

Assignment # 3

E-Commerce



Muhammad Ahmer

16fbscsm070

Sir Basit Hassan

**Question 1: Find information on the different methods scammers can use to hijack e-mail account and what a possible defense may be.**

Answer: There are many methods to hijack or hack mail accounts some of them are given below.

**Phishing**:

Phishing is the attempt where we send fake link or clone to user to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.

**Solution:**

* Never click on a link you did not expect to receive.
* Nobody will ever email you randomly offering you money, gift cards, iPhones, puppies etc. unless they are trying to scam you.

**Password Re-use and Weak Passwords:**

If you’re like most people, you probably re use the same password for multiple services so that it’s easy to remember. This is very dangerous because if hijacker will know one of your passwords you are in problem.

**Solution:**

* Use Strong, Unique Passwords for Every Service
* Use two-Factor Authentication

**Ransom-ware:**

Cyber criminals are in it for the money, and what better way to make money than to hold a person’s entire digital life for ransom?

**Solution:**

**Protecting Yourself Against Ransom-ware**

**Update!**

You know this annoying popups on your device asking you to update now? They go a long way to protecting you.

**Anti-Virus**

they do offer extra protection.

**2. What is the process used by the scammer?** How it works: An individual receives an e-mail purportedly sent from a real friend that goes something like this (these come in variations of countries, amounts of currency needed, etc.):

“I’m writing this e-mail in trouble, I came down to London for a program unfortunately, I was mugged at the park of the hotel where I stayed, all cash, credit, and cell were stolen off me but luckily for me I still have my passport with me, I have no access to my account. I have been to the embassy and the police here, but they are not helping issue at all and my flight leaves tomorrow night, but I am having problems settling the hotel bills and the hotel manager won’t let me leave until I settle the bills. I’m freaked out now. I need about £2,250 or any amount you can lend me to sort-out the bills, I will repay you as soon as I get back home.”

How it happened: Hackers hacked into your e-mail accounts, finding who your contacts are and their e-mail addresses. They then sent out an e-mail to you from people on the list. Alternatively, hackers get into your friend’s e-mail account and find that you are one of their contacts. Then they send you the request for help.

**Question 3**: **It looks as if this attack method is very popular. Why it is used so frequently, and why are so many e-mail accounts being hijacked?**

This is the best and easiest of methods to hijack email accounts.

**EMAIL PHISHING SCAMS**

Email phishing is an easy. An attacker sending out thousands of fraudulent messages can net significant information and sums of money, even if only a small percentage of recipients fall for the scam. As seen above, there are some techniques attackers use to increase their success rates.

For one, they will go to great lengths in designing phishing messages to mimic actual emails from a spoofed organization. Using the same phrasing, typefaces, logos, and signatures makes the messages appear legitimate.

In addition, attackers will usually try to push users into action by creating a sense of urgency.

Lastly, links inside messages resemble their legitimate counterparts, but typically have a misspelled domain name or extra subdomains.

This technique is most used in the hijacker because they just have to create only one template and send it thousands of people. If someone will click any of the link available in the spam email. They will lose their credential.