Module 2

What you'll learn

- Viruses
- Malware
- Social Engineering
- Digital age
- Security domain

Key Terms

Computer Virus : Malicious code written to interfere with computer operation and cause damage to data and software

Malware : Software designed to harm devices or network

Social Engineering : A manipulation technique that exploit human error to gain private information, access or valuables

Phishing : The use of digital communication to trick people into sensitive data or deploying malicious software

Note :- During the Equifax breach, over 143 million customer records were stolen and the breach affected approximately 40% of all Americans

Common Attack CSIRT = computer security incident and response team

- **Phishing** : Some major ones are
  - Business email compromise (
  - Spear for phishing (target specific user)
  - Whaling (executive of company)
  - Vishing (electronic voice exploitation
  - Smishing (use of text message)

Malware : - Viruses
- Worms (duplicate and spread itself)
- Ransomware (ask payment to restore access after breaching)
- Spyware (gather and sell info without consent)

Social Engineering
- social media phishing (collect data from social media)
- water hole attack (attack a website frequently visited by group of users)
- USB baiting : (strategically leave malware USB for employee to find and install)
- Physical social engineering (impersonate)

Raj
DATE / /
PAGE

CISSP Defines 8 domains

1 Security and Risk Management
2 Asset security
3 Security architecture and engineering
4 Communication and network security
5 Identify and access management
6 Security assessment and testing
7 Security operation
8 Software development security

Full form : Certified Information system security ~~Professional~~ Professional

Security and Risk Management :

Define security goals and objective risk mitigation, compliance, business continuity and the law

Asset Security :

Secure digital and physical assets It also related to the storage, maintenance, retention and destruction of data

Security architecture and Engineering

Optimizes data arch. security by ensuring effective tools, system and processors are in place

Risk assessment

DATE / /
PAGE

Communication and network security:
Manage and secure physical network and wireless communication.

Identify and access management:
Keep data secure, by ensuring user follow established policies to control and manage physical assets like office space and logical assets such as network and application.

Security assessment and testing
Conducting security control testing, collecting and analyzing data and conducting security audits to monitor for risks, threat and vulnerability

Security operation:
Conducting investigation and implementing preventative measures

Software development security:
Uses secure coding practices which are a set of recommended guidelines that are used to create secure applications and services