To: New Jersey Board of Bar Examiners Website Users:

We are writing to alert you to an active, credible phishing campaign that is currently targeting several state bar associations and bar applicants nationwide.

What to Watch For:

The fraudulent emails are impersonating state bar executives or state bar IT staff using their real names and titles and are designed to appear legitimate. Common traits include the following:

- **Sender Spoofing:** Emails may come from addresses like **john.doe@sbnm.org.virumail.com**. ***Note:*** Legitimate State Bar staff email addresses end with **@sbnm.org**.
- **Vague or misleading language:** Often referencing secure communication or document requests.
- **Urgent tone:** Designed to prompt immediate action without proper verification.

Example Scam Message:

"As part of our ongoing efforts to ensure the confidentiality and security of sensitive information, we are reaching out to confirm your preference for secure communication…"

What You Should Do:

- Do not reply, click on or open any suspicious links or attachments.
- Report the email using the Technical Support Request CLICK HERE link found in the lower section of this website if you receive a message that seems off, even if it appears to come from a known email address.
- Be extra cautious with emails referencing secure communications or urgent requests.

If you receive a suspicious email, please do not respond, click on any links or download any attachments. Report the suspicious email as noted above for additional assistance.

Thank you for your attention and diligence in protecting our legal community.