Tucker Ellis LLP

Secure Your Home Workspace During the COVID-19 Pandemic

MARCH 2020

Many employees are, for the first time, working from home daily as businesses across the country change their day-to-day operations to protect their employees and the public at large from the novel coronavirus. Just as we have been washing our hands and keeping our distance to protect our health, employees and companies alike should take precautionary measures to avoid undue risks to their data.

Any adjustment to data practices can raise concerns about newer and more creative phishing attempts, potential data breaches, increased vulnerability to ransomware and malware, and other threats both to employees' privacy and to employers' data. Businesses can avoid risks due to vulnerable work-from-home setups or practices by prioritizing the most sensitive risk points.

Now that employees are settled in with their initial setup, here are examples of some steps for work-from-home employees to consider to make their workspace more secure.

Review policies on data security and confidentiality. Most employees have not reviewed their companies' IT and trade secret (or confidentiality) policies since the day they were hired, if then. IT or managerial professionals should send regular updates and reminders to employees to maintain their security hygiene. This presents a great opportunity to have everyone review those policies and for IT or managerial professionals to answer questions about how these apply with equal force in the work-from-home environment.

Clarify personal device etiquette. While the safest option would be for all remote employees to use a corporate device, the reality has many employees working from personal devices. Businesses should remind employees to avoid using personal devices for personal reasons while logged into a company's VPN. Likewise, employees who need to print or scan with a personal device should be discouraged from emailing confidential documents to their personal email to do so. Instead, companies can adjust IT policies to allow personal printer drivers to be installed on company devices.

Secure home Wi-Fi networks. There are several ways to make a home Wi-Fi network more secure. In addition to password-protecting your network, it is also a best practice to not use any personally identifiable naming in the network names. With schools closing, children may be using the same Wi-Fi network in the home, not to mention roommates, spouses, or others

sheltering with you. If possible, create a separate network login (many routers have guest networking capabilities or include a 5G option that you could separate out) to avoid becoming victim to vulnerabilities in less-secure devices.

Keep watch for phishing schemes. This is a good time to be on high alert for phishing attempts. Phishing emails attempt to collect personal information or get users to download malware onto their devices. Currently, there is an uptick in schemes where the phisher imitates the CDC, WHO, or other COVID-19-related authorities. It is tempting to click on links to get all the information possible on the pandemic. A great way for companies to avoid the risk of their employees clicking these links is to provide a company resource page where employees can safely navigate real information about COVID-19.

Vet videoconference services. Videoconferencing technology is a vital piece of the work-from-home puzzle; however, confidential conversations on Zoom, Google Meet, or similar resources should be used with caution due to the potential for security issues on these platforms, especially with their now-widespread use. Zoom recently fixed a bug that had allowed others to access private conferences, but since many of these services are new, additional unknown vulnerabilities may still exist. Further, these third-party services collect data, so a thorough review of privacy and data use policies is recommended.

Securely dispose of physical documents. Most employees will not have shredders readily available to dispose of confidential documents as they would in the office. Employees should not overlook physical document privacy risks, and if employees have private documents to dispose of, they should be kept in a secure location until they can be safely shredded and disposed of.

Double-check social media posts. Photos, videos, and even TikToks of people's work-from-home setups are popular on all social media sites, and they are a fun way to engage employees and improve morale; however, take a second look at your home office photos before posting to confirm that your passwords are not on a Post-it note and confidential documents are not visible. Additionally, avoid posting pictures where the type of computer equipment, specifically brand names, is visible, because would-be hackers can use this information to better attack your company's systems.

For employees who are adjusting to working from home, these measures can help avoid unnecessary risks to their data and their employer's data.[1]

[1] This Client Alert was prepared with the invaluable assistance of Tucker Ellis intellectual property law clerk Helena Guye, a third-year law student at the University of Missouri School of Law.

Tucker Ellis LLP

Client Alert