



SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

COURSE NAME: 19EC625 – CYBER FORENSIC AND DATA SECURITY
III YEAR / VI SEMESTER

Unit III- INTRODUCTION TO COMPUTER FORENSICS Topic: Traditional Computer Crime



What is Computer Crime



Donn Parker is generally cited as

- Computer crime also known as cybercrime is when people use computers to do illegal things.
- It happens when someone who knows a lot about computers uses them in ways that are not allowed. This might include looking at or taking private information that doesn't belong to them.
- It can also mean damaging other people's computers or files. Sometimes, these people use computers to steal or trick others.
- The person doing these bad things is often called a hacker. Computer crimes can hurt both the people and the businesses. This kind of wrongdoing is against the law and can get people into serious trouble.



Categories of Computer Crime



Robert Taylor and company expand on Parker's definitions and present four categories of computer crime

The computer as a target: The attack seeks to deny the legitimate users or owners of the system access to their data or computers. A Denial-of-Service (a.k.a., DOS or DDOS) attack or a virus that renders the computer inoperable would be examples of this category.

The computer as an instrument of the crime: The computer is used to gain some information or data which are further used for criminal objective. For example, a hacker may use a computer system to steal personal information.

The computer as incidental to a crime: Sometimes a computer may not the primary instrument of the crime; it simply can facilitate it. Money laundering and the trading of child pornography would be examples of this category.

Crimes associated with the prevalence of computers: This includes the crimes against the computer industry, such as intellectual property theft and software piracy etc.



Categories of Computer Crime



Wall's four legal categories for cyber crime

Cyber-Trespass: Crossing boundaries into other people's property and/or causing damage—for example, hacking, defacement, and viruses.

Cyber-Deceptions and Thefts: Stealing (money, property)—for instance, credit card fraud and intellectual property violations (a.k.a., "piracy").

Cyber-Pornography: Activities that breach laws regarding obscenity and decency.

Cyber-Violence: Doing psychological harm to, or inciting physical harm against others, thereby breaching laws pertaining to the protection of the person—for example, hate speech and stalking.





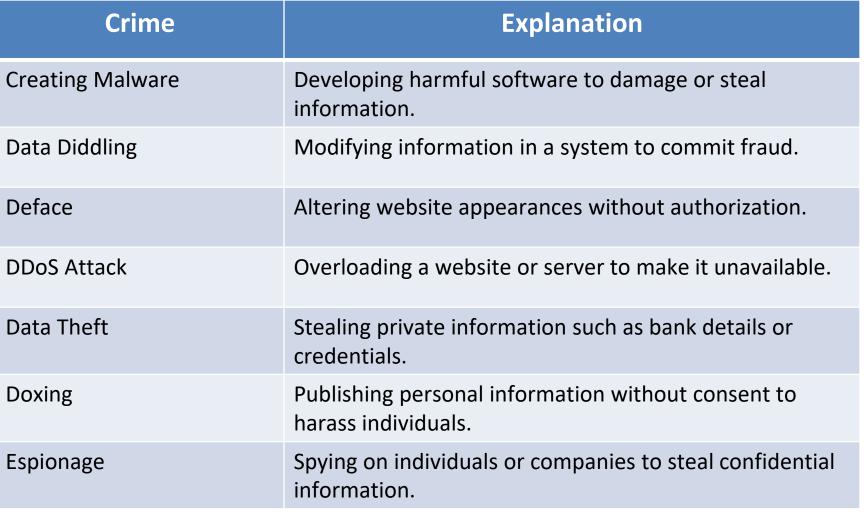
Expl	Crime	Explanation
	Child Pornography	Making, sharing, or keeping illegal sexual content involving children.
	Click Fraud	Manipulating online ads by clicking repeatedly to generate revenue or harm businesses.
	Copyright Violation	Using or distributing copyrighted content without permission.
	Cracking	Breaking security systems or passwords to access private data.
	Cyber Terrorism	Using technology to threaten or attack individuals, businesses, or governments.
	Cyberbullying / Cyberstalking	Harassing, intimidating, or threatening individuals online.
	Cybersquatting	Registering domain names to resell them at high prices.







