Karur Vysya Bank paper 2

1. In a survey of more than 500 companies and government agencies, _____ percent

detected computer security breaches.

A. 20

B. 75

C. 85

D. 99

Answer: C

2. The survey showed that these businesses lost more than _____ due to security

breaches.

A. $100,000 each

B. $377 million

C. five employees each

D. $1 million

Answer: B

3. The typical computer criminal is a(n):

A. young hacker.

B. trusted employee with no criminal record.

C. trusted employee with a long, but unknown criminal record.

D. overseas young cracker.

Answer: B

4. The majority of computer crimes are committed by:

A. hackers.

B. insiders.

C. overseas criminals.

D. young teenage computer geniuses.

Answer: B

5. The common name for the crime of stealing passwords is:

A. spooling.

B. identity theft.

C. spoofing.

D. hacking.

Answer: C Reference: Theft by Computer

6. Collecting personal information and effectively posing as another individual is known as

the crime of:

A. spooling.

B. identity theft.

C. spoofing.

D. hacking.

Answer: B

7. Malicious software is known as:

A. badware.

B. malware.

C. maliciousware.

D. illegalware.

Answer: B

8. A program that performs a useful task while simultaneously allowing destructive acts is a:

A. worm.

B. Trojan horse.

C. virus.

D. macro virus.

Answer: B Moderate

9. An intentionally disruptive program that spreads from program to program or from disk to

disk is known as a:

A. Trojan horse.

B. virus.

C. time bomb.

D. time-related bomb sequence.

Answer: B

10. In 1999, the Melissa virus was a widely publicized:

A. e-mail virus.

B. macro virus.

C. Trojan horse.

D. Time bomb.

Answer: A

11. What type of virus uses computer hosts to reproduce itself?

A. Time bomb

B. Worm

C. Melissa virus

D. Macro virus

Answer: B

12. The thing that eventually terminates a worm virus is a lack of:

A. memory or disk space.

B. time.

C. CD drive space.

D. CD-RW.

Answer: A

13. When a logic bomb is activated by a time-related event, it is known as a:

A. time-related bomb sequence.

B. virus.

C. time bomb.

D. Trojan horse.

Answer: C

14. A logic bomb that was created to erupt on Michelangelo’s birthday is an example of a:

A. time-related bomb sequence.

B. virus.

C. time bomb.

D. Trojan horse.

Answer: C

15. What is the name of an application program that gathers user information and sends it

to someone through the Internet?

A. A virus

B. Spybot

C. Logic bomb

D. Security patch

Answer: B

16. Standardization of Microsoft programs and the Windows operating system has made the

spread of viruses:

A. more complicated.

B. more difficult.

C. easier.

D. slower.

Answer: C

17. HTML viruses infect:

A. your computer.

B. a Web page in the HTML code.

C. both a Web page and the computer that is viewing it.

D. No

18. Software programs that close potential security breaches in an operating system are

known as:

A. security breach fixes.

B. refresh patches.

C. security repairs.

D. security patches.

Answer: D

19. When customers of a Web site are unable to access it due to a bombardment of fake

traffic, it is known as:

A. a virus.

B. a Trojan horse.

C. cracking.

D. a denial of service attack.

Answer: D

20. _____ is the measurement of things such as fingerprints and retinal scans used for

security access.

A. Biometrics

B. Biomeasurement

C. Computer security

D. Smart weapon machinery

Answer: A

21. What is the most common tool used to restrict access to a computer system?

A. User logins

B. Passwords

C. Computer keys

D. Access-control software

Answer: B

22. The most common passwords in the U.S. or Britain include all EXCEPT:

A. love.

B. Fred.

C. God.

D. 123.

Answer: D

23. Hardware or software designed to guard against unauthorized access to a computer

network is known as a(n):

A. hacker-proof program.

B. firewall.

C. hacker-resistant server.

D. encryption safe wall.

Answer: B

24. The scrambling of code is known as:

A. encryption.

B. a firewall.

C. scrambling.

D. password-proofing.

Answer: A

25. If you want to secure a message, use a(n):

A. cryptology source.

B. encryption key.

C. encryption software package.

D. cryptosystem.

Answer: D

26. To prevent the loss of data during power failures, use a(n):

A. encryption program.

B. surge protector.

C. firewall.

D. UPS.

Answer: D

27. A(n) _____ can shield electronic equipment from power spikes.

A. encryption program

B. surge protector

C. firewall

D. UPS

Answer: B

28. All of these are suggestions for safe computing EXCEPT:

A. don’t borrow disks from other people.

B. open all e-mail messages but open them slowly.

C. download shareware and freeware with caution.

D. disinfect your system.

Answer: B

29. Freeware _____ encrypts data.

A. encryption

B. firewall software

C. PGP

D. private and public keys

Answer: C

30. _____ is defined as any crime completed through the use of computer technology.

