Ten Cybersecurity Lessons Learned About Working From Home

by Sharon D. Nelson, Esq. and John W. Simek

The year 2020 will be remembered as the year that lawyers were catapulted into the future. As a result of COVID-19, the majority of law firms suddenly found themselves thrust into a work-from-home (WFH) environment. Some were prepared for working remotely, but many were not. We've helped a lot of lawyers transition to a different working environment by providing training and implementing new technologies in their practice. Along the way, we've learned some things about how lawyers have responded to the pandemic. Here are ten cybersecurity lessons we've learned about WFH.

1. **Home networks are 3.5 times more likely to have at least one family of malware than corporate networks.** A study by BitSight analyzed data from 41,000 U.S. companies. The study found that 25% of devices (e.g. printers, computers, IoT devices, etc.) on a home network had services exposed to the internet. Another scary statistic is that "Nearly one in two organizations (45%) had one or more devices accessing its corporate network from a home network with at least one malware infection." Ouch.
2. **Sharing the device you use for law firm work with family members is a bad idea.** Devices used to access the law firm network and work on confidential client data should only be used for that purpose. Family members should not be using the same device even if there is a separate login ID and password for the device. If a family member inadvertently performs an action that allows the installation of malware, client data and law firm access could be compromised.
3. **Zoom is currently the choice of clients/potential clients.** Teams, Webex, Zoom, and GoToMeeting are all good video conferencing platforms. The reality is that Zoom is the technology of choice for your current and potential clients. All the other platforms are playing catch-up to Zoom. Despite some early histrionic media reports, you can use Zoom securely for client communications.
4. **Make sure your confidential client conversations are kept private.** Many of us are sharing working space in our homes. As a lawyer, you have an obligation to ensure that client conversations are private. That means having a separate room to conduct client conversations and consider using a headset too. You wouldn't loudly discuss a client matter while commuting on the train so why would you allow family members to eavesdrop?
5. **Employee security awareness training is more important than ever.** The WFH environment has put law firm employees into situations that carry different risks than when they were in the firm's office. As item #1 in our list identifies, we need to be even more diligent with practicing safe computing. The cyber criminals know there are a lot of targets working from home using insecure home networks, Training employees to recognize the current cyber threats is an absolute must at this time.
6. **Have a Work-From-Home policy.** If you don't already have one, now would be a good time to develop a WFH policy. The policy serves to set employee expectations and what they should and shouldn't do. Specific technology requirements may be part of the policy too. The policy can also have a statement about family use of devices to further support item #2 in our list.
7. **Consider issuing firm-owned laptops so that you control the security of devices used at home.** More and more of our clients are not purchasing desktop computers, opting for laptops (or

tablets) with docking stations as the primary computing device. Taking that approach makes it much easier to quickly migrate to a WFH scenario. A firm-owned laptop is configured with the security software and applications the user needs to perform their job. Relocating the laptop to the home network preserves the security of the computer, making it safer to use than the typical home machine.

8. **There are options for home users "competing for bandwidth."** Your spouse is probably working from home and your children may be attending school remotely as well. This means that you are probably sharing the same Wi-Fi network as everyone else and experiencing a slowdown. You may want to try the hotspot on your phone to see if the speed would be better than your home network. Directly connecting your computer via Ethernet to the router will help maximize speed. If you don't have Ethernet cabling in your walls, try using an Ethernet powerline adapter. The TP-Link AV1000 is a good choice and should be around $50 at Amazon, although pricing and availability are all over the place.
9. **Utilize a Virtual Private Network (VPN) for remotely connecting to the firm network.** Using a VPN is better than not using one. A VPN creates an encrypted communication channel from your computer to the firm network. Many users will be tempted to use Remote Desktop Protocol (RDP), especially since it is included free with Windows. There are many known vulnerabilities with various versions of RDP. If you must use RDP, consider running RDP through a VPN tunnel instead of exposing RDP directly to the internet and by all means, utilize multi-factor authentication (MFA) for any connection.
10. **Prioritize lawyer wellness.** Lawyers in wellness trouble are a security risk. Lack of concentration, mental health problems or substance abuse can cause serious lapses in making smart decisions concerning the use of technology.

Sharon D. Nelson, Esq. is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She a co-author of 18 books published by the ABA. *snelson@senseient.com*.

John W. Simek is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. *jsimek@senseient.com*.