Don’t Let Ransomware Hold Your Computer Hostage

Picture this: it’s Monday morning, and after a relaxing weekend filled with healthy binges of Netflix, Disney+, and Chinese takeout, you are energized and ready to get your workday started. After a quick sip of coffee and a bite of your favorite bagel, you open your laptop only to find this on your screen:

Stunned, you force a reboot. But once again, you see the screen is unchanged and, to make matters worse, you have even less time to pay the fine. Frantic now, you know your only option is to contact the Office of Cybersecurity, but honestly, what are you supposed to say? You have no idea why this ransom message is displaying on your computer screen. How could this have happened to you?

Chances are, you have been the victim of a ransomware attack and, believe it or not, you are not the only one. In fact, ransomware attacks have risen by 13 percent in the past five years, with an average cost of $1.85 million per incident. In the first half of 2022, there were an estimated 237 million attacks worldwide. There is also the fact that ransomware operators continue to aggressively target the US Healthcare sector, with two groups (Royal ransomware & BlackCat ransomware) being some of the most nefarious. The result of this is that according to Cybercrime magazine the Healthcare industry is estimated to spend $125 billion dollars on Cybersecurity from 2020 to 2025.

Crazy, right?

As its name suggests, ransomware is a form of malware (malicious software) that prevents users from accessing their files or device and demands payment before access will be granted again. Ransomware does not discriminate – everything from mom-and-pop shops to Fortune 500 companies to students gearing up for prom are at risk.

Ransomware affects everyone. In fact, the above screenshot is an actual example of a case of ransomware (or locker ransomware) known as “Money Pac” in which hackers impersonated the FBI and locked computers out of basic functions alleging user engaged in “illegal activity.” This locker ransomware instructed victims to unlock their computers, but the catch was they couldn’t use their own debit or credit card. Instead, they had to buy a “Money Pac” card, load it with $300, then enter the information on the locked computer. Once this was done, the computer

would often remain locked, the hackers would have the money, and the trail was pretty much untraceable.

Sadly, even schools have been hit by ransomware criminals – in March 2023, the Minneapolis Public Schools district announced that hackers obtained highly sensitive documents on schoolchildren and teachers, including behavioral records and social security numbers, and were demanding $1 million. There was also a recent case with the Maryland Department of Health where perpetrators attacked the agency's computer system and demanded payment from the state.

Perhaps one reason why DCH is so adamant about regular cybersecurity training is because ransomware attackers often utilize phishing techniques to gain access to an environment – they target a specific user's computer to gain access to an entire network. And as was illustrated in the "Money Pac" example, cybercriminals don't always hold up their end of the bargain once the money is paid.

It's worth noting that, in addition to locker ransomware such as "Money Pac," there is also crypto ransomware that encrypts valuable files on a system, essentially taking data hostage until you pay a ransom. An example of this is "WannaCry," which targets Windows operating systems and demands payment in the form of Bitcoin.

So, rewinding back to your not-so-typical Monday morning, what can you do to avoid a similar "hostage situation" in the future?

1. Avoid opening suspicious emails or links. If in doubt about an email's legitimacy, utilize "PhishAlarm" or contact the Office of Cybersecurity. Most ransomware is spread through phishing scams, so staying diligent in your inbox is your first line of defense.
2. Ensure you are up to date on security patches. This is why it is critical that you are connected to PulseSecure VPN when you are working remotely, as you will not receive these vital patches otherwise.

3. Most important: NEVER PAY A RANSOM. It only emboldens the criminals behind these scams. If you are a victim of an attack, contact the Office of Cybersecurity (DCHOIS@dch.ga.gov) immediately.

Cybersecurity defense is a team sport, and by doing your part, you can help ensure that the agency and the State of Georgia stay safe – and that your Monday mornings remain ransom-free!