ll now briefly discuss three types of **wired** and **wireless** communications.

Twisted-pair cables are a type of wire that are made of insulated copper that appear “twisted”, or in a spiral pattern. These are commonly used with telephone systems or Local Area Networks.

Co-axial wires include several layers including an inner conductor, inner insulator, outer conductor shield, outer insulator all covered by a plastic cover.

Its appearance gives more of a drill-type shape, and personally reminds of the end of an audio-jack plug.

This wire is commonly used for ethernet and television setups.

Fiber-optic cables are made up of several fibres. These are best used for long-distance connections and are commonly used for an Internet connection, television broadcasting or devices in different industries.

Now onto wireless media.

Infrared waves are best used for short-range connections due to their inability to penetrate through objects. These types of waves are also not visible to humans.

Radio waves, in a sense, are like the complete opposite of infrared waves. They can travel any distance, long or short, and penetrate through any object. These are used with AM and FM radios and cordless phones.

Microwaves require an equal alignment between both receiving and sending antennas, with their distance being equal to the antenna’s height. They’re commonly used with mobile phones and TV distribution.
———————————————————————————————————————

The last section of this presentation covers cyber threats and how you can protect yourself from them.

————————————————————————

Cybersecurity refers to the practice of protecting digital media and data from any cyber attack or threat.

Whether it’s on the internet, through applications or services (either online or offline) through networks, huge masses of personal data are collected and stored. This means that unauthorized access to private info could lead to several different consequences including theft, fraud, spread of malware and viruses, and data corruption.

This is why cybersecurity is so important to use and maintain by anyone using a network, the internet, or a digital device with sensitive information.

————————————————————————

There’s several types of cybersecurity.

Network Security protects users and software from unauthorized access.

Application security makes sure that software is secure and legitimate.

Data Security protects sensitive data and involves Data classification, Encryption, Access controls and Data Loss Prevention (or DLP) measures. (quoted from GeeksforGeeks)

Cloud Security involves securing data hosted on cloud services, such as AWS or the Google Cloud.

Endpoint Security involves defending Internet of Things (IoT) devices like laptops and smart devices. Part of this also involves utilizing firewalls (which monitor and filter malware out of network traffic) and anti-virus software.

Operational Security manages internal security protocols as well as protecting from threats and “human errors”

Internet of Things Security defends and secures any devices connected to the internet from risk.

—————————————————————————————————

Let’s talk about cybercriminals.

Although there is a such thing as ethical hacking, certain hackers with malicious intent aim to gain access and exploit their targets by searching for vulnerabilities within different software and apps.
——————————————————————————————————

The statement that “there are a lot of different cyber threats” is now an understatement, as people are gaining loopholes to hack through any system with rapidly developing technology.

That being said, let’s look at these types of cyber threats.

Malware was created to enter, attack and damage digital systems. Some types of malware are viruses, trojans, spyware and rootkits.

Phishing refers to an attempt to trick users into giving away sensitive information such as name, password, address, etc.

Ransomware involves locking important files/information by encrypting the software and demanding pay, or a ransom, to unlock the data. Failure to comply usually results in a threat to having the information leaked.

Distributed Denial-of-Service, or DDoS attacks, flood a network with large amounts of traffic to make servers crash and disable services on the network.

SQL and NoSQL Injection is when harmful SQL code is inserted into weak or insecure databases to either modify or steal information.

Zero-Day Exploits involve modifying and taking advantage of unknown software vulnerabilities, such as a glitch, before they are able to be patched.

Advanced Persistent Threats, quoted from GeeksforGeeks, use “multi-stage attack[s]” to stay hidden in software and gradually keep control over a network.

Man-in-the-Middle attacks, also taken from GeeksforGeeks, “secretly intercept and modify data exchanged between two parties by exploiting weak encryption or unsecured communication channels”

And last, Insider Threats and Privilege misuse happens when system administrators or employees with access to sensitive info steal data and modify access restrictions.
———————————————————————————————

Now that we’ve gone over the types of cyber security and cyber threats, let’s talk about how you can stay safe online.

To prevent the theft or misuse of your data, be sure to use strong passwords, trusted and secure networks and software, and up-to-date technology with regular updates and maintenance.

This makes it more difficult for cybercriminals to exploit errors in the system and gain access to your private information.

It’s also never a bad idea to stay educated on cybersecurity trends or different types of cyber attacks.

Conclusion:

To conclude this lecture, let’s review what we discussed.

We talked about the difference between analog and digital signals,

The significance of a modem and its relevance to networking,

The function of, uses of and types of computer networks,

Purpose of the OSI Model,

Wired and wireless media,

The key components of cybersecurity,

And some tips to avoid cyber threats.

Below are the references to all information and images used in this presentation.

Thank you for watching.