October 11, 2018

Cyber Alert – Your Mobile is Not Just a Phone — It's a Handheld Mini-Computer Subject to Attack

Risk Management Question: We need to stop treating our mobile phones like they're just phones. They are mini-computers more powerful than the computers that guided the Apollo 11 spacecraft to the moon and back. What common sense steps can lawyers take to protect sensitive and confidential personal and client information accessible on, and sent from, mobile phones, and meet the ethical duty to safeguard client information?

The Issue: Our mobile phones have become an extension of us—they provide ready access to information about where we are supposed to be and when (including directions), and offer 24/7 contact with friends, family and work. Their size, portability, functionality and ubiquitous availability have resulted in our underestimating how vulnerable they are to hacking and social engineering exploits. To protect our own personal information and confidential client information, we need to adjust our mindset and treat our phones like the computers that they are.

Risk Management Solution: A recent infographic from KnowBe4.com—"20 Ways to Block Mobile Attacks"—outlines, as the title suggests, steps that can protect mobile phones from hacking and fraudulent schemes. It is well worth reading and is accessible at: https://www.knowbe4.com/hubfs/20WaysToStopMobileAttacks.pdf.

Some of the suggestions will be familiar to desktop and laptop users:

- Think before clicking on unsolicited text messages and emails.
- Do not send sensitive information over public WiFi without confirmation that it is a secure network.
- Giveaways or contests that sound too good to be true probably are, and may lead to phishing sites that appear legitimate.
- Resist **any** attempt to get you to reveal personal or sensitive information—either by telephone, email, text or other social media platforms. Confirm the sender's identity by contacting a verifiable telephone number (such as the bank's contact number on the credit card).
- Only provide sensitive information to live people and only when you have initiated the call.

Other measures may be less familiar:

- Disable mobile devices' ability to auto-join unfamiliar WiFi networks or Bluetooth pairings.
- Always turn off WiFi and Bluetooth when not in use.
- Install commonly-available software that identifies secure or risky websites.
- Only use apps available from official app stores—never an app download from a browser and be wary of apps from unknown developers. Keep apps updated. When apps are no longer supported by the app store, delete them.

The bottom line is that lawyers should be more conscientious in protecting sensitive information on mobile phones in order to ensure compliance with ethical duties to clients.

Even if you're just using your phone, remember to 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

Annmarie D'Amour
212-471-6231
adamour@hinshawlaw.com