LAW ENFORCEMENT CYBER PRIMER

THREAT GROUPS:

- **Hactivists** – (hacker + activist) target law enforcement to further an ideology or political agenda. Their activities may relate to an established ideology, a specific issue, or a particular cause.
  Example: Anonymous
- **State Actors** – state-sponsored military or intelligence services, groups, and individuals acting on behalf of foreign governments. *Example: China, Iran, North Korea*
- **Terrorist Organizations** – organizations using violence or the threat of violence to further political, religious, or ideological agenda. Accomplishes objective with intimidation, coercion, and fear.
  Example: ISIS
- **Criminal Organizations** – groups engaged in planned and sustained criminal activities.
  Example: Russian Mafia
- **Purposeful or Accidental Insider** – employees or contractors who would purposefully cause harm to an agency. Also includes the accidental insider who is unaware that he or she has become the organization's weakest link in the cyber chain.
  Example: Edward Snowden
- **Individual** – someone who has adopted or taken up a cause.
  Example: Kevin Mitnick

METHODS:

- **Phishing** – the practice of sending email to users with the purpose of tricking them into revealing personal information.
- **Spear Phishing** – a targeted form of phishing. Rather than indiscriminately sending email, spear phishing targets specific groups of users or even a specific user.
- **Whaling** – a form of spear phishing that targets high-level executives.
- **Vishing** – using the phone system or VoIP to trick users into giving up personal and financial information.
- **Tailgating** – sometimes called piggybacking, is the practice of one person following another closely behind without showing credentials.
- **Dumpster Diving** – searching through trash to gain information from discarded documents.
- **Impersonation** – impersonating another with the goal of convincing an authorized user to provide some information to help them defeat a security control.
- **Shoulder Surfing** – looking over the shoulder of someone to gain information.
- **Social Media Platforms** – social media platforms are used to organize and plant attacks.
- **Physical Disruption** – causing damage to physical components.
- **Theft** – theft of physical items/components.

DEPLOYMENT:

- **Virus** –attaches to clean files and infects other clean files. Can spread uncontrollably, damaging a system's core functionality and deleting or corrupting files. Usually appear as an executable file.
- **Trojan** – disguises itself as legitimate software, or is included in legitimate software that has been tampered with. Tends to act discretely and create backdoors.
- **Spyware** – software designed to spy. Hides in the background and takes notes on user activity.
- **Adware** – adware stands for advertising malware that presents unwanted advertisement using intrusive and at times dangerous methods.
- **Spam** – sending unsolicited bulk email.
- **Email** – legitimate email sent from a compromised account or one altered to appear legitimate.
- **Free Software** – free software with malicious code written with the intent of doing harm to data or devices is made available for download.

ATTACKS:

- **Denial-of-Service (DoS)** – an attack from a single source that attempts to disrupt the services provided by another system.
- **Distributed Denial-of-Service (DDoS)** – includes multiple computers attacking a single target. DDoS attacks typically include sustained, abnormally high network traffic.
- **Botnet** – combines the words robot and network. It is a group of computers called zombies controlled through a command control server. The zombies await instructions from whoever controls the botnet.
- **Spoofing** – when one person or entity impersonates or masquerades as someone or something else.
- **Man-in-the-Middle** – a form of active interception allowing an attacker to intercept traffic and insert malicious code to other clients.
- **Replay** – an attacker replays data that was already part of a communication session. In this type of attack a third party attempts to impersonate a client that is involved in the original session.
- **ARP Poisoning** – address resolution protocol poisoning is an attack that misleads computers or switches about the actual MAC address of a system.
- **Ransomware** – malware that locks a victim's computer, typically by encryption, and payment is demanded before the ransomed data is decrypted and access returned to the victim.

FREE TRAINING OPPORTUNITIES	
NW3C: https://www.nw3c.org/online-training	Provides a nationwide support system for law enforcement and regulatory agencies involved in the prevention, investigation, and prosecution of economic and high-tech crime.
FedVTE: https://fedvte.usalearning.gov/	A free online, on-demand cybersecurity training system that is available at no charge for government personnel and veterans. Managed by DHS, FedVTE contains more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis.
NCFI: National Computer Forensics Institute All nominations must be submitted through your local U.S. Secret Service office.	NCFI training courses are offered to state and local law enforcement, prosecutors and judges through funding from the federal government. Travel, lodging, equipment (in some classes), and course fees are provided at no costs to attendees or their agencies.
Cyber Investigation Certification Program (CICP): Available through Law Enforcement Enterprise Portal (LEEP)	Bringing together the expertise of Carnegie Mellon University, the FBI's Cyber Division, and the International Association of Chiefs of Police (IACP), the self-guided online program is available to all federal, state, local, tribal, and territorial (SLTT) first responders and investigators.

