LAWYERS MUTUAL

Risk Management Alert
Cyber Security

The Latest Cyber Risk: Vulnerability of Your Email Accounts

Law firms continue to be under attack by cybercriminals. The current urgent vulnerability we are hoping to address relates to access to your email accounts.

As you know, cybercriminals are intercepting wire transfers in record numbers. Their access to your email system exposes sensitive information. Recent claims involve breaches to cloud-based accounts. There are simply too many law firms that are experiencing the same issues, so we want to offer some risk management tips.

While recent claims have involved cloud-based systems, we are not discouraging you from using cloud-based systems, but we want you to be aware of the risks and properly manage them.

Without proper security features, hackers can read and respond to emails, deleting the evidence from your inbox. They can also set up rules to forward emails to unknown accounts.

Immediate Action Items

- Consult your current IT resource today to confirm your system has the appropriate safeguards in place and to ask questions about any of the tips below that you do not understand.
- Update/manage/modify your existing cloud-based email accounts to ensure:
  1. Passwords are strong and unique in that they are used only for the email account.
  2. Two-factor authentication is enabled on all accounts.
  3. Rules allowing for the automatic forwarding of emails are disabled/not allowed (verify no unauthorized existing rules are present). This does not prevent the sorting of emails into folders or clicking the forward button on an email to send it to someone else.
  4. Regularly check to ensure that there are no rules set on the account without the user's knowledge.
  5. Review sent and deleted emails for accuracy and suspicious activity.
  6. Ensure that logging is enabled - most cloud providers turn this off by default.
- Beware of SMS/Text messages notifying you that your password has been reset without your knowledge. This is a new type of targeted phishing scam.
- Review recent instructions (incoming/outgoing) relating to any wire transfers. Review your authentication and related practices relating to all wire transfers. You should not wire money to a new account without verifying the instructions via telephone first.

Hacked email systems is a global issue and we all need to increase our defenses against these rampant threats. Please be prudent and take immediate action to ensure your systems have the above basic protections in place regarding your email.

Next, review your Information Security practices to ensure proper data backup, data encryption, education surrounding phishing attacks and related items that can impact day-to-day operations.

You can learn more about defending against hacking attempts in our article "You Are the First Line of Defense Against Hackers" available here: http://www.lawyersmutualnc.com/risk-management-resources/articles/you-are-the-first-line-of-defense-against-hackers.

You are welcome to reach out to Lawyers Mutual by calling our Risk Management Hotline at 800.662.8843 and/or Identity Fraud, Inc. (BIZLock) cyber at info@bizlock.net.