

**CYBER SECURITY  
(INFO 3133)**

**Time Allotted: 2½ hrs**

**Full Marks: 60**

*Figures out of the right margin indicate full marks.*

*Candidates are required to answer Group A and any 4 (four) from Group B to E, taking one from each group.*

*Candidates are required to give answer in their own words as far as practicable.*

**Group – A**

1. Answer any twelve:

**12 × 1 = 12**

*Choose the correct alternative for the following*

- (i) Another name for Patriot Hacking  
(a) Reconnaissance (b) Phreaking  
(c) Digital Warfare (d) None of these.
- (ii) Ping flood is associated with.  
(a) Ping of death attack (b) Nuke  
(c) Teardrop attack (d) Flood attack.
- (iii) Which hacker discloses information about security holes in public?  
(a) White Hat (b) Black Hat (c) Grey Hat (d) Brown Hat.
- (iv) Phishing method that relies on introducing malicious code into websites and E-Mails.  
(a) Dragnet (b) Gillnet (c) Rod and Reel (d) All of these.
- (v) What is the name of the viruses that fool a user into downloading and/or executing them by pretending to be useful applications?  
(a) Cracker (b) Worm (c) Trojan horses (d) Keylogger.
- (vi) Device that makes untraceable activity on the Internet.  
(a) Proxy server (b) Malwares (c) Keyloggers (d) Anonymizer
- (vii) Method in which Phisher identify prospective victims in advance and convey false information to entice them for disclosing personal and financial data.  
(a) Rod and Reel (b) Lobsterpot (c) Gillnet (d) Dragnet
- (viii) Three Ps of Cybercrime.  
(a) Phishing, Pharming and Privacy (b) Phishing, Pharming and Phreaking  
(c) Phishing, Pharming and Phoraging (d) None of these
- (ix) Pharming is used for  
(a) Data hiding (b) Data alteration  
(c) Host file poisoning (d) All of these.

- (x) Which of the following helps in Bluetooth hacking?  
 (a) Blue Scanner (b) Blue Sniff  
 (c) Bluesnarfer (d) All of these.

*Fill in the blanks with the correct word*

- (xi) The written Cyber Defamation is called \_\_\_\_\_.  
 (xii) Information gathering about a prospective victim is called \_\_\_\_\_.  
 (xiii) \_\_\_\_\_ prevents users from accessing a system and the files it contains.  
 (xiv) Boot Sector Virus also known as \_\_\_\_\_.  
 (xv) \_\_\_\_\_ goes alongside phishing and makes the unauthorized emails appear to come from legitimate users or business units.

### **Group - B**

2. (a) Differentiate between Cyberspace, Cybersquatting and Cyberterrorism. *[[CO1)(Analyze/IOCQ]]*  
 (b) Differentiate between Salami attack, Logic Bomb and Software Piracy. *[[CO1)(Analyze/IOCQ]]*  
 (c) Differentiate between Techno-crime and Techno-vandalism. *[[CO1)(Analyze/IOCQ]]*  
**6 + 4 + 2 = 12**
3. (a) Differentiate between Green Hat Hacker, Blue Hat Hacker, Yellow Hat Hacker and Red Hat Hacker. *[[CO2)(Analyze/IOCQ]]*  
 (b) Explain any four Passive attack tools used in Cybercrime. *[[CO2)(Understand/LOCQ]]*  
 (c) Explain the working of Cyberstalking in detail. *[[CO2)(Understand/LOCQ]]*  
**4 + 4 + 4 = 12**

### **Group - C**

4. (a) Briefly explain different types of attacks that occur in mobile phones. Explain any 3 guidelines for implementing mobile device security. *[[CO3)(Understand/LOCQ]]*  
 (b) Differentiate between BlueScanner, BlueSniff, Bluejacking and Bluesnarfing. *[[CO3)(Analyze/IOCQ]]*  
**6 + 6 = 12**
5. (a) Briefly explain different stages of Network attack. Explain any 3 techniques of credit card fraud. *[[CO4)(Understand/LOCQ]]*  
 (b) Explain the working mechanism of Vishing with example. Discuss suitable countermeasures for Vishing. *[[CO4)(Understand/LOCQ]]*  
**6 + 6 = 12**

### **Group - D**

6. (a) Defend the statement "Keylogger attack make system vulnerable". *[[CO4)(Analyze/IOCQ]]*  
 (b) How polymorphic virus infects the system-Explain. *[[CO4)(Understand/LOCQ]]*

- (c) Differentiate between Software Keylogger, Hardware Keylogger and Anti Keylogger. [[CO4](Analyze/IOCQ)]  
**4 + 3 + 5 = 12**
7. (a) Differentiate between Smurf attack and Teardrop attack. [[CO5](Analyze/IOCQ)]  
 (b) Differentiate between DoS, DDoS and PDoS attack. [[CO5](Analyze/IOCQ)]  
 (c) Differentiate between Trojan Horse and Backdoor. [[CO5](Analyze/IOCQ)]  
**4 + 4 + 4 = 12**

### Group - E

8. (a) Differentiate between Phishing and Spambots. Differentiate between Lobsterpot, Drognet and Gillnet. [[CO6](Analyze/IOCQ)]  
 (b) Explain any three types of Computer based Techniques of Identity Theft. [[CO6](Understand/LOCQ)]  
 (c) Differentiate between Whaling and Spear Phishing. [[CO6](Analyze/IOCQ)]  
**6 + 3 + 3 = 12**
9. (a) Briefly discuss the steps of Forensic investigation. [[CO6](Understand/LOCQ)]  
 (b) Define Homograph attack. Explain Geotagging in detail. [[CO6](Understand/LOCQ)]  
 (c) Explain any three tools for Digital Forensic Analysis. [[CO6](Understand/LOCQ)]  
**6 + 3 + 3 = 12**

Cognition Level	LOCQ	IOCQ	HOCQ
Percentage distribution	45.83	54.17	0

#### Course Outcome (CO):

1. Define the concept of Cybercrime, Classify types of Cybercrime and Cybercriminals.
2. Discuss the phases in planning cybercrime, Explain Cyber Stalking and different tools for Active attack and Passive attack.
3. Discuss the security challenges posted by mobile devices, Compare the attacks on mobile/Cell phones and differentiate between techniques of Credit Card fraud. Compare the attacks on Bluetooth technologies.
4. Explain the stages of Network attack, Differentiate between Proxy Server and Anonymizer, Classify password cracking attacks, explain types of Virus and Worms, Differentiate between Trojan Horse and Backdoor.
5. Classify and discuss Denial of Service (DOS) attacks, Explain DDOS attack and discuss SQL injection.
6. Explain Phishing and Identity theft and Discuss steps and tools for Digital Forensic Analysis.

*\*LOCQ: Lower Order Cognitive Question; IOCQ: Intermediate Order Cognitive Question; HOCQ: Higher Order Cognitive Question.*

