Cyber Extortion—a New Twist on an Old Trick

Presented by Derrell Crimm, CFP®

Extortion, the practice of obtaining money or some other type of gain through force or threats, is a ploy criminals have used for hundreds of years. Now, they've put a modern twist on this old trick. Scammers have brought extortion to the digital world, and it's becoming increasingly popular among the cybercriminal class.

What is Cyber Extortion?

Cyber extortion, or *cyber-crime extortion*, is when a hacker gets access to your data, hijacks it, and then renders it inaccessible to you unless you pay a demanded ransom. Common forms of cyber extortion perpetrated on individuals include:

- **Ransomware**. Cyber criminals use *ransomware*, a type of malware, to hold your data hostage by encrypting or blocking access to your files. These criminals first gain access to your computer or device through phishing e-mails that come with bogus links or attachments. Once a link is clicked or an attachment opened, the ransomware is downloaded, encrypting your hard drive. A message pops up on your device or computer screen demanding ransom by a certain date or time in exchange for the decryption key—or else your files will be lost forever.
- **Stealing your data and threatening to expose it.** In this case, your data is not necessarily encrypted but rather a cybercriminal has somehow hacked into your computer and now has your sensitive information. The extortionist then threatens to expose the confidential information unless you pay a ransom.

How Can You Prevent Cyber Extortion?

Almost anyone who engages in any kind of online activity can be a target of cyber extortion. Here are a few tips to help ensure that you don't fall victim to it:

- Be sure that you **have up-to-date antivirus and firewalls installed**.
- **Stay vigilant** when it comes to safe e-mail and web browsing.
- **Be suspicious of unsolicited e-mails** you receive and wary of links or attachments from sources you don't know.
- **Think twice before clicking a link or downloading an attachment** that comes with an email you receive, even if the message was sent or forwarded from someone or an organization you know.
- **Back up your data regularly.** This way, if you do fall victim to cyber extortion, you will still have all of your data and won't feel desperate enough to give in to the cyber criminal's ultimatum in order to get the data back.
- **Encrypt *all* your sensitive information.** If extortionists steal your data, they may be able to hold it hostage, but they won't be able to make sense out of or decrypt it.

Most security professionals recommend that victims of cyber extortion *never* negotiate with criminals. Paying the ransom won't guarantee that the attack will stop or that data and information will be recovered. It would also reinforce the notion that cyber extortion works, helping to encourage fraudsters to continue committing this form of crime.

Be sure to follow the best practices recommended above to mitigate your risk of becoming a victim of cyber extortion and to keep your personal information secure. If you have any questions, please feel free to contact our office by phone or email.

Derrell Crimm

AC Financial Partners

1800 International Park Drive | Suite 10 | Birmingham, AL 35243

205.235.3500 | 205.235.5170 fax | www.acfinancialpartners.com | derrell.crimm@acfinancialpartners.com