Law Office Security

Prepared For: Legal Education Society of Alberta

Law and Practice Update

Presented by:

Richard A. Verhaeghe

Verhaeghe Law Office

Athabasca, Alberta

(587) 410-0665

Richard@freedomlaw.ca

For Presentation In:

Calgary - November 7- 8, 2014

I have been tasked with writing a short paper on Law Office Security for the small/ solo law office. In writing this paper, I would like to disclose that I am not an IT person but rather a power user, which means I have enough knowledge to do a serious amount of damage and hire someone smarter than I to fix the mess I have caused. Most of my knowledge is pretty much self-taught and from trial and error (ie. "blowing things up" or "crashing" entire server operating systems). Another power user will probably find this paper on the boring side; and, I acknowledge that I have much yet to learn and that different systems work for different people. Now onto one of my favourite topics: Law Office Security Tips and Tricks. Please note that I am not opposed to using cloud based services and do so on a regular basis; so, part of this paper will be in that direction. I will also show you how to build a private cloud in the event you are opposed to third party commercial based systems.

1. Social Engineering

In the biograph "Ghost in the Wires", Kevin Mitnik found himself on the F.B.I.'s most wanted list for being a computer hacker and was absurdly described as being able to launch a nuclear strike with one telephone call. Part of Kevin Mitnik's success in hacking was simply to telephone people up and pretending to be from the I.T. Department and convincing employees to give up their user names and passwords. He described this trickery as Social Engineering. Over the years I have had several people telephone me pretending to be a supplier and wanting me to commit to paying a bill. No one has yet asked me for a username or password but I expect that is coming; so be very careful about who you give out your user names and passwords to.

2. Passwords

DO NOT use normal passwords, such as 1-2-3-4 or "password", I believe "password" is one of the most commonly used passwords in existence.. I have a username that does not exist in the dictionary, I coined two words such as sun and moon, such sumnoon for a standard username and have a password that always has a prefix of a backwards year and symbol such as easter5619$. I use three different holidays depending where in the alphabet the website falls with the same suffix so as not to use the same password for every site.

3. Routers

Routers are amazing pieces of equipment. They provide solid security from hackers with built in firewalls when properly configured. My personal preferences are the Higher End ASUS Dark Knight Routers. They can be a sieve or a shield to your network. The danger to every single router is that they come with a default username and password, usually "admin" and "admin". Many offices

simply plug in their routers and do nothing more to them. Especially bad are the Telus Actiontec Routers. They are great because they work right out of the box; and, it is not uncommon for me to find the passwords unchanged.

4. Router Port Blocking

We recently noticed that someone was banging away at our network, possibly from a VPN or otherwise originating out of North Africa. A simple solution was to block access to all of our ports except for the Continental United States and Mexico. That way, when I go down to Mexico or the U.S., I can still remote access in to my computer without our system appearing visible in North Africa.

5. Shields Up!

A site I like testing my system again is Gibson Research Corporations ShieldsUp!. It will test all your common ports or All Service Ports and tell your if they are open, closed or in stealth mode. **https://www.grc.com/shieldsup**. If you notice that you have open ports, call your IT Tech to close them immediately. We use multiple programs that connect to the internet and; in just doing a test, every one of my ports was in stealth mode.

6. **Web of Trust**

www.mywot.com

Many websites contain hidden dangers or will redirect you. A first level freeware program is Web of Trust which I have on all our machines. It sometimes gives false readings but will often buy you that second or two before you click and either fill your computer with freeware or go someplace you don't want to. According to WOT:

> Web of Trust (WOT) is a website reputation and review service that helps people make informed decisions about whether to trust a website or not. WOT is based on a unique crowdsourcing approach that collects ratings and reviews from a global community of millions of users who rate and comment on websites based on their personal experiences.
>
> The community-powered approach enables WOT to protect you against threats that only the human eye can spot such as scams, unreliable web stores and questionable content. It complements traditional security solutions that protect computers against technical threats such as viruses and other harmful software. WOT is based on a patented system where user behavior is systematically analyzed and monitored to ensure the ratings are reliable, accurate and constantly updated. In addition, the ratings are validated with trusted third party information, such as blacklists of phishing sites.