Cyber Alert

March 18, 2020

How to Guard Against Proliferating COVID-19 Scams

Risk Management Question: What precautions can lawyers, staff, and law firms take to avoid pandemic-related cyber scams?

The Issue: As the number of attorneys and law firm staff adopting social distancing and working from home increases, so do the related cyber risks. Hackers have well-rehearsed playbooks that seek to exploit distributed workforces using remote connections. As a result, lawyers and staff should be extra vigilant and take additional precautions.

Among other scams, hackers are circulating phony but legitimate looking:

- COVID-19 outbreak maps.
- Emails purportedly from IT teams to employees with the subject line: "ALL STAFF CORONAVIRUS AWARENESS." The emails describe a seminar at which the company will discuss what it's doing in response to COVID-19, which includes a link to register for the seminar.
- Emails claiming to be from vendors about COVID-19 tools and strategies that include links to PDFs and Word Documents and invite the recipient to click and open the attachment.
- SMShing messages closely resembling the employer's phone number, indicating the recipient needs to "click here" to find out about modified firm operations.

These seemingly harmless and legitimate looking emails and attachments are loaded with malware which deploy remote access tools (RAT), keystroke logging malware, desktop image capturing malware, and ransomware. Hackers are looking to potentially gain control of law firm personnel's remote access into the firm, or encrypt computers and anything else the malware can reach.

Risk Management Solutions:

Here are several steps lawyers and staff alike can take to protect themselves and their firm:

1) Always think before you click.
2) Never click on an email or text message from anyone you don't know.
3) If you receive an attachment in an email or text message you were not expecting—even if it's from someone you know—call the person at a known telephone number (*not the number listed in the message*) to confirm the message is legitimate.
4) If you click on something you should have avoided and a box opens that asks you for your password, or to supply some information or click on a link to enable a later version of software: *stop, close out, and immediately call your IT Department* to have a scan run on your device(s).
5) Remember the ongoing risk of public Wi-Fi. If you can connect to Wi-Fi without a password, then the network is insecure. Do not use insecure Wi-Fi to connect to your work server, do any personal banking, or send any type of confidential or personal information.
6) Avoid working in public spaces where third parties can view screens or printed documents.

Now, more than ever, it's important to follow the classic *Hill Street Blues'* watch commander's advice: Let's be careful out there.

Steven M. Puiszis
312-704-3244
spuiszis@hinshawlaw.com

Noah D. Fiedler
414-225-4805
nfiedler@hinshawlaw.com

Joanna L. Storey
415-263-8143
jstorey@hinshawlaw.com

HINSHAW