What is Ransomware?

Something that has plagued computers in recent times would be Crypto Ransomware. Typically, if a criminal wanted to force a victim to give them money they would try and take something precious from them. This can be either a loved one, an expensive item they own, or something with sentimental value. They would then force the victim to pay a substantial fee in order to get that special someone or item back. However, like most crimes in the modern age, computers help make this easier and happen more often. What makes Crypto Ransomware unique is that it is a type or malware, otherwise known as malicious software, that can corrupt important files in a victim's computer. Once this malware is on the computer the victim cannot do anything about it, all they will see is a bunch of gibberish where text should be. The only thing they can do is pay the Ransomware a substantial fee (typically in bitcoin), and they would be able to decrypt their files. This tactic is something that plagues many innocent people everyday, but how does Ransomware work? How can someone prevent this from happening to them?

In a nutshell, crypto ransomware is malware, which basically means that it is a type of software that disrupts or damages the computer and it’s files. However, how does ransomware get onto the computer? Most people download this malware from suspicious email attachments or they downloaded something off of the web and that just so happened to be this ransomware. Most common Crypto Ransomware will sink it’s teeth into the most important files on your computer and corrupt them by either restricting access from the user or encrypting them so they cannot be read. Once downloaded, there is not much the victim can do since their files are permanently damaged now, they can either wipe their computer clean and restart or pay the fine that is being requested. The only way to stop ransomware is by preventing it from being downloaded in the first place.

There are many examples of real ransomware that everyone needs to be aware of. One famous and recent ransomware is Ryuk, which is spread primarily through emails, this malware is one of the most expensive ransomware you can get, with some computer owners having to pay around $300,000 in order to get their system back.

Another example of a dangerous ransomware is WannaCry, which in total took around 4 billion dollars from innocent computer users and cooperations. In fact, this ransomware has infected many multi-billion dollar corporations such as FedEx, Nissian, and Renault. All of it's attacks were done through email phishing. The final example is the first ransomware recorded, AIDS Trojan. This malware, originating in 1989, was distributed via floppy disks and sent to various companies. This ransomware was a bit on the weaker side when it came to corrupting your data, but they did ask for around $189 for each attack. Interestly enough, they asked to be mailed the money, specifically for the money to be sent to a mailbox in Panama.[5] As you can see ransomware is something that is very real and very dangerous, with most ransomwares asking for a huge amount of money. Also it is shown that ransomware not only attacks innocent users but they also try to attack large corporations as well, in fact that is where most ransomware get their money since they know that the data the corporation's hold are extremely important and they have a large amount of money.

The best way to prevent downloading ransomware is never click on unverified links. Be cautious when browsing through the internet and only download software from legitimate sites. Spam emails can also contain malicious attachments that can infect your computer. A common practice to prevent ransomware attacks is to filter and scan content on your mail server. This can reduce the amount of spam email a person sees in the first place thus reducing the chance of downloading malicious attachments. Keeping your computer updated is another way to prevent ransomware attacks. Outdated systems are the most common target for ransomware attacks. By keeping your computer updated you will have the most recent security patches and lower the chance of being infected with ransomware. Lastly, backup your computer periodically is an effective way to ensure you still have access to important data even if your computer is infected with ransomware. Preventing ransomware attack sounds very simple on paper but it's hard to do in practice. Less than 50% of computer users backup their data more than once a year, and 24% of the users never backup their data.[2]

Now that we've covered how to prevent ransomware attacks. What if your computer is already infected with ransomware? The first thing to do is to isolate the infected computer from all networks so the ransomware doesn't spread to other

devices. And then you should turn off all other devices that could potentially be infected to minimize the damage. The best advice to give is never pay the price that you are asked, it is exactly what the criminal wants. Always remember to stay safe when online and use common sense when browsing the internet.

1. Kaspersky. “Tips on How to Prevent Ransomware Attacks.” *Usa.kaspersky.com*, 11 June 2020, https://usa.kaspersky.com/resource-center/threats/how-to-prevent-ransomware
2. Holst, Arne. “U.S. Computer Owners: Data Backup Frequency 2018.” *Statista*, 2 Mar. 2020, https://www.statista.com/statistics/881125/us-data-backup-frequency/
3. “Security Tip (ST19-001).” *Cybersecurity and Infrastructure Security Agency CISA*, https://us-cert.cisa.gov/ncas/tips/ST19-001
4. Fruhlinger, Josh. “Ransomware Explained: How It Works and How to Remove It.” *CSO Online*, CSO, 19 June 2020, https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html
5. “7 Real and Famous Cases of Ransomware Attacks.” *Gatefy*, https://www.gatefy.com/blog/real-and-famous-cases-ransomware-attacks/.