Chapter 2: Personal Security

TRUE/FALSE

1. Virtually anyone could type in a person’s username and pretend to be that person.

   ANS: T PTS: 1 REF: 40

2. Passwords are still considered a strong defense against attackers.

   ANS: F PTS: 1 REF: 40

3. The weakness of passwords centers on human memory.

   ANS: T PTS: 1 REF: 40

4. When creating passwords, the most important principle is that length is more important than complexity.

   ANS: T PTS: 1 REF: 54

5. FACTA grants consumers free access to their credit score.

   ANS: F PTS: 1 REF: 57

MULTIPLE CHOICE

1. A ____ attack begins with the attacker creating digests of common dictionary words, and then comparing those in a stolen password file.

   a. man in the middle
   b. brute force
   c. dictionary
   d. hash

   ANS: C PTS: 1 REF: 42

2. ____ is sending an e-mail or displaying a Web announcement that falsely claims to be from a legitimate enterprise, in an attempt to trick the user into surrendering private information.

   a. Pharming
   b. Phishing
   c. Polling
   d. Flashing

   ANS: B PTS: 1 REF: 45

3. Social engineering ____ means to create a fictitious character and then play out the role of that person on a victim.

   a. conformity
   b. impersonation
   c. identity theft
   d. common roles

   ANS: B PTS: 1 REF: 45

4. The average phishing site only exists for ____ days to prevent law enforcement agencies from tracking the attackers.

   a. 1.7
   b. 2.1
   c. 3.8
   d. 4.3

ANS: C PTS: 1 REF: 46

5. Instead of asking the user to visit a fraudulent Web site, ____ automatically redirects the user to the fake site.
a. whaling
b. vishing
c. spear phishing
d. pharming

ANS: D PTS: 1 REF: 47

6. Whereas phishing involves sending millions of generic e-mail messages to users, ____ targets only specific users.
a. whaling
b. vishing
c. spear phishing
d. pharming

ANS: C PTS: 1 REF: 47

7. ____ identify individuals within the organization who are in positions of authority.
a. Phone directories
b. Policy manuals
c. System manuals
d. Organizational charts

ANS: D PTS: 1 REF: 48

8. ____ may reveal the true level of security within the organization.
a. Phone directories
b. Policy manuals
c. System manuals
d. Organizational charts

ANS: B PTS: 1 REF: 48

9. ____ involves using someone’s personal information, such as a Social Security number, to establish bank or credit card accounts that are then left unpaid, leaving the victim with the debts and ruining their credit rating.
a. Identity borrowing
b. Identity theft
c. Information theft
d. Property theft

ANS: B PTS: 1 REF: 49

10. Grouping individuals and organizations into clusters or groups based on their likes and interests is called ____.
a. affiliate marketing
b. affiliate networking
c. social networking
d. social marketing

ANS: C PTS: 1 REF: 50

11. The Web sites that facilitate linking individuals with common interests and function as an online community of users are called ____.
a. social marketing sites
b. affiliate network sites
c. affiliation sites
d. social networking sites

ANS: D PTS: 1 REF: 50

12. ____ means an attacker who pretends to be from a legitimate research firm asks for personal information.
a. Dumpster diving
b. Phishing
c. Stealing
d. Pretexting

ANS: D PTS: 1 REF: 50

13. Stolen wallets and purses contain personal information that can be used in identity theft. This is known as ____.
a. dumpster diving
b. phishing
c. stealing
d. pretexting

ANS: C PTS: 1 REF: 50

14. Using a standard ____ form, attackers can divert all mail to their post office box so that the victim never sees any charges made.
a. mail bouncing
b. forwarding
c. change-of-address
d. mail redirect

ANS: C PTS: 1 REF: 50

15. The best approach to establishing strong security with passwords is to use a ____.
a. password generation program
b. password management tool
c. password fault program
d. password vault program

ANS: B PTS: 1 REF: 51

16. A ____ is a program that lets a user create and store multiple strong passwords in a single user database file that is protected by one strong master password.
a. password management application
b. password generation program
c. password fault program
d. password vault program

ANS: A PTS: 1 REF: 52

17. The ____ of 2003 contains rules regarding consumer privacy.
a. Credit and Transactions Act
b. Fair and Accurate Credit Transactions Act
c. Fair Credit Reporting Act
d. Accurate Transactions Act

ANS: B PTS: 1 REF: 57

18. FACTA grants consumers the right to request one free credit report from each of the three national credit-reporting firms every ____.
a. 2 months
b. 6 months
c. 12 months
d. 18 months

ANS: C PTS: 1 REF: 57

19. If a consumer finds a problem on her credit report, she must first send a letter to the credit-reporting agency. Under federal law, the agency has ____ days to investigate and respond to the alleged inaccuracy and issue a corrected report.
a. 15
b. 30
c. 45
d. 60

ANS: B PTS: 1 REF: 57

20. A ____ is a numerical measurement used by lenders to assess a consumer’s creditworthiness.
a. credit report
b. credit score
c. credit level
d. credit rank

ANS: B PTS: 1 REF: 57

21. Credit score reports cost about ____.
a. $10
b. $15
c. $20
d. $25

ANS: A PTS: 1 REF: 57

COMPLETION

1. A(n) ____________________ is a unique name used for identification.

ANS: username

PTS: 1 REF: 40

2. Technically speaking, the process for creating a password digital representation is based on a hash algorithm, which creates a(n) ____________________.

