**Part 1 - Cyber Attack Methods**

**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.**

StartPage search engine: “world’s most private search engine,” tried to stay on the down-low.

Facebook: the one place on the internet where everybody puts *way* too much information.

Employ.net: Scoped the rest of the employees of Qualicart to find targets and get info, such as signature format.

Domain Registry: Made a website similar to Qualicart with one misspell, and set up a fake account that looked very familiar to the boss’ email.

“MalwaresRUs”: Downloaded a Malware kit and embedded attachment into emails.

Gmail: used to deliver the payload to unsuspecting victims.

Tor Browser: Onion layer security that is hard to track

**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.**

Human error missing the details + people share too easily: Everything down to the company signature was perfectly mimicked to perform this attack. Without someone taking the bait, the company would have remained unaffected.

**What extent of damage was done to the victim? Provide examples of real-world companies that have experienced this type of attack.**

The company suffered heavy losses paying for the ransom to avoid negative press, and proceeded to get negative press anyway. This was because the attackers STOLE all the information and released it! The CEO had to take the fall, and many lost their jobs.

A real-world example of this is:

On August 25, the cybersecurity company Group-IB published a report detailing a months-long phishing campaign that has compromised at least 130 companies, including Cloudflare, Doordash, Mailchimp, and Twilio.

**What type of cybersecurity expert would likely be properly trained to prevent this type of attack, and what type of interventions would he or she employ?**

The most trained cybersecurity expert would most likely be a former scammer/hacker. The reason for this is they look at the fine details and exploit them, by any means necessary. This is not something you can simply learn in school by doing assignments.

When it comes to preventing this attack, it is important to deal with a few key issues: the first one being human error. Some intervention can include a restriction to downloading/opening files, more company-wide policy on security, hiding access of critical information from those who do not need it, or providing incentive for discovering phishing attempts.

*“Running an SQL Injection Attack - Computerphile”*

**What types of application programs are vulnerable to this attack?**

MySQL, PostGreSQL, SQLServer especially with wildcards.

**What type of damage could be done to the victim with this attack?**

Catastrophic damage! Any command can be ran, and all information from your users can be obtained illegally.

**Provide examples of real-world companies that have experienced this type of attack and what it cost them.**

The largest SQL injection attack to-date was on Heartland Payment Systems in 2008. The SQL injection gained access to credit card processing systems.Although the attack began in March, 2008, it wasn’t discovered until January, 2009. The company was unable to do business for 5 months afterward and was fined $145 million as compensation for fraudulent payments made.

**What type of cybersecurity expert would likely be properly trained to prevent this type of attack, and what type of interventions would he or she employ?**

Update your database management software. Enforce the principle of least privilege (PoLP), which means each account only has enough access to do its job and nothing more. Use prepared statements or stored procedures.

*“Credit Card Skimmers”*

**What types of application programs are vulnerable to this attack?**

Gas station pumps, credit card swipers, skimmers installed on any card reader.

**What type of damage could be done to the victim with this attack?**

Sell your credit card number, clone your credit card, buy tanks of gas with your credit card.

**Provide examples of real-world companies that have experienced this type of attack and what it cost them.**

Gas stations experience this type of skimming all the time. It is estimated to be a $10 million dollar industry to siphon gas with stolen credit cards alone!

**What type of cybersecurity expert would likely be properly trained to prevent this type of attack, and what type of interventions would he or she employ?**

Any routine maintenance guy can spot a skimmer if they look around for one. Routine checks and alarms can prevent this type of attack from getting out of hand.

*“WIFI – Man in the Middle Attack”*

**What types of application programs are vulnerable to this attack?**

Computers automatically attempting to reconnect to wifi networks. A wireless router can intercept the signal and pretend to be said wifi network.

**What type of damage could be done to the victim with this attack? Provide examples of real-world companies that have experienced this type of attack and what it cost them.**

All of the victim's Internet traffic flowing through the hacker's router such as e-mail, instant messages and browser sessions are easily viewed or even modified by the hacker. An example of this is that Hackers pulled off an elaborate man-in-the-middle campaign to rip off an Israeli startup by intercepting a wire transfer from a Chinese venture-capital firm intended for the new business.

**What type of cybersecurity expert would likely be properly trained to prevent this type of attack, and what type of interventions would he or she employ?**

If you aren't actively searching to determine if your communications have been intercepted, a Man-in-the-middle attack can potentially go unnoticed until it's too late. Strong WEP/WAP Encryption on Access Points prevents unwanted users from joining your network just by being nearby. Forcing HTTPS can also prevent the attacker from having any use of the data.

**Part 2 – Three Cyber Attack Cases**

*“How Equifax Got Hacked”*

**What types of data were the attackers trying to steal?**

Private records of 147.9 million Americans along with 15.2 million British citizens and about 19,000 Canadian citizens were compromised in the breach, making it one of the largest cybercrimes related to identity theft.

**What preventative measures could have been done to prevent the attack?**

The data breach into Equifax was principally through a third-party software exploit that had been patched, and Equifax failed to update their servers with it. Further faults were later identified in Equifax’s system, including: insecure network design which lacked sufficient segmentation, inadequate encryption PII, and ineffective mechanisms for breach detection.

**Enumerate the damages the company suffered—financial, reputation, customer relationships, and legal.**

Following the announcement of the breach, Equifax's actions received widespread criticism for how it was handled. On top of failing to protect all of it customers, Equifax did a subpar job of notifying them if and what information was compromised. Legal battles with the FTC ensued, resulting in a settlement that included $300 million to a fund for victim compensation, $175 million to the states and territories in the agreement, and $100 million to the CFPB in fines.

*“Dissecting the Target Breach”*

**What types of data were the attackers trying to steal?**

Cybercriminals were able to steal 40 million credit and debit records and 70 million customer records.

**What preventative measures could have been done to prevent the attack?**

If Target had properly segregated its network, it would have been much harder for a cyber-attack of this magnitude to have occurred.

**Enumerate the damages the company suffered—financial, reputation, customer relationships, and legal.**

The estimated cost of Target data breach goes well beyond the $18 million settlement. In fact, it’s estimated the company lost over $200 million. Following the holiday season, customers were wary, and news of the data breach swiftly spread. Reportedly, earnings fell 46% for Target following the attack, with far fewer households shopping at Target after the breach. Target had to do work to restore its public reputation.

*“How Yahoo Was Hacked”*

**What types of data were the attackers trying to steal?**

Names, email addresses, telephone numbers, encrypted or unencrypted security questions and answers, dates of birth, and hashed passwords.

**What preventative measures could have been done to prevent the attack?**

Yahoo! needed to invest in cybersecurity earlier. This is unfortunately a case of “too little too late”. Despite this, a large proportion of the data could have been protected by communicating to their user base and asking for simple password resets. However, they opted not to do this, as they feared it would annoy users and cause them to switch services.

**Enumerate the damages the company suffered—financial, reputation, customer relationships, and legal.**

The Internet service company Yahoo! was subject to the largest data breach on record. They have been criticized for their late disclosure of both the breaches and their security measures, and they are currently facing several lawsuits as well as an investigation by members of Congress. The breaches impacted Verizon Communications's July 2016 plans to acquire Yahoo! for about $4.8 billion, which resulted in a decrease of $350 million in the final price on the deal closed in June 2017.