April 1, 2020

Cyber Hygiene – Best Practices While Working Remotely

By Joseph M. Ruscak

As companies transition to employees working from home during the current COVID-19 related disruptions, cyber criminals look at these changes as huge opportunities. In the last week alone, there have been numerous cyber-attacks disrupting businesses by accessing information from remote workers. These disruptions ranged from phishing attacks to gain information from at-home employees to social engineering attacks targeted to entice remote workers to undertake disruptive actions, like the transfer of funds. With this rise in attacks and active threats, it is more important than ever that you and your business stay vigilant and focused on working securely. Please consider the following:

VPN

If your company does not use a Virtual Private Network (VPN), now is the time to consider one. A VPN extends a private network across a public network and enables users to send and receive data as if their computing devices were directly connected to the private network. This allows sequestering of critical information and prohibits users from taking the critical information outside of the VPN environment. While sometimes bulky and slower, the protections that VPN's offer are immeasurable, especially if working with sensitive information.

EXTERNAL E-MAILS

Does your business utilize an "EXTERNAL" stamp in your e-mail to identify messages originating outside your internal systems? This branding can be added easily to any number of e-mail systems. When an e-mail is sent claiming to be from a member of your company, but has the "EXTERNAL" stamp, it is likely a phishing scam. You can then report the breach to your IT team and discard.

VTC

As large numbers of people turn to video-teleconferencing (VTC) platforms to stay connected, reports of VTC hijacking, also called "Zoom-bombing", are emerging nationwide. The FBI is reporting conferences being disrupted by pornographic, hate images and threatening language. The easiest way to avoid disruption is to make sure your meeting is private and control its access. Use password-only access where allowed.

ATTACHMENTS

Be especially vigilant with file attachments. If you did not expect an e-mail with a file, then verify it with the sender, separate from the e-mail, with a phone call. Do not reply or forward, the sender could be a hacker and possibly tracking your actions.

HYPERLINKS

Be especially vigilant with embedded web links. Examine links before clicking. Look carefully for changes in spelling or fake names that resemble real names. This is a common tactic used to hijack you to a fake or questionable website. Again, a simple phone call to the sender confirming could avoid significant internal havoc.

PERSONAL ACCOUNTS

Avoid forwarding e-mails and documents to personal accounts. Moving a document back and forth between protected and unprotected systems exposes your company and your documents to risk.

PHONES & TABLETS

Pay special attention when working on a phone and tablet. It can be easier due to screen size to miss fake names, links and documents. The mechanisms that make phones accessible are prime targets for exposing weak protocols.

SOCIAL MEDIA

Be extremely cautious with messages or social media that share COVID-19 maps or other information via links or attachments. Because this information is crucial at this time, hackers will take advantage of our vulnerabilities. The best information is, and will continue to be on your local, state and federal health agencies and the CDC website. Directly use those websites and avoid clicking links or opening attachments in unsolicited e-mails on this topic.

REPORT PROBLEMS

If you suspect you have clicked a link or opened something that may be a problem, report it immediately to your IT Support Staff. Do not wait. Especially call if you have entered your username, password or other personal information into an unexpected prompt after opening a link or file. You should always error on the side of caution and report. Catching a problem within the first hour is considerably easier to remedy for your IT Staff than not reporting at all.

Please contact us for more information about how we can partner with your team to assist you in conveying best practices and to learn more about the other services offered in our Cybersecurity and Data Privacy Practice Area.

Joseph M. Ruscak
330.849.6716| jruscak@ralaw.com

Chad L. Mowery
330.849.6782| cmowery@ralaw.com

Mark Young
216.820.4210| emyoung@ralaw.com

Jeffrey J. Farkas
330.849.6673 | jfarkas@ralaw.com

This alert is informational only and should not be construed as legal advice. ©2020 Roetzel & Andress LPA. All rights reserved. For more information, please contact Roetzel's Marketing Department at 330.762.7725

This alert is informational only and should not be construed as legal advice. ©2020 Roetzel & Andress LPA. All rights reserved. For more information, please contact Roetzel's Marketing Department at 330.762.7725