practicePRO

CYBERSECURITY AND FRAUD PREVENTION TIPS

Phishing attacks and other forms of cyberfraud are an increasingly common source of loss for lawyers. Our constantly changing technology, and the changing tactics used by fraudsters, require constant vigilance and adaptation. Here are a few tips to keep your and your clients' information secure and prevent fraud.

1. IMPLEMENT ROBUST COMPUTER AND PHONE SECURITY PRACTICES

- Ensure that you have robust password protocols, including training your staff to use complex alphanumeric passwords along with two-factor authentication.
- Make sure computers have adequate anti-virus protection and are regularly updated. Use end-to-end encryption when transmitting data over the internet.
- Implement regular data back-ups to a secure server or storage to prevent fraudsters from holding your data hostage following a ransomware attack.
- Consider trying penetration testing tools to assess network vulnerabilities.

2. PROVIDE STAFF TRAINING ON IDENTIFYING BAD CHEQUES AND PHISHING MESSAGES

- Train yourself and your staff to notice red flags associated with bad cheques and phishing attacks.
- Visit the practicePRO fraud prevention webpage for the LAWPRO Fraud Fact Sheets and tips for identifying fraud

3. VERIFY INSTRUCTIONS RECEIVED BY EMAIL

- Spear-phishing attacks will often involve email instructions that appear to have originated from a client, law firm on the other side of a transaction or other trusted party, but are deceptions by fraudsters. Before following requests that come by email, particularly involving the transfer of funds, call the party providing those instructions on the phone to confirm their accuracy.

4. ENSURE YOU HAVE SUFFICIENT CYBER INSURANCE

- Malpractice insurance only protects certain cyber risks and firms should not assume their general liability insurance will cover all cyber risks. Consider whether a policy directly addressing the costs associated with cyberattacks is appropriate for your practice.

5. MAKE OR UPDATE YOUR INCIDENT RESPONSE PLAN

- Because a cyberattack can cause significant harm, law firms should be prepared to take action immediately. An Incident Response Plan addresses the steps for the detection, containment, and eradication of a cyber breach, recovery of normal operations, and follow-up analysis. LAWPRO's resources on incident response plans can help you get started.

LEARN MORE ABOUT CYBERSECURITY AND FRAUD PREVENTION TIPS:
See the practicePRO fraud prevention webpage and the **cyber dangers webpage.**

This publication includes techniques which are designed to minimize the likelihood of being sued for professional liability. The material presented does not establish, report, or create the standard of care for lawyers. The material is not a complete analysis of any of the topics covered, and readers should conduct their own appropriate legal research.