## 20 One-Liners to Remember

Quick-fire facts for last-minute revision.

1. **IIBF conducts a Certificate Examination in Prevention of Cyber Crimes and Fraud Management.**
   This is a dedicated banking certification focused on cyber security and fraud awareness.

2. **Inserting a USB loaded with malware into a system is an example of physical hacking.**
   This distinguishes physical access attacks from remote unauthorised access methods.

3. **A firewall is a software or hardware system that controls permission or denial of network access based on set rules.**
   Firewalls are a core security control tested in the cyber crime syllabus.

4. **White-hat hackers work legally, sometimes hired by companies to test their own security systems.**
   This contrasts with malicious hackers who exploit vulnerabilities for criminal gain.

5. **Data theft includes downloading or copying data without the permission of the person in charge of the computer.**
   This is a specific definition tested in the cyber crime exam syllabus.

6 **Cyberstalking means harassing someone through an electronic medium.**

This is distinct from other cyber offences like fraud or virus attacks.

7 **Deceiving or cheating a person using a computer device is punishable under both the IPC and the IT Act.**

Cyber cheating falls under overlapping legal provisions in Indian law.

8 **A keylogger is a special program used for recording and tracking a user's keystrokes.**

This distinguishes keyloggers from other malware types like Trojans, viruses and worms.

9 **Cyber espionage is the practice of gathering sensitive information by using technology to spy on someone.**

This is a distinct category from general hacking or malware attacks.

10 **A cyberattack is an attempt to steal, damage, spy on or destroy computer systems, networks or associated information.**

This is the general definition of a cyberattack tested in the syllabus.

11 **One-time passwords and two-factor authentication both help prevent phishing.**

These security controls add extra verification steps beyond a simple password.

12 **A denial-of-service attack is a concerted effort to prevent a website or service from functioning efficiently.**

This attack targets availability rather than stealing data directly.

13 **Phishing uses special programs to fool individuals into believing traditional security protects them during online banking.**

This deceptive tactic is a major focus area in the cyber crime and fraud syllabus.

14 **Social engineering is a mode of ethical hacking that attempts to access a network using an employee's credentials.**

It exploits human trust rather than purely technical vulnerabilities.

15 **A brute force attack tries to crack a password through repeated, often system-driven, attempts.**

This differs from session hijacking, Trojan horses and rootkits, which use other methods.

16 **Cyber crime is the offence or attack itself, while cyber security is the defence against such attacks.**

This distinction is commonly tested by contrasting examples like phishing versus firewalls.

17 **Examples of cyber crime include phishing, hacking, ransomware and data theft.**

These are offensive actions that cause financial or data loss for victims.

18 **Examples of cyber security controls include firewalls, OTP and two-factor authentication.**
These are defensive measures aimed at protecting, detecting and preventing attacks.

19 **The Information Technology Act and relevant sections of the IPC underpin fraud management law in India.**
Candidates must know which cyber offences are punishable under which law.

20 **Common syllabus traps include confusing a worm with a Trojan, or spyware with a keylogger.**
These similar-sounding malware types have distinct technical definitions tested in exams.