NOW + NEXT

DATA PRIVACY AND SECURITY LAW ALERT | NIXON PEABODY LLP

MARCH 23, 2020

How to protect your remote workforce from cyberattacks: Tips to consider as working from home becomes the norm

By Jason Gonzalez, Jenny Holmes, and Troy Lieberman

As employers and employees are adjusting to the new "normal" of working from home, the risk of a cyberattack has never been greater. Hackers are preying on innocent employees and their lax cybersecurity practices as an easy way to gain access to organizations of all sizes and across all industries. Now, more than ever, it's important to remind your workforce to remain vigilant about cybersecurity. Employers should consider circulating any company privacy or information security policies as a helpful reminder for employees. It's imperative that your employees review and understand these policies. We encourage employers and employees alike to try to maintain the same or similar security standards as normal.

We put together a few additional reminders as we navigate this challenging time:

- Working outside the office may mean that others can more easily see confidential information on a computer screen. Be sure to log off or lock your computer when stepping away from your work station, even for a short period of time.
- Even while working from home or elsewhere out of the office, employees are still responsible for complying with all company policies and procedures. This includes complying with any non-disclosure or other confidentiality agreements that may be in place.
- Be especially vigilant for phishing scams and avoid opening attachments from any untrusted emails. These can include purported "coronavirus" or "COVID-19" alerts; unfortunately, scammers are taking advantage of the current situation. Employers should encourage employees to check with the company's IT department if they have any questions about the validity of a particular email before opening any attachments.
- Employers should require that employees use the company's VPN system or similar remote access system to connect. Employees should be reminded to not save documents locally on their computer and to not use personal webmail or texting to conduct company business.
- Employees should avoid printing out documents at home. If an employee must do so, they should not throw any confidential documents in the trash or recycling when finished. Employees should save all documents somewhere safe and private, and bring them to work for

secure shredding once the office reopens.

- Be cognizant of smart-home devices. Even though such devices are designed to only be activated by certain words, one study has shown that these devices can inadvertently activate between 1.5 and 19 times per day. Confidential conversations should happen away from such devices.
- Employees should update the password on internet modems and wireless access points to make sure they are not still using the default password that came with the device. Hackers can purchase those passwords on the dark web and gain easy access.
- Everyone should be sure to completely shut down his or her computer every night, and reboot it in the morning. This helps keep it more secure.

Above all, employees should be advised what to do and whom to immediately contact in the event of a suspected or actual data breach. Be mindful to encourage employees to self-report any incident, rather than instill fear. While your employees can be the company's biggest weakness in terms of data security, they can also be your first and best line of defense.

Finally, we strongly recommend considering whether any changes to your information security programs are warranted. Many state laws require review and updates of privacy and security policies as company circumstances change and moving an entire workforce to a remote situation is certainly a material change.

Get the latest updates on the evolving COVID-19 pandemic. New info posted regularly on nixonpeabody.com.

For more information on the content of this alert, please contact our Coronavirus Response Team, your Nixon Peabody attorney, or:

- Jason Gonzalez at jgonzalez@nixonpeabody.com or 213-629-6019
- Jenny Holmes at jholmes@nixonpeabody.com or 585-263-1494
- Troy Lieberman at tlieberman@nixonpeabody.com or 617-345-1281