DIGITAL MOUNTAIN®

SPRING 2020 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we provide an overview of mobile device management and malware prevention. With the unprecedented increase of telecommuting resulting from the Coronavirus pandemic, secure data management by organizations is more critical than ever.

Coronavirus Spreads Malware Concerns

As the United States copes with the accelerating spread of the novel Coronavirus, 2019-nCoV, also known as COVID-19, a corollary cybersecurity threat is also accelerating. Phishing emails related to the COVID-19 outbreak are making use of the worldwide health threat to prey upon the concerns of recipients, employing many of the same tactics used in previous phishing scams. Additionally, email scams that don't involve malware are also taking advantage of the COVID-19 outbreak and showing up in inboxes looking for a victim. With the added stress of the new illness, many people are watching their emails for vital information, yet forgetting the basics of how to prevent device infection via malicious emails. This combination creates a situation in which hackers and scammers can thrive on remote employees susceptible to revamped tricks.

Providing a False Sense of Security

Many of the COVID-19 related phishing emails are employing stolen graphics from trusted sources of information such as the World Health Organization (WHO), the United Nations (UN), and various government agencies. The graphics add an air of legitimacy in a time of uncertainty, and it's understandable that if you received an email claiming to be from the Department of Health and Human Services with an attachment promising how to prevent the spread of illness in the workplace, you'd be hard pressed not to open the attachment. This type of phishing email is increasingly being labeled "malicious news" for both its malware attachments and false content. A recent phishing email purporting to be from the WHO included a dialogue box requesting the recipient verify their email account and password before they could access information regarding COVID-19. The site turned out to be fake, and the hackers netted email login credentials. Of course, in any case when recipients click on malicious attachments or enter their credentials – they expose their devices and their personally identifiable information to hackers.

Executable code can be inserted into practically any file type, and COVID-19 related phishing emails have made use of .PDF, .DOCX, and .MP4 file types. Perhaps a more unfamiliar strategy is to create an application file with the prefix HXXP, designed to fool victims into thinking they're opening a hyperlink to a webpage, when in fact, they're executing the installation of an application that will install malware on their device.

Back to Security Basics

Irrespective of the look or content of an email, there's good reason to be cautious of email from an unusual or unknown source. When you receive email, the following steps should help reduce the risk of malware taking up residence on your device:

1. Check the sender's address as it appears in the inbox – twice, especially if the sender is not already in your contacts. Think twice before opening email from sender's whose addresses:
   a. Are a series of seemingly random letters or numbers.
   b. Are a variant of an organization's name, but not a match. For example, the Centers for Disease Control sends emails from @cdc.gov addresses, not @cdc.com.
   c. Are misspellings of legitimate organizations. The WHO will not call themselves World Heath Organization, but a hacker might.
   d. Are vague names or titles. CEO@, Administrator@, or YourFriend@, especially if followed by any of the above warning signs which are very likely malicious emails.
2. Use your mail application's preview function for your protection. If you see something that doesn't look right, delete the email without opening and clear the trash folder.
3. Use email and attachment scanning applications to help spot unclean attachments. Make sure to keep your security applications updated.
4. Turn off automatic attachment opening settings. Nothing should open on your device until you ask it to.
5. Never respond to an email you think could be from a hacker.

If you notice your device acting abnormally, or you think you may have malware on your device, start by running your security software, but don't rely on it. Your best bet is contact a trusted provider, like Digital Mountain, to help you through a malware crisis.

Phishing Isn't the Only Danger

Emails scams of all types are on the rise, including some very creative rehashes of the infamous advance-fee scheme. In what was originally a snail mail scam that later morphed into an email scam, a fictitious government minister from a foreign country would send a letter to a target (usually a CEO or prominent business figure) proposing that in exchange for a certain amount of money to cover the costs of moving a multi-million dollar sum of money out of the foreign country, a large return payment would be made. With the Coronavirus scams, requests for donations are made by fake scientists who are "very close" to developing a cure or a vaccine, but are running short of funds. Other scams include sending out direct marketing emails for fake cures and supplies that are in short supply. One of the most creative tricks is the fake invoice scam where companies are sent a bill for supplies like gloves and masks never ordered, or, in the alternative, a company pays in advance but is sent an inferior product, sent less than ordered, or sent nothing at all.

By taking some precautions, you can avoid these email scams. Before responding to an email that seems too good to be true:

1. Follow your instincts – if it's sounds like a miracle, it's probably a scam.
2. Don't respond to emails requesting a read receipt. You may end up seeing more in your inbox as a result of your confirmation that the email was read.
3. Rely on trusted suppliers. Companies with whom you regularly conduct business are more likely to continue being trustworthy.
4. Never send advance payments to a person or entity you are not sure is legitimate.
5. Copy and paste a portion of the text into an internet search engine. Chances are if it's a scam email, someone has put up a warning.

Phishing emails and email scams are frustrating and stressful at the best of times. The good news is that by practicing the security basics, we can protect ourselves from whatever new circumstances hackers attempt to exploit. Consistent email safety, like washing our hands and covering our sneezes, is a long-term way to protect our devices. However, just as you'd seek professional help for an illness or injury, don't wait to consult Digital Mountain if you think your device is infected with malware.

Please direct questions and inquiries about cybersecurity, computer forensics and electronic discovery to info@digitalmountain.com.

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com. In the short term, she is available for webinars and remote e-conferences.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: