Unit 3: Safe Computing

Vocabulary

**Vocab or concepts from the APCSP course description

Distributed Denial of Service (DDoS)	An attack on a network resource that prevents authorized users from accessing the system
**Trust model	The Internet is based on a "trust" model meaning Certificates of Authority are issued that insure the public keys shared by sites we want to do secure processing with are legitimate. Example: If we are buying a product online, our web browsers can trust that the company site is the correct one based on their digital certificate and we can proceed with our credit card transaction.
Cybersecurity	Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks.
Cyber warfare; cybercrime	Cybercrime is any criminal activity that involves a computer, networked device or a network.
**Phishing	a technique that attempts to trick a user into providing personal information. That personal information can then be used to access sensitive online resources, such as bank accounts and emails.
**Viruses	a malicious program that can copy itself and gain access to a computer in an unauthorized way. Computer viruses often attach themselves to legitimate programs and start running independently on a computer.
Firewall	A gateway machine and software that protects a network by filtering the traffic it allows
**Symmetric key encryption	Encryption that uses the same key for both encryption and decryption.
**Public key encryption	Public key encryption pairs a public key for encryption and a private key for decryption. The sender does not need the receiver's private key to encrypt a message, but the receiver's private key is required to decrypt the message.

**Certificate authorities	A Certificate Authority (CA) (or Certification Authority) is an entity that issues digital certificates to validate the ownership of encryption keys used in secure communications and are based on a trust model.
**Digital certificate	A representation of a sender's authenticated public key used to minimize malicious forgeries
DNS spoofing	Domain Name Server (DNS) spoofing (a.k.a. DNS cache poisoning) is an attack in which altered DNS records are used to redirect online traffic to a fraudulent website that resembles its intended destination.
**Malware	A computer program that attempts to bypass appropriate authorization safeguards and/or perform unauthorized functions
Mal-advertising	Malvertising the use of online advertising to spread malware. It typically involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages.
TSL / SSL	public key encryption protocol to allow safe communication on the internet
**keylogging	the use of a program to record every keystroke made by a computer user in order to gain fraudulent access to passwords and other confidential information.
**Rogue access point	a wireless access point that gives unauthorized access to secure networks.
**Freeware/shareware	software that is available free of charge and often distributed informally for evaluation, after which a fee may be requested for continued use.
**Multi Factor authentication	a method of computer access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism, typically in at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).
**Authentication measures	Protect devices and information from unauthorized access. Examples include passwords and multi factor authentication.
**Personally Identifiable Information (PII)	Information about an individual that identifies, links, relates or describes them. Examples of PII include: social security number, age, race, phone numbers, medical information, financial information
**Search engine	a program that searches for and identifies items in a database that correspond to keywords or characters specified by the user, used especially for finding particular sites on the World Wide Web.

**Web cookies	An HTTP **cookie** (**web cookie**, browser **cookie**) is a small piece of data that a server sends to the user's **web** browser. The browser may store it and send it back with later requests to the same server. Typically, it's used to tell if two requests came from the same browser — keeping a user logged-in,
**Identity theft	The fraudulent acquisition and use of a person's private identifying information, usually for financial gain.
**Geolocation	the process or technique of identifying the geographical location of a person or device by means of digital information processed via the Internet.
**Metadata	data about data. For example, the piece of data may be an image, while the metadata may include the date of creation or the file size of the image.