MALPRACTICE ALERT

SOCIAL ENGINEERING FRAUD

MINNESOTA LAWYERS MUTUAL INSURANCE COMPANY

Social Engineering Fraud

Historically most law firm data breaches were related to the loss or theft of a laptop, thumb drive, smartphone, or other mobile device. Technology advancements have made it possible for a criminal to get access to the same information online through social engineering attacks. One of the most vulnerable areas in a law firm's security is emails. Social engineering is a type of malicious attack that relies on individual human interaction and our trusting human nature to trick people into breaking normal security procedures.

It's more important than ever to have systems and policies in place to help detect and deter fraud through social engineering tactics. Since humans are "the weakest link" in the security chain, firm-wide education is the first step toward reducing risk. If your partners and employees are aware of the characteristics of risky emails, they will be more likely to recognize them and avoid becoming a victim.

The following summarizes a few of the attack strategies:

- **Phishing**: In a phishing scam, a malicious party sends a fraudulent email disguised as a legitimate email, often purporting to be from a trusted source. The message is meant to trick the recipient into sharing personal or financial information or clicking on a link that installs malware.

- **Pretexting**: In yet another type of social engineering attack, called pretexting, one party lies to another to gain access to privileged data. For example, a pretexting scam could involve an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient. Examples are the phony emails requesting that you update account information online or the telephone scam in which the attackers claim to be the IRS requesting social security numbers, tax information or changes in wire transfer instructions.

- **Baiting**: Baiting is a form of social engineering attack that does not rely upon email. In a baiting attack, the aggressor leaves a malware-infected device, such as a USB flash drive in a place where it is sure to be found. That device, when plugged in, kicks off a malware attack

How to Avoid

Minnesota Lawyers Mutual strongly encourages its insureds to review the recommendations presented in the following materials, to become acquainted with the current threats, and develop procedures for handling sensitive information:

- **Federal Bureau of Investigation's PSA, *Business E-mail Compromise*** released on May 4, 2017. The announcement provides additional information on the types of scams, real-life scenarios, and what to do if you fall victim.

- **ABA Journal article *Using Unencrypted Email in Client Communications*** posted May 11, 2017. The article announces the recently released ***Formal Ethics Opinion 477*** that updates Formal Ethics Opinion 99-413, which was issued in 1999 before the widespread use of tablet devices, smartphones, and cloud storage.

- **MLM Malpractice Alert**: ***Interception of Incoming Wires***

- **MLM Malpractice Alert: *Email Scams***

Malpractice Alerts is an E-mail Subscription Service highlighting legal decisions, pending legislation and industry trends to help lawyers anticipate and prepare for potential changes in the marketplace. With insight from malpractice defense and MLM staff attorneys, this new service is provided at no extra charge to MLM insureds and offers timely expertise on important malpractice topics.