The Equifax Hack – A Teachable Moment for your Law Practice

Over 140 million victims. That is a rough estimate of the number of people impacted by the Equifax security breach. A company that is charged with handling some of our most personal and valuable information was not able to protect itself from a cyber attack. Equifax isn't alone either. Yahoo, Netflix and numerous other mega corporations have all been unable to protect themselves against the devious tactics of hackers. So, what can you learn from these news making misfortunes? I went on a hunt to find out.

The Evolving Threat

Cyber security experts note that hackers are reinventing their approach to attacks. For example, the vast expansion of IoT (also known as the Internet of Things) has opened the door to significantly more security hack entrance points. A seemingly innocent "smart" thermostat could become an entryway for hackers to access your most confidential files.

These cyber criminals are also evolving in their use of the information gained. While the selling of social security numbers and account information is still quite lucrative on the dark web, hackers are also choosing to hold the information ransom in hopes of a big payout. Netflix experienced this type of security breach when hackers demanded money for the return of an unaired television episode.

A Layered Approach

When addressing the importance of securing confidential information, many experts recommend a layered approach. Layered cyber security uses

various components to create a more secure barrier around protected data. An article in Entrepreneur explored numerous security layers and their importance within a small business environment. Some of the featured measures included:

- Physical security – It isn't smart to throw old hardware into a dumpster behind the building, instead of having it professionally destroyed. It's also unwise to leave confidential files lying around the office, where unauthorized individuals can easily access them. While many law practices take extensive cyber security measures, managers sometimes forget that physical barriers make up the first layer of protection.
- Wireless security – We live in a world free from wires, but you must still ensure that your wireless connection conforms to reasonable security standards. Updated WPA2 security settings give added protection, along with strong passwords that cannot be easily guessed.
- Email security – As explained in the Entrepreneur article, once a hacker has access to your email accounts, access to all other accounts is generally not far behind. Think about it. When you need to reset your bank account password, how is that handled? Most likely, it is done through your email. So, as you go about resetting your passwords to keep your accounts safe, you could be opening the door to a hacker. Enforce email security among your employees. Prohibit them from accessing links and attachments from within their email accounts. Also, ensure that they are using strong passwords and refraining from accessing their work email accounts from unsecured networks.

As proven by the Equifax hack, there is no 100% guaranteed method of preventing security breaches. However, you can better protect your practice by making smart, proactive security decisions. TimeSolv helps you meet this need by equipping our law firm time tracking and billing system with the comprehensive, state-of-the-art security measures. Click here to find out all of the ways that TimeSolv works to protect your law firm's most confidential data.

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.