HINSHAW

Alerts

Social Engineering Fraud

March 14, 2018
Law Firm Cyber Alerts

Risk Management Question: How can lawyers identify and avoid increasingly common social engineering scams?

The Issue: The FBI reports that social engineering scams have resulted in over $5 billion lost over a recent 36-month period. Social engineering involves a variety of deceptive schemes and techniques used by fraudsters aimed at tricking a victim into taking actions that can range from providing information, clicking on links or attachments, or transferring funds. Social engineering exploits can involve phone calls, emails, text messages or any combination thereof. Many of these exploits are based on publicly available information from a law firm's website or a lawyer's, or a family member's, social media activity. They often begin with a seemingly innocent phone call.

Within the last couple of weeks, a number of law firms that share threat information reported an increased number of social engineering, phishing-type phone calls seeking information. Last week, one of the lawyers in Hinshaw's New York office received such a call from a person, supposedly in New Jersey, who claimed that he was being scammed. The caller was given our lawyer's name and told to send our lawyer $4000. This is an example of how scammers will try to take advantage of our natural instinct to help — and to take on new work. Another common social engineering scam involves a call from a person posing as an IT help desk worker asking for information in order to update software or fix a computer problem.

Anyone could be targeted; the questions asked may seem harmless, but there is a reason for those questions. Social engineers will go to great lengths to gain access to information or data that they can exploit, including personal information, passwords, account numbers, phone numbers or phone lists, information about your computer or your network. The information you provide may help them take their next step in their social engineering scheme. **Do not underestimate the risk of engaging a person on the phone that you don't know.**

Risk Management Solutions:

- Never provide any information about your firm or someone at the firm (no matter how harmless the requested information may seem) to someone you don't know. There is likely a lot of information available on your firm's website which may be used by callers to give them the appearance of credibility. Be polite, but be firm, and don't engage a stranger on the phone

Attorneys

Steven M. Puiszis

Service Areas

Cyber Security for Law Firms

Law Firm Cyber Alerts

Lawyers for the Profession®

who is looking for information.

- If you receive a voicemail message from someone you don't know and you decide to return the call, run a quick google search on the person and try to obtain a phone number to use when making the call. If possible, avoid using the phone number in the message because you could be speaking with a fraudster.
- Don't trust caller ID — the number can be spoofed. So if you receive a call from someone purportedly from inside your firm and you are asked to provide information, politely explain you will call the person back. Look the person up on your firm's directory and call the number back.

Microsoft has reported the number of social engineering exploits now exceed the number of attacks based on software vulnerabilities. **Take this risk seriously**.

Remember, let's be careful out there.

Download Cyber Alert - Social Engineer Fraud (PDF)