Answers for Phishing: The Quiz

Security Liaison Fall 2014 Meeting

1. Answer: B. — Phishing is an activity of defrauding an online account user of financial information by posing as a legitimate company. In most cases, hackers will create sites similar to legitimate business websites. The fake replica sites trick users into sharing their personal information — such as account numbers, passwords, user names and social security numbers — with hackers. The hackers in turn use the information to gain access to assets and information for their own financial gain. Sometimes they use the information to siphon funds or they sell the information to other criminals for them to siphon fund or use a credit card to purchase goods and services.
2. Answer: C. — Kaspersky Lab reported 37.3 million computer users were targeted by phishing attacks during a one-year period between May 2012 and April 2013. The main targets were Facebook, Yahoo, Google and Amazon.
3. Answer: B. — The technique of phishing was first introduced in detail in 1987. The first use of the word was in 1995 by Jason Shannon of AST Computers. The word is a combination of the words fishing (used because people are baited into sharing their information) and phreaking (a term used for hacking into a telecommunications system to obtain free calls).
4. Answer: C. — While estimates can vary, a branding company estimates that phishing costs US banks and credit card companies $2.8 billion annually.
5. Answer: A. — One of the first companies hit by a phishing attack was AOL. The attack came from a community called warez, which exchanged pirated software. That led to credit card fraud and other online crimes.
6. Answer: False. — Most hackers know how to replicate legitimate logos to trick computer users into willingly and unknowingly giving up their personal information.
7. Answer: True. — Finding information on phishing is as easy as doing a Google search. There are online videos and tutorial on creating fake Facebook pages, email accounts, and ways to effectively solicit information from unsuspecting computer users.
8. Answer: True. — When an account of someone you know is compromised, attackers may also use the contacts or friends lists from the hacked account to phish for more victims. If you get what seems like a strange request from a friend, it is best to ask that friend if he/she sent the request and make sure his/her account has not been compromised.
9. Answer: True. — Many times, people respond to phishing emails because they fear an account is going to be suspended. Sometimes, they respond and provide information even if they do not have an account with the company named in the phishing email.
10. Answer: False. — You are not in the clear if you receive phishing emails and do not respond. It is estimated that more than 1 billion spam email – many which include phishing attacks — flood email boxes each year.

The important thing is to stay vigilant: Do not click on links, download files or open attachments from unknown senders; guard against spam and be wary of links in emails that ask for personal information even if it appears to come from a legitimate business.