LAW ENFORCEMENT CYBER PRIMER

TERMS AND CONCEPTS

- **DHCP** - The dynamic host configuration protocol allows computers to automatically request and be assigned IP addresses and other network settings.
- **DNS** - Domain Name System. The domain name system is how computers convert human-readable domain names and hostnames to numerical IP addresses. When you type Google.com into your web browser's address bar, your computer contacts its DNS server and the DNS server replies with the numerical IP address of Goodge's server
- **Domain Name** - Domain names are the base part of website names. For example, cnn.com or google.com. Note that domain names are just another type of hostname.
- **Ethernet** – Ethernet is the standard wired network technology in use almost everywhere today. If your computer is connected to a network via a cable, it's likely using an Ethernet cable, which plugs into an Ethernet port on your computer.
- **Firewall** – A firewall is a security system designed to prevent unauthorized access on a private network. Firewalls can be implemented as hardware or software.
- **Gateway** – A node on a network that serves as an entrance to another network. It routes traffic between networks.
- **Hostname** – A hostname is a human-readable label that points to a device connected to a network.
- **HTTP** – The hypertext transfer protocol is the standard protocol modern web browsers and the web uses.
- **IP Address** – An identifier for devices on a TCP/IP network. Networks using TCP/IP route messages based on the IP address of the destination. An Internet Protocol address, or IP address, is a numerical address that corresponds to your computer on a network. When a computer wants to connect to another computer, it connects to that computer's IP address.
- **ISP** – Internet Service Provider. This is the company that provides an Internet connection. For example, Comcast and Verizon
- **LAN** – Local Area Network. This is a small network that is confined to a local area. For example, a home network or an office network.
- **Localhost** - The hostname "localhost" always corresponds to the device you're using. This uses the loopback network interface — a network interface implemented in software — to connect directly to your own PC.
- **MAC Address** – Each network interface has a media access control address, or MAC address — also known as a physical address. This is a unique identifier designed to identify different computers on a network.
- **NAT** – Network Address Translation is used by routers to share a single IP address among many devices.
- **Packet** - A packet is a unit of data sent between devices.
- **Port (virtual)** - When an application wants to send or receive traffic, it uses a virtual port between 1 to 65,535. This allows for multiple applications on a computer to use the same network.
- **Protocol** - Protocols are different ways of communicating over the Internet. TCP and UDP are the most common protocols.
- **Router** - A device that forwards data packets along networks. A router is connected to at least two networks and are located at gateways.
- **URL** - A uniform resource locator, or URL, is also known as a web address.
- **WAN** - A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

THREE FACTORS OF AUTHENTICATION

Something you know	→ username, password
Something you have	→ token, authentication app.
Something you are	→ biometrics

⬇

Combine two *different* factors to create Two-Factor Authentication

INFORMATION SECURITY TRIAD

Confidentiality	Prevents the unauthorized disclosure of data using multiple methods such as authentication combined with access controls and cryptography.
Integrity	Provides assurances that data has not been modified, tampered with or corrupted.
Availability	Data and services are available when needed.

Confidentiality + Integrity + Availability = CIA Triad

Different elements of the CIA Triad will take the lead in different companies. For example, a bank may consider integrity the most important, whereas a data processing company may see availability as the most important.

VIRTUAL CURRENCY

A medium of exchange that operates like currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction.

Two Types:

1. Nonconvertible – fake money used in gaming systems.
2. Convertible – has an equivalent value in real currency, or acts as a substitute for real currency e.g., Bitcoin.

Real Currency v Convertible Virtual Currency

	Real Currency	Convertible V.C.
Backed by	Products, services, economy of issuing company.	Products, services, and sound consensus of users.
Governed by	Central banks	Mathematics and distributed computing
International transfers	Several days	Minutes
International transfer cost	2-3% of transaction	0 - $.01
Chargebacks	Possible	No chargebacks

1. **Centralized** – has a centralized repository and a single administrator. Uses intermediary to issue currency, maintain central payment ledger, and determine exchange rate e.g., linden dollars, perfect money, webmoney, WoW gold.
2. **Decentralized** – no central repository and no single administrator. Can be obtained by computing or manufacturing effort e.g., bitcoin, ethereum, litecoin, dash, monero.

Bitcoin is most the popular Virtual Currency.

Bitcoin Wallets

Website	Browser based. User signs in with username & password.
Mobile	Run from a smartphone app.
Software	Runs on a desktop or laptop. Most common.
Cold Storage	Dedicated hardware that is specifically built to hold cryptocurrency and keep it secure. This includes USB devices.

- A Private Key allows Bitcoins to be spent.
- A Public Key is used to transfer Bitcoins between users.