# Categorization of Cybercrimes and Prevention Measures

## 1. Hacking

* **Description:** **Unauthorized access** to computer systems to steal or manipulate data.
* **Prevention:**
  + Use strong passwords and multi-factor authentication.
  + Regularly update software and security patches.
  + Implement firewalls and intrusion detection systems.

## 2. Identity Theft

* **Description**: **Stealing personal information** to impersonate someone for financial or personal gain.
* **Prevention:**
  + Avoid sharing personal details online.
  + Use identity theft protection services.
  + Monitor financial and credit reports.

## 3. Online Fraud

* **Description:** Deceptive practices used to **scam** individuals or organizations out of money or personal information.
* **Prevention:**
  + Be cautious of phishing emails and fake websites.
  + Verify sources before making online transactions.
  + Use secure payment methods.

## 4. Cyberstalking and Harassment

* **Description:** Persistent and malicious **online harassment**.
* **Prevention:**
  + Report abusive behavior on social media.
  + Block and avoid interacting with harassers.
  + Maintain privacy settings on social platforms.

## 5. Malware Attacks

* **Description:** Software designed **to harm or exploit computer systems**.
* **Prevention:**
  + Install reputable antivirus and anti-malware programs.
  + Avoid downloading unknown files or attachments.
  + Regularly update security software.

## 6. Distributed Denial of Service (DDoS) Attacks

* **Description:** **Overloading a network** or website to make it unavailable.
* **Prevention:**
  + Use network traffic monitoring tools.
  + Implement DDoS protection services.
  + Use rate limiting and IP blocking mechanisms.

## 7. Eavesdropping

* **Description:** **Intercepting** **private communications** without consent.
* **Prevention:**
  + Use encrypted messaging apps.
  + Secure Wi-Fi networks with strong passwords.
  + Avoid using public Wi-Fi for sensitive transactions.

## 8. Cyber Espionage

* **Description: Gaining unauthorized access to confidential information** for political or financial gain.
* **Prevention:**
  + Use strong encryption for sensitive data.
  + Implement strict access controls.
  + Conduct regular security audits.

## 9. Intellectual Property Theft

* **Description:** Unauthorized use or distribution of **copyrighted or proprietary** content.
* **Prevention:**
  + Use watermarking and digital rights management (DRM).
  + Monitor and report unauthorized use of copyrighted material.
  + Secure intellectual property with legal protections.

## 10. Online Defamation

* **Description:** Spreading false or damaging information online.
* **Prevention:**
  + Report defamatory content to platform administrators.
  + Use legal actions if necessary.
  + Maintain positive online presence and reputation.

## 11. Child Exploitation

* **Description:** Using online platforms to exploit or harm minors.
* **Prevention:**
  + Monitor children’s internet usage.
  + Educate children about online dangers.
  + Report suspicious activity to law enforcement.

## 12. Cyberbullying

* **Description:** Using digital platforms to intimidate, threaten, or humiliate others.
* **Prevention:**
  + Encourage open communication about online experiences.
  + Block and report bullies.
  + Promote awareness campaigns in schools and communities.