Name: Morgan Parker

Group Number: 20

Group Members:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Part I:** Please read the following **three** cases carefully. For each case, identify ***relevant*** ***security threats*** and recommend a ***security action*** that can prevent or mitigate the threats. (4 points)

**Case 1:** On July 10th, 2006, many Citigroup customers were the victim of a successful security attack. Cybercriminals used multiple attack methods. They first sent emails with links to a fake Citigroup website to customers and asked them to update their account information. The bogus website sits between the real Citigroup website and the customers’ computers and steals the information as consumers entered them. The information was then automatically forwarded to the real bank website and used to access customer accounts.

Security Threats (name two threats):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Security Actions (list one action):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Case 2:** The Love Bug, different from a virus because of its ability to travel independently through networks, flooded the Internet with e-mails in May 2000 with the subject, ILOVEYOU. The body of the deceptive e-mail read, "Kindly check the attached love letter coming from me." When opened, the e-mail wreaked havoc on computers, replicating it automatically, sending copies to everyone in the user's address book. First detected in Asia, Love Bug spread across the world, infecting U.S. government computers at Congress, the White House and the Pentagon. Officials estimated that the worm affected 80 percent of businesses in Australia, and a similar percentage in the United States. Onel de Guzman, who masterminded the worm, which caused billions of dollars in damages, was never charged. Since the release of the bug, Philippine has adopted cyber laws, but Guzman cannot be charged retroactively for his crime.

Security Threats (name one threat):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Security Actions (list one action):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Case 3:** On February 7, 2000,an apparently coordinated attack overwhelmed Yahoo's Web hosting service, which bore the brunt of the attack. Attackers bombard the website with fake packets of information requests. When the targeted server responds, the attackers' system sends more requests. The affected Web site struggles to keep up with the mounting number of requests, slowing performance for users or ultimately crashing the system. At the peak of the outage, which lasted from about 10:30 a.m. PST until shortly after 1 p.m., the Yahoo-directed requests totaled roughly 1 gigabit per second, more information than some Web sites receive in a year, Yahoo spokeswoman Diane Hunt said. "Yahoo is a company that's prepared to handle really high levels of traffic," said Elias Levy, chief technical officer for Internet consulting firm Security Focus. "To be able to take down that network would require a lot of hosts coordinating their actions." In one of the most common forms, an attacker will effectively take over another machine, or a group of machines connected to the Web, and then program these "slave" machines to send streams of information at the target site. Experts say that similar attacks are likely to happen, taking advantage of inherent weaknesses in the Internet's system of open, interconnected networks. No security system will guard against every attack, they say.

Security Threats (name two threats):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Security Actions (list one action):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Part II: Tell phishing sites from safe sites (5 points)**

Below I list **ten** web addresses. Mark them as either ***phishing*** websites or ***safe*** websites. Make sure to not only mark it but more importantly discuss why it is phishing or safe. You do NOT need to include reasons for your choice though.

\_\_\_\_\_\_\_\_\_\_\_\_ <http://202.57.255.177/citizensbank.com/index.php>

\_\_\_\_\_\_\_\_\_\_\_\_ http://www.usbank.com/en/personalhome.cfm

\_\_\_\_\_\_\_\_\_\_\_\_ <http://147.46.236.55/PayPal/login.html>

\_\_\_\_\_\_\_\_\_\_\_\_ <http://www.amazon.com.varzea.us/>

\_\_\_\_\_\_\_\_\_\_\_\_ <http://www.account-process.net/chase/index.html>

\_\_\_\_\_\_\_\_\_\_\_\_ <http://pages.ebay.com/services/forum/feedback.html>

\_\_\_\_\_\_\_\_\_\_\_\_ <http://ebay.com.verification.co.uk>

\_\_\_\_\_\_\_\_\_\_\_\_ <http://www.paypal-ssl.com/>

\_\_\_\_\_\_\_\_\_\_\_\_ <http://ebay-accept.com/login.php>

\_\_\_\_\_\_\_\_\_\_\_\_ <https://www.paypal.com/cgi-bin/webscr>

**Part III: Review and discuss security actions you can take stay safe online (1 point).**

Here is a list of security actions recommended in the Gallaugher chapter. Go over the list together and share your personal experiences. What does each one mean? Do you follow these guidelines? Which ones are you doing well? Which ones would you like to improve?

* Surf smart
* Stay vigilant
* Stay updated with patches
* Install a full suite of security software
* Secure home networks and encrypt hard drives
* Use strong passwords
* Regularly update passwords
* Be disposal smart
* Regularly back up your system
* Check with your administrator.

Identify and describe one thing that most, if not all, group members would like to improve.

Our Medtronic speaker talked about a website haveibeenpwned.com, where you can check whether your email addresses have been compromised in a data breach before. Type in your email addresses and see what it says.