**Anatomy of Attack: Cybersecurity Update 2017**

1. What types of software does the person in the video use to perform her attack? Research the names and techniques you saw briefly presented in the video and explain what they are.
   1. The person in the video used the target companies’ website and Gmail to perform their attack. They simply used social engineering to obtain workers' emails through the website's contact section without unethical intrusion.
2. What is the primary vulnerability in the company that the hacker relies on to succeed? Provide examples of real-world companies that have experienced this type of attack.
   1. The primary vulnerability in the company that the hacker relies on to succeed is that they were able to obtain the information of so many employees through their contact system.
3. What extent of damage was done to the victim? Provide examples of real-world companies that have experienced this type of attack.
   1. Every person who opened the attachment in the phishing email was a victim of the attack. This enabled the ransomware to be installed in the system.
4. What type of cybersecurity expert would likely be properly trained to prevent this attack, and what type of interventions would he or she employ?
   1. During my internship, all emails received on my company email would be flagged whether they originated from inside the company. If not, they would be automatically flagged as an outside email. This is an excellent way to prevent unwanted software from entering the user’s system.

**Running an SQL Injection Attack**

1. What types of application programs are vulnerable to this attack?
   1. Unsecure web programs running on PHP servers that use MySQL databases
2. What type of damage could be done to the victim of this attack?
   1. The victim’s data, such as inventory and logins, could be stolen from their servers and databases.
3. Provide examples of real-world companies that have experienced this attack and what it cost them.
   1. Talk talk (?mispronounced?) experienced this attack using Python scripts.
4. What cybersecurity expert would likely be adequately trained to prevent this attack?
   1. Any expert familiar with Parameterized queries, sanitizing inputs not to allow single quotes, and second-order SQL Queries, for example.

**Credit Card Skimmers**

1. What types of application programs are vulnerable to this attack?
   1. Card readers installed in gas stations could be vulnerable to this attack—specifically the swipe readers.
2. What type of damage could be done to the victim with this attack?
   1. The victim’s credit card information could be stolen; therefore, their funds could be stolen.
3. Provide examples of real-world companies that have experienced this attack and what it cost them.
   1. Nearly every credit provider and gas company has been a victim of this attack.
4. What type of cybersecurity expert would likely be adequately trained to prevent this attack, and what type of interventions would he or she employ?
   1. Preferably an expert trained by someone who has committed the crime. Because someone with real-world experience is teaching them, these experts may know what to look for when pursuing these scams.

**WIFI-man in the middle attack**

1. What types of application programs are vulnerable to this attack?
   1. Every program that connects to the internet is vulnerable to this attack.
2. What type of damage could be done to the victim with this attack? Provide examples of real-world companies that have experienced this attack and what it cost them.
   1. In this example, the victim could have their login information stolen depending on the media the victim is trying to log into. Because using the same passwords for all accounts is expected, the victim could lose more than just their social media login.
3. What type of cybersecurity expert would likely be properly trained to prevent this attack, and what type of interventions would he or she employ?
   1. In this scenario, the intelligent thing to do is not to use the free wifi in public spaces. Using a personal hotspot, say one on a smartphone, would be beneficial.

**How Target could have prevented customer data hack**

**Dissecting the Target breach**

1. What types of data were the attackers trying to steal?
   1. Credit card information was the main target (no pun intended)
2. What preventative measures could have been done to prevent the attack?
   1. The exploited vulnerabilities could have been mitigated by:
      1. Scanning with any antivirus
      2. Check for removal of autorun keys
      3. Disabling external FTP access
3. Enumerate the damages the company suffered-financial, reputation, customer relationships, and legal
   1. It is estimated that Target lost over 200 million dollars, including an 18 million dollar settlement.
   2. Target’s reputation tanked in the following quarter, with profits falling nearly 50%
   3. In 3 years, Target’s CEO and other employees lost their jobs, including 140 lawsuits.

**Yahoo’s data breach explained**

**How Yahoo was hacked**

1. What types of data were the attackers trying to steal?
   1. Attackers stole account names, email addresses, phone numbers, birthdates, hashed passwords, and security questions and answers from over half a billion users.
2. What preventative measures could have been taken to prevent the attack?
   1. Yahoo could have simply asked users to change their passwords when they discovered their data had been breached.
3. Enumerate the damages the company suffered financially, reputation, customer relationships, and legal.
   1. To begin with, Yahoo had to file for bankruptcy, they lost everything.
   2. Reputation-wise, nobody wanted to use Yahoo after the data breach news surfaced.
   3. Legally, Yahoo is close to ending their payout for their class action lawsuit for the data breach victims.