Jykeim Giddens

01/03/2022

CyberCriminology

What do Social Scientist know about Ransomware?

Introduction

Technology is the forefront of today's 21st century. There are so many technological advances that has shaped our future for the better. We can do so many things in a much more convenient way such as grocery shop without being in a store, order food without being at a restaurant, and contact people in other forms than the standard text/call which is done via social media. I want you to think about how often you use a phone/tablet or computer to complete your daily task. The average American spends about 5 to 6 hours a day on their smartphones, 1/3 of that is probably spent via internet. People that engage with the internet daily probably do not realize how much valuable information that they are sharing with websites and companies due to the lack of information being taught about the internet. This leads me to my main topic which is Ransomware. Yes, this just what it sounds like, someone taking your money for ransom…. well, this is not exactly the case.

Malicious Activity

What is Ransomware? This is a malicious piece of software that prevents you from gaining access to any critical files or systems on your computer or personal devices. In addition to you not being able to access your personal device, it requires you to pay some sort of ransom (money) to be able to access your device. Usually, the payment is in a form of cryptocurrency so an individual that created the Ransomware cannot be traced back to his origin. Who creates the Ransomware? High level hackers are the individuals that create these malicious programs. They seek to gain a monetary value from companies or people that have something to lose. For instance, a company that has a "secret formula" or banking institutions that need to access people's bank accounts have a higher risk of obtaining Ransomware because they have something to lose and that could inhibit them from receiving business or losing their reputation.

Defense against Ransomware

In the first article, *It's easier to defend against ransomware than you might think, author and research assistant of Systems Security Lab, Northeastern University (2016)* discusses against defending against a ransomware attack. Initially he describes that with the advance features in cryptosystems it is deemed nearly impossible to recover files from a ransomware attack without fully paying the ransom. Although, it is harder to recover from an attack, he mentions that it is much easier to defend against a ransomware attack with some simple solutions. One solution is performing back-ups regularly to an offsite cloud storage such as AWS and other cloud services. In a case that you are a victim of ransomware you do not have to pay the ransom because you know you have all your important files stored in another location with easy access to them.

Scholars such as *Scott Shackelford Associate Professor of Business Law and Ethics*, and *Megan Wade Master of Public Affairs Candidate in Information Systems, Indiana University* discusses other potential ways on how we should be dealing with Ransomware attacks. They talk about approaching ransomware situations as if it were actual people being held hostage. These situations are highly distinct between each other, but they do hold one thing in common which can be negotiation. The authors of this article insist that negotiating with cybercriminals in a manner that you would do a criminal holding a hostage is vital to helping the organization or person. Negotiating can help extend payment deadlines, or maybe even lower the ransom. Again, the main objective of a ransom attack is to get a monetary value. If you can at least negotiate a reasonable price in a reasonable time, it could help you save money and time in the end. The authors also presume that there will be risks associated with trying to resolve a ransomware attack. People that refuse to negotiate with cybercriminals often end up paying more than what the ransom initially asked for. The state of Canada has managed to lower their ransomware attack payments by 55% just through negotiations alone.

Ransomware and the public sector

Ransomware can also occur in public settings such as school systems. This has been a popular target since most public schools do not spend enough time on the concept of cybersecurity. According to the author *Nir Kshetri, Professor of Management University Of North Carolina Greensboro*, cyberattacks that involve ransomware have doubled between spring and fall of 2020. One of the most recent cyber-attacks was in Fairfax County, Virginia. Public schools are not as highly prepared for cyberattacks compared to other government and private organizations. They do not have the necessary funds to pay for what the Ransom that is being requested. There are not many staff that are trained in technology other than what they use to teach their material. Public schools are also a primary target for Ransomware due to the vast amount of children's data that they can receive. Most cyber-actors target children because it is harder to identify when a child has been hacked or data is being used maliciously.

As stated previously, there are many solutions to help you prepare for a Ransomware attack, but it merely impossible to overcome once you are a victim. Computers used to be the main source for Ransomware attacks, but now that data has been able to be more portable digitally, it has begun to spread to other devices such as MacBook's, mobile cell phones, and IoT devices such as smartwatches along with smart home devices. Author *David Glance, Director UWA Center for Software Practice, The University of Western Australia* illustrated the ransomware attack for mobile phones called a locker ransomware. It works the same as most ransomware but just more specifically for mobile phones. Most of our modern-day devices that are connected to the internet can be a victim of a Ransomware attack or any cyber-attack.

Author *Michael Axeslean Lecture (Business Information Systems), The University of Queensland* discusses the benefits between paying or not paying the ransom caused by the malicious software Ransomware. He discusses the importance between having a plan that involves paying the ransom and a plan that does not pay the ransom. He iterates that paying the ransom could just keep encouraging the cyber actor to continue using ransomware on your systems because you will be more prevalent to paying them then paying for security for your systems.

Overview and Protection against Ransomware

Overall, the goal of ransomware is to protect your systems and your privacy. Being more vigilant of important websites and links will help ensure that you do not become a victim to ransomware and other cyber-attacks. You must be able to determine the cost-benefit analysis when dealing with Ransomware in a private and public organization. When deciding not to pay a ransom, you must determine if it is worth losing all your data. If you have cloud services, where your data is being repeatedly backed-up then you may be able to afford to not pay the ransom and move to your cloud services to retrieve all your data. The main thing to remember is to prepare for ransomware attacks. These attacks do not happen unless you activate them. People are the number one cause for cyber attacks followed by bad security habits. The goal to remember is to be vigilant on the internet and take precaution. Implementing good security practices is vital to defend against ransomware. There are numerous incident response organizations that can help you recover your data as well.

References

Amin Kharraz Research Assistant. (2021, December 22). *It's easier to defend against ransomware than you might think*. The Conversation. Retrieved January 4, 2022, from https://theconversation.com/its-easier-to-defend-against-ransomware-than-you-might-think-57258

David Glance Director of UWA Centre for Software Practice. (2018, July 10). *Holding our devices hostage. can we stay safe against the threat of ransomware?* The Conversation. Retrieved January 4, 2022, from https://theconversation.com/holding-our-devices-hostage-can-we-stay-safe-against-the-threat-of-ransomware-45869

Micheal Axelsen Lecturer (Business Information Systems). (2021, February 1). *When it comes to ransomware, it's sometimes best to pay up*. The Conversation. Retrieved January 4, 2022, from https://theconversation.com/when-it-comes-to-ransomware-its-sometimes-best-to-pay-up-78036

Nir Kshetri Professor of Management. (2021, October 28). *K-12 schools need to take cyberattacks more seriously*. The Conversation. Retrieved January 4, 2022, from https://theconversation.com/k-12-schools-need-to-take-cyberattacks-more-seriously-151976

Scott Shackelford Associate Professor of Business Law and Ethics; Director, & Megan Wade Master of Public Affairs Candidate in Information Systems. (2021, December 22). *Deal with ransomware the way police deal with hostage situations*. The Conversation. Retrieved January 4, 2022, from https://theconversation.com/deal-with-ransomware-the-way-police-deal-with-hostage-situations-129213