Payroll Data Privacy in the Time of Working From Home

BY DANIEL MESSELOFF, ESQ., AND JANE DAVIDSON, ESQ.

Happy New Year! Not 2021, but year two of companies adjusting to a remote workforce, where employees must monitor their own payroll records from afar. Many payroll professionals themselves are working remotely, too, and trying to juggle all their responsibilities. Just as all of us have been wearing masks, washing our hands, and keeping our distance to protect our health, payroll professionals and other employees should take precautionary measures to avoid undue risks and protect their data.

Payroll professionals handle sensitive employee data, so maintaining best practices is essential to everyone's security.

Payroll professionals frequently handle sensitive data, but bringing that data into their homes adds additional privacy concerns that are important to maintaining employees' privacy and avoiding a data breach.

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 companies' data. Payroll professionals can avoid their own risks due to vulnerable work-from-home setups or practices by prioritizing the most sensitive risk points.

Here are examples of some steps for work-from-home payroll professionals and other employees to consider making their workspaces more secure:

Review Policies on Data Security, Confidentiality

Payroll professionals handle sensitive employee data, so maintaining best practices is essential to everyone's security. Most employees haven't reviewed their companies' IT and trade secret (or confidentiality) policies since the day they were hired, if ever. 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 payroll professionals to use a corporate device, the unavoidable reality is that many employees work from personal devices like their own computers and/or phones.

Avoid using personal devices for personal reasons while logged into your company's VPN. Likewise, if you or other employees need to print or scan with a personal device, try not to email confidential documents to your personal email address to do so. Instead, companies can adjust IT policies to allow personal printer drivers to be installed on company devices. If you have been using personal email or devices to send or receive sensitive employee data, then do some spring cleaning to permanently delete any files from those unsecured locations.

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 anything personally identifiable in the network names. With some schools still closed, 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. If

---

Daniel Messeloff, Esq., and Jane Davidson, Esq., are attorneys with the law firm of Tucker Ellis LLP, based in Cleveland, Ohio. They assist payroll professionals and other executives with helping their companies comply with a wide range of laws. Messeloff is also a member of the APA's Board of Contributing Writers for PAYTECH. *They can be reached at Daniel.Messeloff@tuckerellis.com and Jane.Davidson@tuckerellis.com.*

you are concerned about the security of your home internet, bring this concern to IT and to management to confirm your network's security and/or request your company's help with these types of upgrades.

Keep Watch for Phishing Schemes

"Phishing" emails attempt to collect personal information or get users to download malware onto their devices. This is a good time to be on high alert for phishing attempts, as there are many circulating that contain fraudulent wait lists for vaccines or impersonating the Centers for Disease Control and Prevention (CDC), World Health Organization (WHO), or other COVID-19-related authorities. 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, Microsoft Teams, 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 fixed most of its early 2020 issues, but since many of these services are new, additional unknown vulnerabilities may still exist. These third-party services also collect data, so you should thoroughly review the services' own privacy and data use policies.

Securely Dispose of Physical Documents

Most employees will not have shredders readily available to dispose of confidential documents as they would in the office. Don't overlook privacy risks with handling physical documents. If any employees have private documents to dispose of, they should keep them in a secure location until they can be safely shredded.

Double Check Social Media Posts

Connecting with others online is an important part of maintaining a sense of normalcy in a work-from-home environment. 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 aren't on a Post-it Note and that confidential documents aren't visible. Additionally, avoid posting pictures where the type of computer equipment, specifically brand names, is visible. Would-be hackers can use this information to better attack your company's systems. Finally, whether physical or electronic documents, payroll documents can contain sensitive data that can be visible in photos. Remember, other members of your household may be creating content as well, so make sure they are aware of your safe social rules.

Now that employees have become more comfortable in the work-from-home environment, assessing and updating data practices is a necessary and timely step to avoid unnecessary risks. A 2021 data protection practices assessment is an easy way to make sure everyone is on the same page. ■

This article is for educational purposes only. Nothing in this article should be construed as legal advice. Specific questions should be addressed with an attorney.