A. Computer forensics

B. Computer crime

C. Hacking

D. Cracking

Answer: B

31. Most computer systems rely solely on _____ for authentication.

A. logins

B. passwords

C. encryption

D. lock and key

Answer: B

32. Creating strong computer security to prevent computer crime usually simultaneously

helps protect :

A. privacy rights.

B. personal ethics.

C. the number of cookies downloaded to your personal computer.

D. personal space.

Answer: A

33. Over _____ was spent by businesses and government to repair problems in regard

to Y2K.

A. 20 million dollars

B. 100 million dollars

C. 1 billion dollars

D. 100 billion dollars

Answer: D

34. What is a complex system that takes on nearly complete responsibility for a task

eliminating the need for people, verification, or decision making?

A. Autonomous system

B. Missile defense auto-system

C. Smart weapon

D. Independent system

Answer: D

35. Security procedures can:

A. will eliminate all computer security risk.

B. reduce but not eliminate risks.

C. are prohibitively expensive.

D. are inaccessible for the average home user.

Answer: B

ICICI Bank PO Exam 2010 – Computer General Awareness Question Paper 2

Question No. 36 to 58

Fill in the Blank:

36. The field of computer _____ uses special software to scan hard drives of potential

criminal suspects.

Answer: forensics Reference: Online Outlaws: Computer Crime Difficulty: Challenging

37. Computer _____ often goes unreported because businesses fear negative publicity.

Answer: crime

38. _____ connections are the most frequent point of attack for Internet commerce.

Answer: Internet

39. _____ is the most common form of computer crime.

Answer: Theft

40. A survey by eMarketer.com found that _____ are the most often cited online fraud

cases.

Answer: online auctions Reference: Identity Theft

41. Theft of computers is most common for PDAs and _____ computers.

Answer: notebook

42. When you use a disk in several different computers within the same day, you are taking

the chance of contracting a(n) _____.

Answer: virus Reference: Viruses Difficulty: Easy

43. A(n) _____ attaches itself to documents that contain embedded programs that

automate tasks.

Answer: macro virus

44. Both viruses and _____ use computer hosts to replicate.

Answer: worms

45. _____ programs search for and eliminate viruses.

Answer: Antivirus

46. A security patch is a software program that closes possible security breaches in the

operating system. The cost to the consumer is _____.

Answer: nothing or free

47. _____ was once the word used for malicious computer wizardry.

Answer: Hackers or hacking

48. _____ refers to electronic trespassing or criminal hacking.

Answer: Cracking

49. DoS stands for _____.

Answer: denial of service

50. DDoS stands for _____.

Answer: distributed denial of service

51. _____ hijack Web pages and redirect users to other sites.

Answer: Webjackers

52. _____ software monitors and records computer transactions.

Answer: Audit-control

46. A security patch is a software program that closes possible security breaches in the

operating system. The cost to the consumer is _____.

Answer: nothing or free

47. _____ was once the word used for malicious computer wizardry.

Answer: Hackers or hacking

48. _____ refers to electronic trespassing or criminal hacking.

Answer: Cracking

49. DoS stands for _____.

Answer: denial of service

50. DDoS stands for _____.

Answer: distributed denial of service

51. _____ hijack Web pages and redirect users to other sites.

Answer: Webjackers

52. _____ software monitors and records computer transactions.

Answer: Audit-control

53. Each individual who uses a public key cryptosystem has _____ keys.

Answer: two Reference: How It Works: 10.2 Cryptography

54. PGP stands for _____.

Answer: Pretty Good Privacy

55. Most operating systems, including Windows XP, assign each user a unique _____.

Answer: user identifier or user ID

56. It should now be common knowledge that users should not open _____ from e-mail

recipients that the user does not know.

Answer: attachments

57. Match the acts and centers with their purposes:
I. Computer Fraud and Abuse Act A. created by Attorney General Janet Reno in 1998
II. USA Patriot Act B. defines what kinds of communications are legal online
III. Digital Millennium Copyright Act C. created in 2001 as a response to the terrorist attacks
of September 11, 2001
IV. Telecommunications Act of 1996 D. provides instant information on crimes and criminals
V. Communications Decency Act E. declared unconstitutional by the Supreme Court
VI. National Infrastructure Protection Center F. created as a result of the first headlinemaking
worm
VII. National Crime Information Center G. used to arrest a student for writing to crack an
Adobe product
Answers: F, C, G, B, E, A, D
58. Match the following rules of thumb about safe computing with the proper descriptions:
I. share with care A. be aware of e-mail from what appear to be legitimate companies
II. handle e-mail carefully B. don't choose a dictionary word
III. disinfect regularly C. keep your disks in your own computer
IV. take your password seriously D. copy, copy, copy
V. if it's important, back it up E. encrypt
VI. sensitive info over the Internet? F. use antivirus software
Answers: C, A, F, B, D, E