KV BILASPUR

CYBER JAAGROOKTA DIWAS

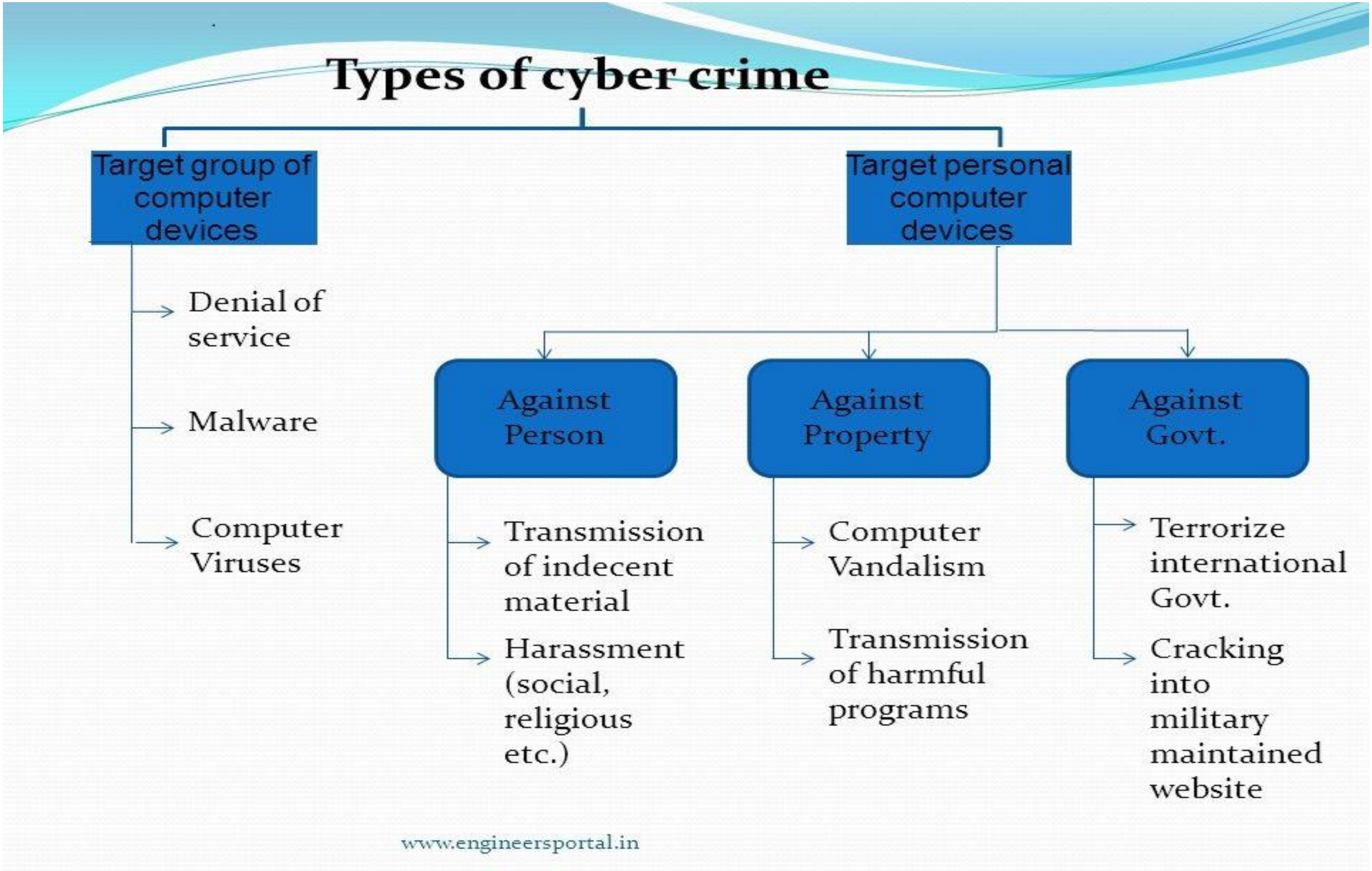
DATE – 06-10-2021

What is cybercrime?

