20 True or False

Decide, then check the answer and reason below each statement.

Question 1

IIBF conducts a Certificate Examination in Prevention of Cyber Crimes and Fraud Management.

TRUE

This is the specific certification exam covered by the mock test guide.

Question 2

Inserting a malware-loaded USB into a system is classified as physical hacking, not remote access.

TRUE

Physical hacking involves direct physical contact with the device, unlike remote unauthorised access.

Question 3

A firewall is defined as a system that controls permission or denial of network access based on set rules.

TRUE

This is the standard definition of a firewall in the cyber crime syllabus.

Question 4

White-hat hackers are criminals who hack systems purely for personal financial gain.

FALSE

White-hat hackers work non-criminally and are sometimes hired by companies to test security.

Question 5

Data theft is defined as accessing data with full authorisation from the computer owner.

FALSE

Data theft specifically involves accessing or copying data without authorisation.

Question 6

Cyberstalking means harassing someone through an electronic medium.

TRUE

This is the specific definition tested for cyberstalking.

Question 7

Cyber cheating using a computer or mobile device is not punishable under any Indian law.

FALSE

Cyber cheating is punishable under both the IPC and the IT Act.

Question 8

A keylogger is a program designed specifically to record and track a user's keystrokes.

TRUE

This distinguishes keyloggers from other malware like viruses or worms.

Question 9

Cyber espionage involves using technology to spy on someone and gather sensitive information.

TRUE

This is the specific definition of cyber espionage in the syllabus.

Question 10

A denial-of-service attack aims to steal a victim's password through repeated guessing.

FALSE

A denial-of-service attack aims to disrupt a website or service, not guess passwords; that describes a brute force attack.

Question 11

One-time passwords and two-factor authentication are both listed as ways to help prevent phishing.

TRUE

Both act as additional verification layers against phishing attempts.

Question 12

A brute force attack tries to crack a password through repeated, often automated attempts.

TRUE

This is the standard definition of a brute force attack in network security.

Question 13

Social engineering as a mode of ethical hacking involves exploiting an employee's credentials to access a network.

TRUE

Social engineering relies on human trust rather than purely technical exploits.

Question 14

Cyber crime is defined as the defence against attacks, while cyber security is the offence itself.

FALSE

It is the reverse: cyber crime is the offence, and cyber security is the defence.

Question 15

Examples of cyber crime given in the guide include phishing, hacking, ransomware and data theft.

TRUE

These are listed as examples of the offence side, cyber crime.

Question 16

Firewalls, OTP and two-factor authentication are listed as examples of cyber security measures.

TRUE

These are defensive controls used to protect systems from attacks.

Question 17

The IT Act and relevant IPC sections are described as irrelevant to fraud management in India.

FALSE

The IT Act and IPC sections are described as underpinning fraud management law in India.

Question 18

Confusing a worm with a Trojan is listed as a common mistake candidates make in this exam.

TRUE

The guide explicitly flags this as a common confusion between similar malware terms.

Question 19

The mock test guide recommends skipping questions you are unsure about during practice.

FALSE

The guide recommends attempting every question and making a best guess, just like the real exam.

Question 20

According to the guide, mock tests alone, without conceptual study, are described as the single best way to clear the exam.

FALSE

The guide states mock tests work best when combined with conceptual study and structured revision.