**Tutorial 7**

1. Define and explain the following terms:

· Smishing

· Malware

· Pharming

· Vishing

Answer:

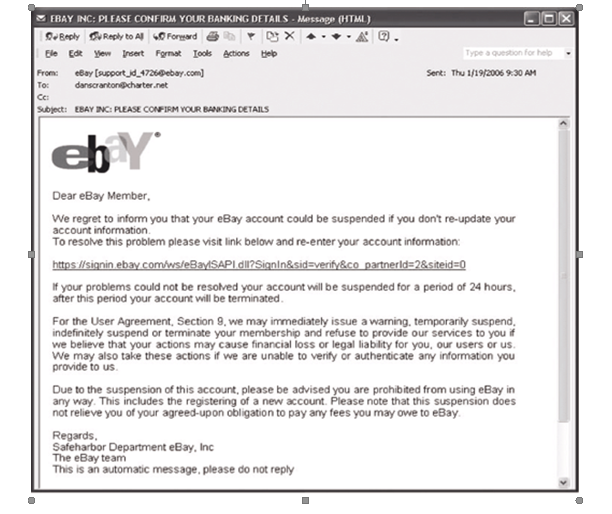
Smishing: When someone tries to trick you into giving them your private information via a text or SMS message.

Malware: collective name for a number of malicious software variants, including viruses, ransomware and spyware

Pharming: Is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent websites without their knowledge

Vishing: A type of message, such as an email, text, phone call or direct-chat message that appears to be from a trusted source, but isn't. To steal someone’s identity and money.

2. Base on the figure below, identify the problem and suggest an appropriate solution.



3. In your opinion, what are the three factors that contribute to a system’s security weaknesses? Do you agree that hiring a white hat hacker can help to improve a company’s security? Justify your answer. (PYQ Aug/Sept 2015/2016)

* Unskilled system user

In fact, 84% of computer security incidents are human related. Sometimes hackers do not need high skill and knowledge in hacking into a system, they just need a gateway which could be provided by the clueless user. They might trick users into downloading or execute some unknown software if the user were not familiar enough with the system.

* Low system development capital

Some of the companies did not pay enough attention to the security features of the system so there will be only a small amount of budget would be assigned for the system development. With low budget, high quality security features could not be developed hence cause the system security weakness that might easily be accessed by the hacker.

* Do not have regular system maintenance

Even with a good quality system security feature, companies still have to execute regular maintenance for the system management and improvement. If the company did not maintain their system regularly, the system security feature would be outdated and easily accessed by the hacker since there was a long period of time for them to hack without any system improvement.

* In my opinion, white hat hackers were important in helping a company find out all the system weaknesses. They have the skill that are capable of spotting all the system problems so that the maintenance team can improve the system furthermore and terminate all of those system loopholes to prevent outside malicious hackers..

4. Dave, a sophomore in high school, is an avid computer fan. He has learned how to program in several languages and spends a good deal of his free time accessing local public bulletin board systems on his father's computer. Dave's father has a computer in their home so that he can work in the evenings and on the weekends when needed. Dave's father has encouraged Dave to learn about computers and has even set up a separate account on CompuServe for his son so that he can play games. Although Dave uses CompuServe occasionally, he has become interested in other private systems.

Inside one of the private systems is a message board where hackers exchange information on their various exploits in attacking other private systems. Dave carefully reads these messages and often writes some, explaining step by step how to access a local power company's system. Dave often jokes about how he knows his father's electric bill before it is even received in the mail. Dave explores other private systems, though he never changes the systems or any of the files available on-line. He simply enjoys the challenge of figuring out how to "crack" systems protection.

Do you agree with Dave actions? Is it ethical or legal for that action? Justify your answer with appropriate explanation.

I do not agree with Dave's actions. Even though Dave does not change the systems or any of the files available online, his action was still violating the act of Computer Fraud And Abuse (CFAA) enacted in 1986 in the United States. Besides that, his action has also gone against the rules of Social Contract Theory, which Dave used to retrieve others data and information to fulfill his self interest. People should not assessed to any of the private confidencial data of other people because this is a very unethical action.

5. Discuss the following different types of hackers:

ü Black hat hacker

ü White hat hacker

ü Grey hat hacker

**Black hat hacker**

-Individual with extraordinary computing skills

-Does destructive work alway

-Use their skill maliciously for personal gain

-hack banks,steal credit cards and defaces websites

**White hat hacker**

-Individual Professional Hacker

-Used for defensive purpose

-Computer security experts and help to protect from black hats

-don't use their skill for illegal purpose

**Grey hat hacker**

-They work for defensive and offensive at their own will

-It is a combination a of white hat hackers and black hat hackers

6. Explain how can the satellite technology help in military warfare? How can the terrorists misuse the satellite technology in the warfare? (PYQ April 2014/2015)

Satellite technology in military warfare provides communication systems,intelligence gathering and navigation.For example,cruise missiles may transmit live video footage or receive updated target information via satellite technology.

On the other hand,the terrorists also misuse satellite technology in military warfare.The terrorists use satellite-data-driven tools such as Google earth to help plan their attacks during military warface.

7. Compare the advancement of computing and communication technologies between today’s war news reporter and the previous generation. (PYQ Aug/Sept 2015/2016)

In the past, war reporters could not get a panoramic view of the war. The process of war can only be recorded through simple shooting techniques and writing, and it takes a long time to mail or deliver it back to let people know the situation of the war. When people see the report, it may not be the latest battle’s situation. Today's war reporters can use drones to take panoramic views of the war. And the reporter can also shoot battlefield videos and edit the electronic version of battlefield reports to send to all parts of the world or online platforms via the Internet anytime, anywhere. People can know the situation of the war in time, and reporters can update the situation at any time.