Cybercrime encompasses any criminal act dealing with computers and networks (called hacking). Additionally, cybercrime also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cybercrimes when the illegal activities are committed through the use of a computer and the Internet.

Rarely, cybercrime aims to damage computers for reasons other than profit. These could be political or personal.

Types of cybercrime



Types of cyber crime

Target group of computer devices

- Denial of service
- Malware
- Computer Viruses

Target personal computer devices

Against Person

- Transmission of indecent material
- Harassment (social, religious etc.)

Against Property

- Computer Vandalism
- Transmission of harmful programs

Against Govt.

- Terrorize international Govt.
- Cracking into military maintained website

www.engineersportal.in

WHAT IS PHISHING?

Phishing is the criminal and fraudulent act of attempting to acquire sensitive information such as usernames, password and credit card details by masquerading as a trustworthy entity or person in an electronic communication.

What is identity theft?

Identity theft, also known as *identity fraud*, is a crime in which an imposter obtains key pieces of personally identifiable information (PII), such as Social Security or driver's license numbers, to impersonate someone else.

The stolen information can be used to run up debt purchasing credit, goods and services in the name of the victim or to provide the thief with false credentials. In rare cases, an imposter might provide false identification to police, creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen.

- **WHAT IS CYBERSTALKING?**

- Cyberstalking, which is simply an extension of the physical form of stalking, is where the electronic mediums such as the Internet are used to pursue, harass or contact another in an unsolicited fashion

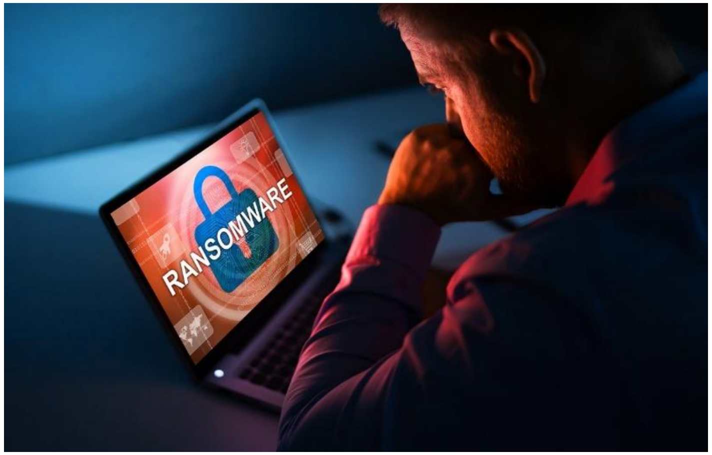
CYBER OBSCENITY

Cyber obscenity includes pornographic websites, pornographic online magazines and the internet to download and transmit pornographic pictures, photos and writing. The photographs of women are used, morphed and distributed in the internet with obscene postures.

- **Vandals**

- Vandals often use hacking techniques to deface a website or destroy data and files, but there are also those who just want to steal resources (make use of other people's servers without their knowledge or permission) or to cover their tracks by stealthily making use of hardware owned by legitimate businesses to carry out processing for illegal operations or to relay spam and viruses to others.

- **RANSOMWARE**



- Ransomware is malware that typically enables cyber extortion for financial gain. Criminals can hide links to Ransomware in seemingly normal emails or web pages.

- Once activated, Ransomware prevents users from interacting with their files, applications or systems until a ransom is paid, typically in the form of an anonymous currency such as Bitcoin.
- Ransomware is a serious and growing cyber threat that often affects individuals and has recently made headlines for broader attacks on businesses. Payment demands vary based on targeted organizations, and can range from hundreds to millions of dollars.
- Ransomware is often introduced into an organization through phishing emails, but it may also be introduced via exploits, USB drives and other media containing malware. It functions quickly. It spreads from machine to machine via the corporate network, affecting endpoint devices (PCs, laptops) and servers, and can also spread to storage media on the network. Once files are encrypted it is (for all intents and purposes) impossible to unlock them