KOLEY ■ JESSEN

Tips to Promote a Secure Remote Working Environment During COVID-19

03.16.2020

ATTORNEYS

Maureen E. Fulton

PRACTICE AREAS

Data Privacy and Security

Has Your Company Instituted a Work-From-Home Policy Because of COVID-19?

In order to achieve social distancing during the COVID-19 coronavirus outbreak, millions of employees in the United States are either already working from home, or businesses are sprinting to prepare for their employees to work remotely. As everyone settles in for what could be weeks or months of remote work, it is important to ensure that companies, and their workers, are aware of heightened cybersecurity risks facing them and follow best practices when it comes to keeping company systems and data secure.

On Friday, March 13, the Cybersecurity and Infrastructure Agency ("CISA"), part of the United States Department of Homeland Security, **issued an alert** encouraging companies to "adopt a heightened state of cybersecurity" when considering alternative workplace options. CISA's alert advised businesses to update their hardware and devices to push through security patches; alert employees to an expected increase in phishing attempts; ramp up remote access cybersecurity tasks; implement multi-factor authentication and strong passwords; and test system user limitations.

Below are five tips that your business and its employees should consider following to protect against malware, hacking, and ransomware:

Tips to Promote a Secure Remote Working Environment During COVID-19

1. **Don't Click on That Suspicious Link or Open that Unfamiliar Attachment**

This is an important reminder at any time, but it is especially imperative now, when stress is heightened and guards may be down: implore employees to be very cautious when clicking on links or opening attachments that are sent in emails. Hackers are sending out many more phishing attacks than usual, some related to COVID-19 to prey on eagerness to learn more about the virus and the latest updates, and some that are unrelated. For example, a malicious website is circulating in phishing emails that purports to be the live map for COVID-19 global cases run by Johns Hopkins University.

Encourage workers that for each email they receive, they should look carefully at the subject line and the sender to ensure legitimacy. They should not click on a link unless they are sure they know the sender's email address is correct by closely examining the email address. Employees should not open any attachments unless they were expecting an attachment to be sent.

2. **Require Stronger Passwords and Multi-Factor Authentication For Sign-Ins**

Your business might have a password strength requirement for employees signing onto the network, such as minimum character length, use of special characters, etc. To the extent you can bolster those requirements by mandating employees use longer passwords (as one example, a 15- to 20-character passphrase) that is changed every 90-120 days, do so. If you have the ability to enable multi-factor authentication for network sign-in – requiring the use of a text message or phone call in conjunction with a password in order to log on – do so. What are initially minor inconveniences with respect to verifying sign-ins will become routine. Multi-factor authentication is one of the easiest fixes that goes a long way toward protecting your system.

3. **Institute and Enforce Company Cybersecurity Policies**

Perhaps your business does not have prior extensive experience with remote working, and therefore work-from-home policies have not yet been put into place. Now is the time to institute cybersecurity policies to let your employees know what is expected of them to protect your business' systems and data when working remotely.

For example, enact a policy that remote workers should only use company-approved computers and are not allowed to download any work information onto a personal computer that has not been approved for work use. As another example, institute a directive prohibiting workers from connecting to public WiFi on their work or company-approved laptops. These policies will minimize data theft or compromise.

4. **Use the Telephone for Any Sensitive Business Such as Wire Transfers or Sharing Confidential Information**

When not in the office, it is easy to fall into the habit of transacting all business by email. When conducting any sensitive company matters, however, it is best to pick up the phone and call. Ask for double or triple confirmation for wire transfer transactions or when sending or receiving company confidential information. If anything in an email seems off or even not as straightforward as you would like, a verbal confirmation will ease your mind.

5. **Offer Resources to Answer Your Employees' Cybersecurity Questions**

Make sure your employees know that if they have questions about a strange-looking email or website, or how they can complete a transaction in the most secure manner, they have the ability to ask someone in your company for assistance. Your system is only as strong as your weakest employee, and ensuring open lines of communication will help protect against intruders. Offer a dedicated email address or contact person for employees to be able to call with questions or concerns.

Koley Jessen continues to monitor the situation and stay current on cybersecurity issues in light of the COVID-19 coronavirus outbreak. If your organization has additional questions or concerns as the situation develops, please contact a member of the Koley Jessen Data Privacy and Security practice area. Koley Jessen team members are also available to draft any cybersecurity policies that your business may need to put into place.