## Types of Phishing:

### Business Email Compromise (BEC):

Hackers use a trusted email to look trustworthy in a malicious email looking to steal your data.

### Spear Phishing:

Spear phishing is a form of phishing, which is an attack directed toward a certain group or person.

### Whaling:

Whaling is a type of attack that targets executives at an organization.

### Vishing:

Vishing is a type of cyber attack that uses a prediction algorithm to learn the victim's voice, to guilt the victim into giving their personal information.

### Smishing:

Smishing is the last type of phishing attack that will be mentioned. Uses text messages for hackers to attempt to disguise themselves that they're not.

## Types of Malware:

### Virus:

A virus acts like a real virus. Attempting to harm a computer's processes, and sometimes even destroying the computer in the worst cases.

### Worm:

A worm is another type of malware. That tries to duplicate itself across computers.

### Ransomware:

Ransomware is a sort of cyber attack that encrypts a user's data and demands payment, typically in cryptocurrency, for the decryption key required to restore access to the information.

### Spyware:

Spyware gathers your personal information and sells it.

## Types of Engineering:

### Social Media Phishing:

Social media phishing uses the victim's data from any social media and then uses it to plan an attack.

### Watering Hole Attack:

The Watering Hole attack is a type of attack that uses information from recently leaked websites that have high traffic.

### USB Baiting:

USB baiting is an attack that has the threat actor pray that someone will use the USB drive out of curiosity, for that drive to inject malware onto the computer.

### Physical Social Engineering:

A threat actor impersonates a trusted figure and gets authorized access.

## Social Engineering Principles:

### Authority:

Threat actor posing as a trusted figure.

### Intimidation:

Bullying the victim for information.

### Conscientiousness / Social Proof:

The threat actor pretends to be someone or is that person, Who is asking for confidential information.

### Scarcity:

A threat actor displays that there is a limited amount of a product. Endeavoring to get the victim to give their personal information without giving full thought.

### Formality:

The threat actor shows that they have a social connection, which they don't have.

### Trust:

The treat actor goes to make the victim believe that they are a figure of authority.

### Urgency:

A Threat actor usually takes what the victim has of personal information, and demands that the victim needs to give this thing the threat actor wants now, so the victim can live in peace.

## CISSP Security Domains:

### Security & Risk Management:

Define goals and objectives such as risk mitigation, compliance, continuity, and the law.

### Asset Security:

Secure physical & digital assets. Relates to storage, maintenance retention, and destruction of data.

### Security Architecture & Engineering:

Ensures tools, systems, & Processes. So that they are up to date.

### Communication & Network Security:

Ensures that the user manages physical networks, & wireless communications.

### Identity & Access Management.

Follows data security by making users follow established policies & manage physical assets.

### Security Assessment & Testing:

Conducting security control, testing, collecting, analyzing data, and conducting security audits to monitor risks, threats, and vulnerabilities.

### Security Operations:

To conduct investigations and implement preventative measures.

### Software Development Security:

Write code that follows security guidelines and frameworks for applications and services, to keep software secure.

## Types of Cyber Attack:

### Password attack:

A password attack constantly tries to brute force a user's password. By using a trainable table to decrypt the hashes.

### Social Engineering Attack:

All of the types of attacks that were mentioned before in Social Engineering, to exploit a victim into giving personal information.

### Physical attack:

A physical attack uses any device such as a malicious USB unit. To trick the victim, but can also be a case of credit card cloning.

### Adversal AI

The threat actor uses a prediction algorithm to conduct and act more effectively with machine learning.

### Supply Chain Attack

The supply chain attack targets, systems, software, & variabilities. Usually, unsecured third parties can affect multiple organizations.

### Crypto-Graphic Attack:

A cryptographic attack breaches important forums such as your birthday, collision, and downgrade.

## Threat Actor Types:

### Advanced Persistent threats:

APTs have significant skill in accessing networks, they tend to research their targets to remain undetected. Their motivations include damaging critical infrastructure, and gaining access to intellectual property.

### Insider threats:

The threat actor type abuses authorized access to cause harm. Motivations may be, sabotage, corruption, espionage, and data leaks.

### Hacktivists:

Due to their political agenda, they take what they think is politically right, demonstrations, propaganda, social change campaigns, and fame. They use these to accomplish their goals.

## Hacker Types:

A hacker uses computers to gain access to networks & data.

### Authorized / Ethical Hackers

Authorized hackers or Ethical hackers follow ethics, find breach potentials, and report them.

### Semi Authorized Hackers

Like an Authorized hacker, they research vulnerabilities and report them. They don't take advantage of them like a vigilante.

### Unauthorized/Unethical Hackers

These Unethical hackers do what Authorized hackers do, but instead, they have no respect for the law. Collecting and selling confidential information.