***Technology In Action, Complete, 14e* (Evans et al.)**
Chapter 9   Securing Your System: Protecting Your Digital Data and Devices

1) All of the following are top cybercrimes reported to the IC3 EXCEPT _____.
A) identity theft
B) non-auction scam
C) advance fee fraud
D) malware fraud

2) Which of the following is formally defined as any criminal action perpetrated primarily through the use of a computer?
A) Social networking
B) Cybercrime
C) Phishing
D) Hacking

3) The Internet Crime Complaint Center (IC3) is a partnership between the _____.
A) FBI and the IRS
B) FBI and the CIA
C) FBI and National White Collar Crime Center
D) NRA and the U.S. Department of Defense

4) Government impersonation scams involve _____.
A) people pretending to represent official organizations such as the Dept. of Homeland Security or IRS
B) running auctions that do not exist
C) convincing people to send money as a "good faith" gesture
D) collecting funds and not delivering the goods

5) Creating and distributing _____ is one of the most widespread types of cybercrimes.
A) spam
B) computer viruses
C) cookies
D) zombies

6) Which of the following is NOT a virus category?
A) Worm
B) Logic bomb
C) Macro
D) Pharming

7) All of the following activities may infect your computer with a virus EXCEPT _____.
A) sharing flash drives
B) downloading video files from peer-to-peer sites
C) downloading or running an e-mail attachment file
D) printing a document

8) Which is NOT one of the four key pieces of personal information you should protect from identity thieves?
A) Social Security number
B) Anniversary
C) Date of birth
D) Street address

9) Which type of virus was the famous Michelangelo virus?
A) A worm
B) A time bomb
C) A script virus
D) An e-mail virus

10) A _____ is a virus that is triggered on a certain date.
A) worm
B) macro
C) logic bomb
D) time bomb

11) A(n) _____ takes advantage of file transport methods, such as e-mail, to spread on its own.
A) worm
B) script virus
C) encryption virus
D) macro virus

12) A _____ is a virus that is attached to documents such as Word or Excel files.
A) script virus
B) macro virus
C) polymorphic virus
D) Trojan horse

13) Which of the following classifications of viruses can change its own code to avoid detection?
A) Stealth
B) Multipartite
C) Polymorphic
D) Worm

14) Regarding computer protection, quarantining is defined as _____.
A) updating your antivirus software
B) placing a found virus in a secure area on the hard drive
C) repairing an infected file
D) deleting an infected file

15) A(n) _____ is the portion of virus code that is unique to a particular computer virus.
A) virus signature
B) encryption code
C) compression code
D) virus pattern

16) _____ hackers break into systems legally for non-malicious reasons such as to test system security vulnerabilities.
A) Black-hat
B) Grey-hat
C) White-hat
D) Green-hat

17) A packet analyzer is a program that can enable a hacker to do all of the following EXCEPT _____.
A) use your debit card information to purchase items illegally
B) assume your identity
C) steal your logons and passwords for various accounts
D) launch a denial of service (DoS) attack on your computer

18) A _____ allows a hacker to gain access to your computer and take almost complete control of it without your knowledge.
A) denial of service (DoS)
B) zombie
C) logic bomb
D) rootkit

19) You can block logical ports from invaders and make your computer invisible to others on the Internet by installing _____.
A) a packet sniffer
B) a firewall
C) a packet filter
D) antivirus software

20) _____ floods a computer with requests until it shuts down and refuses to answer any requests for information.
A) A Trojan horse
B) A polymorphic virus
C) A DDoS attack
D) Pretexting

21) In computing, a _____ is named after a housing construction feature that slows the spread of fires from house to house.
A) firehouse
B) firebreak
C) firewall
D) fire extinguisher

22) Configuring a firewall to ignore all incoming packets that request access to a specific port is known as _____.
A) packet filtering
B) packet switching
C) static addressing
D) logical port blocking

23) Rules for creating passwords include all of the following EXCEPT _____.
A) keep your password a secret
B) change your password frequently
C) keep a master password that is the same for all of your accounts
D) use letters, numbers, and symbols in your passwords

24) CAPTCHA is _____.
A) antivirus software
B) a password method
C) the wavy hard-to-read letter and number sequence that you type to prove that you are human to a website
D) a rootkit virus

25) Viruses, adware and spyware are referred to collectively as _____.
A) bloatware
B) grayware
C) alertware
D) firmware

26) _____ is a program that gathers information about your surfing habits without your knowledge.
A) Adware
B) Ghostware
C) Shareware
D) Spyware

27) Which of the following statements about cookies is NOT true?
A) Cookies obtain your personal information by searching your hard drive.
B) Cookies are text files.
C) Cookies help companies determine the traffic flow through their website.
D) Some companies sell the personal information found in cookies to other companies.

28) Social _____ is any technique that uses social skills to generate human interaction that entices individuals to reveal sensitive information.
A) engineering
B) theft
C) pretexting
D) pharming

29) When malicious code is planted on your computer and alters your browser's ability to find web addresses, it is known as _____.
A) phishing
B) pharming
C) pretexting
D) polymorphing

30) Using your computer for non-work activities while you are being paid to work is known as _____.
A) cyberloafing
B) cybersleeping
C) cyberlazing
D) cyberbreaking