*TREXIN INSIGHT PAPER*

June 3, 2020

# WORKING FROM HOME – SAFELY AND SECURELY

*Now that it looks like Work From Home (WFH) will be with us for awhile, it is time to improve your home environment.*

As I write this, on the later stages of the COVID-19 pandemic, the business world is considering widespread Work From Home (WFH)—new for many but familiar to IT professionals. As a result, my CISO colleagues have been concerned that the next big breach might come by targeting the sprawl of new home office environments.

Here at Trexin we thankfully have a remarkably small attack surface, due to our extensive use of the cloud for our core systems, along with good hygiene such as Multi-Factor Authentication everywhere, data encryption, and Data Loss Prevention. Also, we make sure to leverage our Clients' security mechanisms (VPN, Remote Desktop, etc.) to ensure we aren't the source of an incident for them.

Still, I lay awake at night thinking about our team's home environment which is often shared with roommates or family who may fall for malware or phishing, and with many devices such as smart thermostats, speakers, doorbells, and TVs which could be hijacked. I worry that this "Environment of Things" may become a staging area for further attacks on Clients (or us) in spite of the multiple layers of protections.

On this point, I've compiled some recommendations on securing your WFH environment. I specifically did not mention VPNs or virus/malware protection, since that's my (Trexin) responsibility as an employer to provide:

- Use strong passwords and different passwords! I broke down and started using LastPass a couple years ago to manage my passwords, and it changed my life. 1Password and Dashlane also are well-liked.
- Change the default password on your router if not every device in your home! Hackers love default passwords.
- Freeware is a cornerstone of our existence, but please browse through your apps and eliminate those you really don't use. A lot of your information is at risk because you don't know what they do with that information.
- It's hard but try to keep your personal life/devices as separate from your work life/devices as possible. At least you can keep your personal life off your work devices, if you're at home near your other devices anyway!
- Watch out for phishing, which now may come even more often. Phishing activity has doubled (at least) during the pandemic, and emails/texts may appear to come from "reliable" source such as family, friends, employer, the World Health Organization (WHO), Medicare, unemployment agencies, your bank, etc. Just be careful about clicking on links or downloading files in messages, especially if they request any kind of personal information.

I tried to write the bullets above so that they apply to all your endpoint computing devices: laptops, tablets, and phones. Please try to read them the same way.

Now consider those other connected smart devices in your home environment: wireless printers, scanners, TVs of course; but also speakers, Alexa/Home, doorbells, cameras, baby monitors, various toys, etc. And does your car connect to your router as well as your phone, when parked at home? Not all of them take user privacy and security into account, so here are some specific steps:

- Do you really need the device to be “smart”? For instance, I disabled the connection from my TVs, thermostat, and cars to my router.
- Patch all software/firmware (especially the router itself).
- Did I mention changing all default passwords?
- No-name bargain brands tend to be less serious about security in their devices. Cheap devices from obscure companies tend to have serious security flaws.
- Literally consider turning off microphones (e.g., Alexa, Home) and cameras (e.g, nanny cams or security) nearby wherever you have set up your home office. By default they automatically record when they detect sound or motion and could accidentally pick up and record sensitive or private information.

I know this involves some extra work on your part, but you end up with a more secure home for yourself, your family, and your organization.

This TIP was written by Glenn Kapetansky, Senior Principal and Chief Security Officer at Trexin. Glenn welcomes comments and discussion on this topic and can be reached at glenn.kapetansky@trexin.com.