April 23, 2019

A new method to phish you—a wireless voicemail message

Risk Management Question: What can lawyers do to identify how hackers are using business tools–such as the transcription of voice messages into emails—as weapons to access law firms' systems, and how should the attacks be handled?

The Issue: Instant transcription of voicemail messages and receiving those transcriptions by email when not in the office have made lawyers' lives a little easier. Because the transcription is not perfect, most such systems provide a link to a .wav file, permitting the addressee to listen to the voicemail recording. Hackers know this and are taking advantage of it. Beware of receiving an email that purportedly includes a link to a Wireless Voicemail message. In email messages sent to at least one firm that we know about, the Voice.wav download button in the email is actually a link to a third-party malicious website.

Risk Management Solution: Never click on a link or an attachment from anyone you don't know or an attachment you were not expecting to receive, even from a known sender. Pick up the phone and call the sender, but do not use the phone number in the email because you could be calling a hacker. Even when the communication is somewhat commonplace or familiar, always think before you click.

Remember, let's be careful out there.


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


Anthony E. Davis
212-471-1100
adavis@hinshawlaw.com


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


Lauren N. Kus
312-704-3000
lkus@hinshawlaw.com

HINSHAW