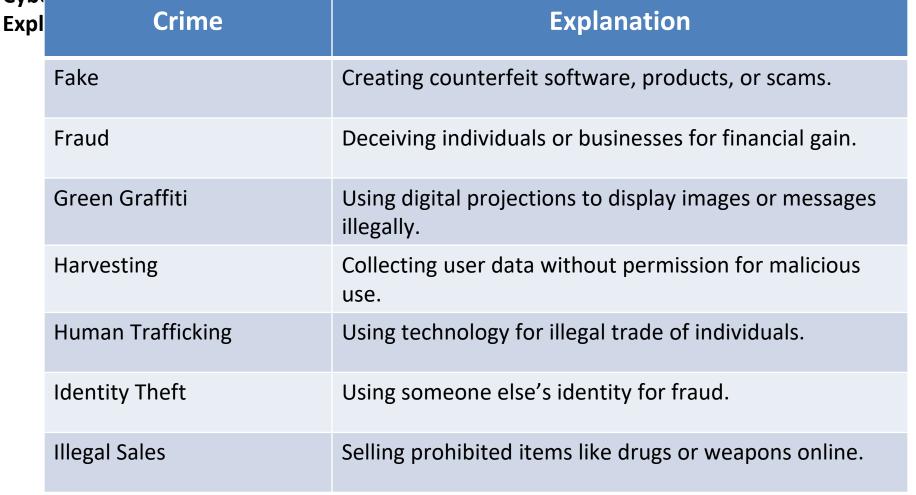
Expl







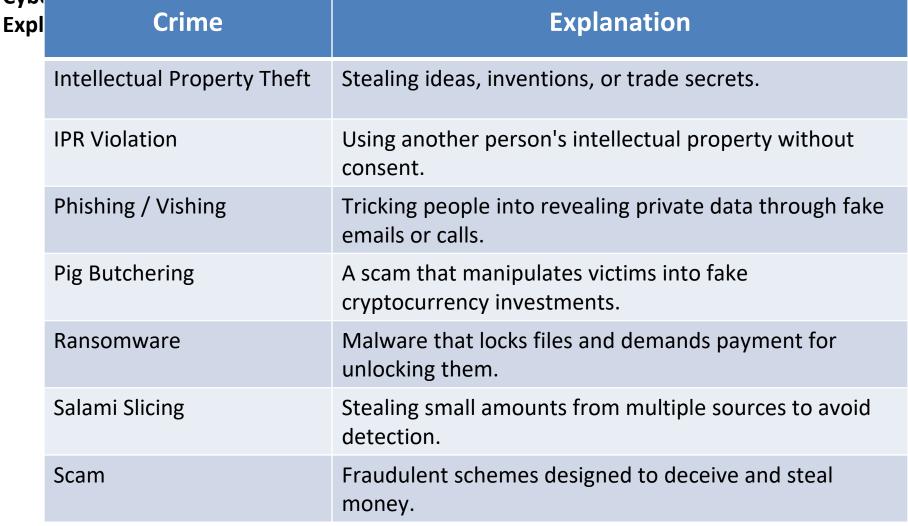
















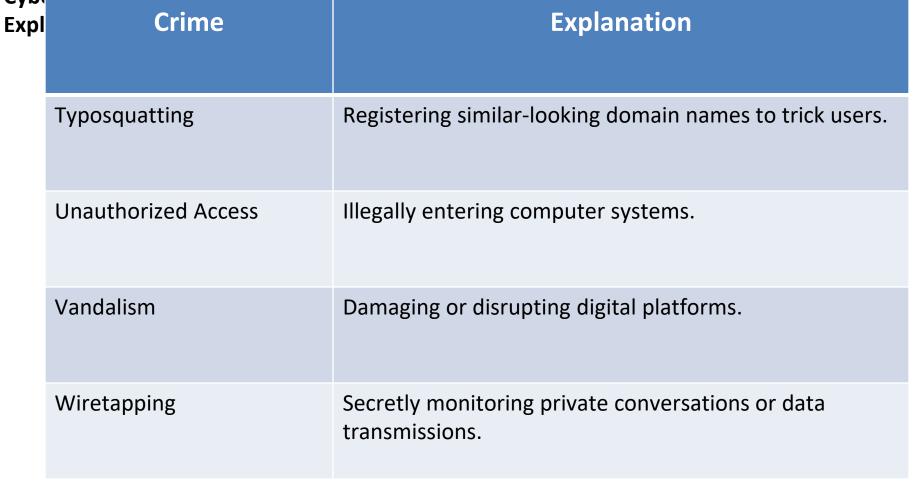


Expl	Crime	Explanation
	Sextortion	Threatening to share private images unless demands are met.
	Slander	Spreading false information to damage reputations.
	Software Piracy	Using or distributing unauthorized software copies.
	Spamming	Sending large amounts of unwanted emails.
	Spoofing	Pretending to be someone else online to deceive systems or people.
	Swatting	Making fake emergency calls to send police to someone's house.
	Theft	Stealing physical or digital assets.

















Thank you.....