CYBERSECURITY

Be aware: Tips to Avoid Falling for Email or Phishing Scams

Email scams are rampant and many of them can fool even a sophisticated professional. The New Jersey State Bar Association is looking out for its members and offers the following tips to keep your practice and private information safe.

Beware of Suspicious Emails and Do not Click Suspicious Links

- Be very suspicious of any emails you receive from trusted entities like your bank. While these addresses may look official, they usually contain inconspicuous differences that redirect you to a fraudulent site.
- If the email contains a link, don't click on it.
- Deceptive links that mimic legitimate URL addresses are a common tools con artists use in phishing scams.
- Instead of clicking on the link, type in the web address of the institution into the browser to access the website.

Know the Common Phishing Language:

- Look out for common phishing language in emails like: "Verify your account."
- Legitimate businesses will not send you an email to ask for your login information or sensitive personal information.
- Also, look out for emails that try to convey a sense of urgency.
- Warnings that your account has been compromised, for example, are a common way to lure victims. Again, contact the company directly to inquire about such emails rather than using any link or other contact information provided in the email.
- Finally, be wary of any email that does not address you directly.
- While some phishing scams will use your name in the email, many are sent out as spam messages to thousands at a time.
- Most legitimate businesses will use your first and/or last name in all communication.

It's good practice to look at all the emails and websites suspiciously. Getting sucked into a phishing scam can cost you thousands of dollars and a good amount of your valuable time. An ounce of prevention now can save a pound of cure later.