Cyber crimes encompass a wide range of illegal activities carried out using computers and the internet. Some common types include:

1. Identity Theft: Stealing personal information like passwords, credit card numbers, or social security numbers to commit fraud.

2. Phishing: Sending deceptive emails or messages pretending to be from reputable sources to trick individuals into revealing sensitive information or installing malware.

3. Malware: Software designed to damage or gain unauthorized access to computer systems. This includes viruses, worms, ransomware, and spyware.

4. Hacking: Unauthorized access to computer systems or networks to steal, manipulate, or disrupt data.

5. Cyberbullying: Using digital communication to harass, threaten, or intimidate others.

6. Online Fraud: Deceptive practices aimed at tricking individuals or organizations into providing money or sensitive information.

7. Cyber Espionage: Illegally obtaining confidential information from governments, corporations, or individuals for political, economic, or personal gain.

8. Child Exploitation: Using the internet to distribute child pornography or groom minors for sexual exploitation.

9. Denial of Service (DoS) Attacks: Overloading servers or networks with excessive traffic to make websites or online services unavailable.

10. Data Breaches: Unauthorized access to and exposure of sensitive information stored by individuals or organizations.

Combating cyber crimes requires a multi-faceted approach involving technology, legislation, education, and international cooperation. Organizations and individuals should take measures such as using strong passwords, keeping software updated, being cautious with email attachments and links, and staying informed about the latest cyber threats.