ANS: digest

PTS: 1 REF: 42

3. ____________________ is a group-based behavior, yet it can be used on an individual by convincing the victim that everyone else has been giving the attacker the requested information.

ANS: Conformity

PTS: 1 REF: 44

4. A(n) ____________________ is a false warning, often contained in an e-mail message claiming to come from the IT department.

ANS: hoax

PTS: 1 REF: 47

5. ____________________ involves digging through trash receptacles to find information that can be useful in an attack.

ANS: Dumpster diving

PTS: 1 REF: 48

MATCHING

Match each term with the correct statement below.
a. Authentication
b. Brute force attack
c. Strong passwords
d. Whaling
e. Password
f. Vishing
g. Shoulder surfing
h. Tailgating
i. Social engineering

1. use of a telephone call instead of e-mail to contact a potential victim

2. one type of spear phishing
3. information entered is observed by another person
4. any secret combination of letters, numbers, and/or symbols that serves to validate or authenticate a user by what she knows
5. trying to guess a password through combining a systematic combination of characters
6. means of gathering information for an attack by relying on the weaknesses of individuals
7. WUuAxB2aWBndTf7MfEtm is an example of this
8. process that confirms a user’s identity
9. once an authorized person opens the door then virtually any number of individuals can follow behind and also enter the building or area

1.	ANS: F	PTS: 1	REF: 47
2.	ANS: D	PTS: 1	REF: 47
3.	ANS: G	PTS: 1	REF: 49
4.	ANS: E	PTS: 1	REF: 40
5.	ANS: B	PTS: 1	REF: 43
6.	ANS: I	PTS: 1	REF: 44
7.	ANS: C	PTS: 1	REF: 54
8.	ANS: A	PTS: 1	REF: 39
9.	ANS: H	PTS: 1	REF: 49

SHORT ANSWER

1. List four characteristics of weak passwords.

   ANS:
   Characteristics of weak passwords include:
   * A common word used as a password (such as tigers). Attackers can use an electronic dictionary of common words to easily discover the password.
   * Short passwords (such as 12345). Short passwords are easier to break than long passwords.
   * Personal information in a password (such as the name of a child or pet). These passwords can be easy to guess or the information can be found on the user’s social networking site.
   * A static password. If a user does not change a password, an attacker who gains access to a device or account will have unlimited access for the foreseeable future.

   PTS: 1 REF: 41

2. Describe phishing.

   ANS:
   One of the most common forms of social engineering is phishing, or sending an e-mail or displaying a Web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrendering private information. The user is asked to respond to an e-mail or is directed to a Web site where they are instructed to update personal information, such as passwords, credit card numbers, Social Security numbers, bank account numbers, or other information for which the legitimate organization already has a record. However, the Web site is actually a fake and is set up to steal the user’s information.

   PTS: 1 REF: 45-46

3. List at least four actions that can be undertaken by identity thieves.

ANS:
The following are some of the actions that can be undertaken by identity thieves:
* Produce counterfeit checks or debit cards and then remove all money from the bank account
* Establish phone or wireless service in the victim's name
* File for bankruptcy under the person's name to avoid eviction
* Go on spending sprees using fraudulently obtained credit and debit card account numbers to buy expensive items such as large-screen televisions that can easily be resold
* Open a bank account in the person's name and write bad checks on that account
* Open a new credit card account, using the name, date of birth, and Social Security number of the identity-theft victim. When the thief does not pay the bills, the delinquent account is reported on the victim's credit report
* Obtain loans for expensive items such as autos and other motor vehicles

PTS: 1 REF: 49-50

4. Briefly describe various shoulder surfing scenarios.

ANS:
Shoulder surfing can be performed in virtually any public location where an individual is asked to enter personal identification. This includes:
* Entering a PIN at an ATM
* Completing a purchase in a store by entering a debit card PIN at the register
* Writing down a Social Security number on a paper form
* Entering a password on a computer keyboard in a coffee shop or airport

Casually observing what is entered can be done from a distance of up to 15 feet (4.5 meters). More sophisticated techniques include using binoculars (such as in a large train or airport terminal) or using small closed-circuit television cameras that are concealed in a book or backpack.

