The Freelancer's Guide to Cybersecurity Podcast Episode 5: Protecting Your Home Office From Your Smart Home

Episode released 10/28/2020

Transcript

Hey there, on today's podcast, we're going to discuss protection your home office from your smart home.

The FBI has described the surge in IoT devices as giving bad actors—the formal term for hackers—"a virtual drive-by of your digital life." IoT, or Internet of Things, devices are those small "smart" devices people let into their lives without much thought, like fitness trackers, thermostats, televisions, and refrigerators. These devices—maybe precisely because folks don't give them much thought—are vulnerable to bad actors and open all devices in the home to hacking. If you work from home, you need to protect your home office from your smart home.

In most homes, all devices use the same wi-fi router to access the internet, leaving every device in the home as vulnerable as the least-secure device in the home. Those files you secured on your laptop? Not secure, because your smart doorbell (or fridge, or tv, or whatever) has lousy firmware that allowed a hacker to access your home network.

Now, lest anyone fret that any work outside the office is necessarily less secure than on-site work due to these devices, it's important to note that companies and institutions have found that on-site security suffers mightily from employees' use of personal devices on office networks. So these inconspicuous devices we've let into our lives seem to cut a wide swath of cyber vulnerability.

But, if you work from a home office, you absolutely can protect your work and your devices from the personal IoT sharing your network. While the best solution is to run your business and IoT devices on separate networks, that's not practical for most folks. Here are some practical precautions you can take:

1. **Secure your router.** According to Avast, "59.7% of routers have weak credentials or some vulnerabilities" and "59.1% of users worldwide have never logged into their router or have never updated its firmware." In my

experience, many people have not changed the factory preset credentials, leaving their network extremely vulnerable. We provide two resources for you in our detailed show notes that will guide you in securing and updating your router.

2. **Limit IoT devices' access.** If you manage your smart devices with apps, do not accept the default permissions these apps will request without careful review. Does the app for your fitness tracker really need to access your phone's mic and camera? Probably not. As a rule, review the access you grant to every app on a device, and limit that access as much as possible to minimize the risk of a breach.
3. **Protect your devices with secure credentials.** Don't accept preset passwords and use a strong unique password for each device.
4. **Update your devices.** Updates often contain security patches for the firmware installed on your device. If there is an auto-update function, use it.

Working from home can be just as secure (or even more secure) than working on-site, but it requires taking control of the tools you employ to run your business and your home. Even the tiny ones you don't think about much.

Hey, it's Kelly here. Just wanted to remind everybody that, if you find this podcast helpful, please subscribe on your favorite podcast app and share it with others. And if you *really* like it, please be sure to rate it and leave a review! This podcast is new, and any shares, comments, and ratings will help spread the word and support the podcast. Also, if you have any ideas about topics you'd like covered on the podcast, please leave a comment on our website, cyber.dukecityconsulting.com.

Thanks!