Cybercrime

Cybercrime refers to illegal activities carried out with a computer over a network such as the internet.

Types of Cyber Crime

Cybercrime takes many different forms. Criminals who infiltrate computers and networks have developed a variety of malicious software and social engineering techniques used individually or in combination when use in committing different types of cybercrime.

The key characteristics of cybercrime include:

- The use of digital technologies – either a desktop or laptop computer, but also mobile phones and games consoles.

- Cybercrime takes place over networked devices. (NB this means one of the main strategies for protecting yourself is to DISCONNECT OR SWITCH OFF your devices whenever you can!)

- Most cybercrime is informational – it involves an attempt to access and steal personal or corporate/ government information or an attack on online identities. Cybercrime is non-local in nature – it takes place in 'cyberspace', not in a real physical location.

- There are physical locations where 'attacks' originate from, and these are often in different countries to the victims, making cybercrime very global in nature.

- There is a considerable 'data gap' when it comes to what we know about cyber criminals – more than 80% of victims of online fraud can say NOTHING about the person that committed a crime against them for example.

Some of the most common types of cybercrime include:

- Identity and data theft
- internet fraud (online scams)
- hacking (unauthorised access to networks)
- Infecting devices with viruses
- Denial of Service attacks (DOS attacks)
- file sharing in breach of copyright
- 3D Printing of illegal products
- Cyberwarfare
- child pornography

Hacking

Criminal hacking is the act of gaining unauthorized access to data in a computer or network. Exploiting weaknesses in these systems, hackers steal data ranging from personal information and corporate secrets to government intelligence. Hackers also infiltrate networks to disrupt

operations of companies and governments. Computer and network intrusions cost billions of dollars annually, according to the FBI.

Malware

Malware, or malicious software, refers to any code designed to interfere with a computer's normal functioning or commit a cybercrime. Common types of malware include viruses, worms, trojans, and various hybrid programs as well as adware, spyware, and ransomware.

Ransomware attacks are growing in volume and sophistication, the FBI reports. Locking valuable digital files and demanding a ransom for their release, ransomware attacks are commonly executed using a trojan — malware that disguises its true intent. Ransomware typically infiltrates via email, luring a user to click on an attachment or visit a website that infects their computer with malicious code. Common ransomware targets include hospitals, schools, state and local governments, law enforcement agencies, and businesses. Ransomware also targets individual users, holding personal information, photos, or other records.

Identity Theft

According to the FBI, identity theft occurs when someone “unlawfully obtains another individual's personal information and uses it to commit theft or fraud”. Not all identity thefts are a result of cyber-attacks, but malware such as trojans and spyware are often used to steal personal information.

A common method for perpetrating identity theft, phishing refers to a method used by cyber criminals to obtain confidential information using emails or texts. Scammers pose as a trusted source (often a bank or well-known company) and trick recipients into providing personal information, such as account passwords and social security numbers. Phishing messages often use a story—for example, a claim that the sender has noticed suspicious activity with an account—to entice recipients to click a link or open an attachment.

Social Engineering

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. Cyber criminals use social engineering to commit fraud online. Platforms such as online dating sites provide opportunities to initiate conversations with potential victims. Once the criminal establishes a relationship with the target and gains their trust, the criminal asks for money or information. Social engineering techniques are often combined with technology elements. For example, phishing attempts often make use of deceptive and manipulative messaging in addition to malware and fake websites.

Software Piracy

Software piracy is unauthorized reproduction, distribution, and use of software. Pirated software takes the form of counterfeited commercial products and illegal downloads and reproductions, as well as violations of licensing agreements that limit the number of users who can access a program. As much as 37% of software installed on personal computers globally is unlicensed, according to BSA | The Software Alliance. In addition to being illegal, pirated software contributes to the spread of malware, which can be inserted by cyber criminals into unauthorized software copies.