PTS: 1 REF: 49

5. Discuss reasons why social networking sites are popular with attackers.

ANS:
Although using any Web site has risks associated with it, social networking sites can carry additional risks. These risks include:
* Personal data can be used maliciously. Users post personal information on their pages for others to read, such as birthdays, where they live, their plans for the upcoming weekend, and the like. However, attackers can use this information for a variety of malicious purposes. For example, knowing that a person is on vacation could allow a burglar to break into an empty home, the name of a pet could be a weak password that a user has created, or too much personal information could result in identity theft.
* Users may be too trusting. Attackers often join a social networking site and pretend to be part of the network of users. After several days or weeks, users begin to feel they know the attackers and may start to provide personal information or click on embedded links provided by the attacker that loads malware onto the user's computer.
* Social networking security is lax or confusing. Because social networking sites by design are intended to share information, these sites have often made it too easy for unauthorized users to view other people's information. To combat this many sites change their security options on a haphazard basis, making it difficult for users to keep up with the changes.
* Accepting friends may have unforeseen consequences. Some social networking users readily accept any "friend" request they receive, even if they are not familiar with that person. This can result in problem, since whomever is accepted as a friend may then be able to see not only all of that user's personal information but also the personal information of their friends'.

PTS: 1 REF: 51

6. What are some of the characteristics of weak passwords?

ANS:
In addition to the characteristics such as using a common dictionary word, creating a short password, or using personal information in a password, there are two additional characteristics of weak passwords that may be alarming to most users:
* Any password that can be memorized is a weak password.
* Any password that is repeated on multiple accounts is a weak password.

PTS: 1 REF: 52

7. What are some of the features offered by a password management application?

ANS:
Many of these applications include the following features:
* In-memory protection. Passwords are encrypted while the application is running, so even when the operating system performs functions (like caching to disk), it will not reveal any passwords.
* Key files. A key file is a separate unique file that can be carried on a USB flash drive or other similar device. In order to open the password database, not only must the password be entered, but the key file must also be present. This prevents an attacker who obtains the database password from using it.
* Lock to user account. The database can be locked so that it can only be opened by the same person who created it.
* Import and export. The password list can be exported to various formats and new passwords can be imported.
* Password groupings. User passwords can be arranged as a tree, so that a group can have subgroups.
* Random password generator. A built-in random password generator can create strong random passwords based on different settings

PTS: 1 REF: 53

8. What are some of the recommendations for creating strong passwords?

ANS:
The following are general recommendations regarding creating strong passwords:
* Do not use passwords that consist of dictionary words or phonetic words.
* Do not use birthdays, family member names, pet names, addresses, or any personal information.
* Do not repeat characters (xxx) or use sequences (abc, 123, qwerty).
* The password should be a minimum of 12 characters in length. For online accounts that require higher security, such as an online banking account, a minimum of 18 characters is recommended.
* Because attack programs cannot parse passwords as humans can (and see individual words), consider using a longer passphrase (theraininspainfallsmainlyontheplain).

PTS: 1 REF: 55

9. What are general recommendations for recognizing phishing attacks?

ANS:
Although phishing attacks vary, they generally start with the receipt of an e-mail message that claims to come from a reputable source, such as a bank or Web site with which the user has an account. The e-mail message may contain the following:

* Official logos. Phishers often include the logo of the vendor and otherwise try to make the e-mail look like the vendor’s Web site as a way to convince the recipient that the message is genuine. Yet the presence of logos does not mean that the e-mail is legitimate.
* Web links. Phishing e-mails almost always contain a link that the user is asked to click on. Often these addresses are close variations of a legitimate address, such as www.ebay_secure.com, www.e–bay.com, or www.e-baynet.com.
* Urgent request. Most phishing e-mails encourage the recipient to act immediately or else their account will be deactivated or a similar threatening action will occur shortly.

Even if you carefully scrutinize your e-mail messages, it can be difficult to recognize phishing attacks. The best approach is to consider any unexpected e-mail that claims to come from a reputable source as a phishing message.

PTS: 1 REF: 56

10. What are some recommendations for avoiding identity theft?

ANS:
Avoiding identity theft involves two basic steps. The first step is to deter thieves by safeguarding information. This includes:
* Shred financial documents and paperwork that contains personal information before discarding it.
* Do not carry a Social Security number in a wallet or write it on a check.
* Do not provide personal information either over the phone or through an e-mail message.
* Keep personal information in a secure location in a home or apartment.

The second step is to monitor financial statements and accounts by doing the following:
* Be alert to signs that may indicate unusual activity in an account, such as a bill that did not arrive at the normal time or a large increase in unsolicited credit cards or account statements.
* Follow up on calls regarding purchases that were not made.
* Review financial and billing statements each month carefully as soon as they arrive.

PTS: 1 REF: 56