A well-trained staff promotes cybersecurity

Law firms are constantly faced with cybersecurity threats. The high value of data stored in your office files and computers places a target on your practice for internet attackers. While there are numerous steps you can take to help protect your firm, one of the most essential resources are the people who work for your practice everyday. Staff members can be one of your greatest assets or your biggest liability. So, it is vitally important to provide them with adequate cybersecurity training. Law firms are constantly faced with cybersecurity threats. The high value of data stored in your office files and computers places a target on your practice for internet attackers. While there are numerous steps you can take to help protect your firm, one of the most essential resources are the people who work for your practice everyday. Staff members can be one of your greatest assets or your biggest liability. So, it is vitally important to provide them with adequate cybersecurity training.

As explained by the National CyberSecurity Alliance, “The best security technology in the world can’t help you unless employees understand their roles and responsibilities in safeguarding sensitive data and protecting company resources. This will involve putting practices and policies in place that promote security and training employees to be able to identify and avoid risks.”

You can employ numerous methods to ensure that your firm members get the training they need. If you have a dedicated IT department of point person, provide resources to develop a staff training program. Remember that cyber threats are constantly evolving, so refresher courses may be necessary to maintain a well- trained staff. If you don’t have a cybersecurity guru on staff, consider outsourcing your training needs or utilizing an internet-based instructional program. There are numerous options available, but keep in mind that they may not all address the unique

concerns of legal practice. Try to find a service or program that is specifically geared towards a law office.

If you decide to be adventurous and develop your own training system, here are some tips on the information you may consider including:

- Best practices for creating and maintaining strong passwords
- Downloading and internet access restrictions when working on firm-issued computers and devices
- Guidelines for opening email attachments and or questionable website links
- Reporting suspicious activities or wrongdoing
- Awareness of your physical surroundings
- Adequate backups of work product
- Restrictions on the sharing of passwords and computer access
- Restrictions on the use of personal emails and unsecured networks for work-related tasks
- The various types of cyber attacks and how to identify them

Your firm members and staff are the first line of defense against a cyber attack, so every member of the firm should receive training. Employee negligence accounts for approximately 19% of all data breaches, according to a 2015 data breach cost study. Don't let inadequate training lead to a costly breach of your confidential client files.

About Erika Winston:

Erika Winston is a freelance writer with a passion for law. Through her business, The Legal Writing Studio, she helps legal professionals deliver effective written messages. Erika is a regular contributor to TimeSolv and a variety of other publications.