Ransomware: The Modern Equivalent Of Being Tied To Train Tracks

When we think of ransom, we typically think of a black-and-white movie with a kidnapper leaving notes made from a variety of newspaper cuttings. Today, ransom is much less melodramatic, much more common and targets something you might not expect: your computer files.

In late 2013, the ransomware threat was added to the list of things that can kill your computer alongside bugs and crashes. Hackers made a new bug that's capable of taking over a computer, encrypting all its files and displaying a brief message demanding money to decrypt them. Sometimes, affected companies or individuals would pay up, the hacker would decrypt the computer as promised and everyone would be on their merry way. Victims would sometimes refuse to pay the fees in the given time and would then lose their valuable files forever. And sometimes, victims would fork over the cash, only to have the hackers disappear with the files still locked and therefore as lost as before the victims paid up.

One study estimates that in its first 100 days as a scheme, ransomware infected 250,000 computers. It earned the hackers a collected $6 million in bitcoins. If that trend continued, we can expect that they've hacked at least 24 million computers in the past two years. including one major hospital that reportedly forked over $17,000 to get its files back.

The original operator of ransomware, Cryptolocker, was shut down in May of 2014. Still, many ransomware copies arose shortly after and continues to wreak havoc. The program continues to evolve, now locking computers and displaying menacing countdowns to create a heightened sense of urgency to pay up.

The question now, of course, is what you should do to protect yourself. For starters, if the only computer you have to worry about is a private computer, ransomware is a less significant risk. Ransomware scammers tend to target computers of companies that have the capability to hand over large sums of money. If your computer handles the larger functions of a company, there are still some steps you can take to protect yourself.

1.) Don't trust online solutions

For starters, there are many software programs that promise to completely rid your computer of ransomware, but those are best left on the virtual shelf. Ironically, some of those alleged file-saving downloads are actually ransomware in disguise. Your best bet is to backup your files however you can – onto an external hard drive, onto a separate computer or even on paper. Anything you do will ensure that, when the hackers come, you'll already have those encrypted files elsewhere. It's advisable to check at least once a month to ensure everything you need is safely backed up.

2.) Hold onto your money

While it might seem like the only option that gives you a chance to get your files back, the FBI has issued a statement asking people not to pay such ransoms. If hackers are paid, they have more incentive to continue, and payment really doesn't influence whether they decrypt your files or not. "The FBI does not condone payment of ransom, as payment of extortion monies may encourage continued criminal activity, lead to other victimizations, or be used to facilitate serious crimes," as FBI Special Agent Christopher Stangl elaborates in an interview. If you're desperate for your files, paying may seem like the only option, but consider the difference that could be made if no one paid them anymore. Crime syndicates would be stopped without any work from the FBI.

3.) Call the cops, but don't hold your breath

Many are currently asking whether anything significant has been done by the FBI to this point. This includes Sen. Ron Wyden, who wrote to James Comey, the director of the FBI, to ask how the agency intended to clean up the ransomware problem. Comey responded that they were making progress, but pointed out that making arrests wasn't

easy as “most of the top cybercriminal actors are located outside of the United States.” Still, he went on to assure Wyden that, “The FBI is committed to following the money in investigating all crimes with a financial component; ransomware is no exception.”

4.) Back up and stay safe

While the FBI has its best men on the task of catching these cyber culprits, it’s your responsibility to be as safe as possible until they do. Back your files up. Don’t click on any sketchy-looking links. Buy security that a trusted provider assures you is safe. Ransom is no longer a thing of black-and-white movies; but in the digital age, it’s still our job to protect ourselves.

SOURCES*:

http://www.bankinfosecurity.com/blogs/please-dont-pay-ransoms-fbi-urges-p-2120?rf=2016-05-05-eb&mkt_tok=eyJpIjoiTnpnMVlUTmxPRFpoWVRRMSIsInQiOiJub1IxSlpyaUtcLzZEMHNFdlA1R25MYzdHVUdMakZGckdqc1BYY0VFb25BZnZcLzdXVnJ6SE9hUStnZ0xpamluNHd5RU5PYkJhdDFaT1dGdzYzZFwvODRVZzFHT0dxeWxFM00xXC9HMksxcU9nK1E9In0%3D

http://www.usatoday.com/story/news/nation/2014/05/14/ransom-ware-computer-dark-web-criminal/8843633/

http://www.pcworld.com/article/2901672/how-to-prevent-ransomware-what-one-company-learned-the-hard-way.html

This article is for you complements of MembersAlliance Credit Union.

Please feel free to share!

2550 S. Alpine Rd. Rockford, IL 61108 – Phone 815-226-2260

https://www.membersalliance.org/