Hughes Hubbard & Reed

Working from Home: Best Practices for Data Security

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

Attorney advertising. Readers are advised that prior results do not guarantee a similar outcome. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. For information regarding the selection process of awards, please visit https://www.hugheshubbard.com/legal-notices-methodologies.

March 30, 2020 - The COVID-19 pandemic is forcing millions of people to work from home on a sustained basis—many for the very first time. This abrupt shift is creating challenges for employers and employees alike, and companies have been doing their best to help their personnel adjust to the new paradigm. While company efforts should continue to emphasize health and safety, this is a good time to remind work-from-home personnel about cybersecurity. To assist companies in doing so, here are ten ways that work-from-home personnel can protect company information.

1. Follow Company Policy. In most cases, a company's regular work-from-home procedures should continue to apply. Companies should review existing policies and remind their personnel to comply with them.

2. Watch Out for Phishing Emails. This is a time of heightened phishing activity as hackers try to take advantage of the current situation. In addition to the usual phishing attempts, there have been reports of fake emails—purporting to come from the CDC or local authorities—touting important information about the virus. Work-from-home personnel should be especially careful not to click on links or attachments in unsolicited emails.

3. Continue to be Vigilant about Scams. Work-from-home personnel should also be wary of scams. On March 23, 2020, the FBI and the Department of Health and Human Services separately issued alerts describing common COVID-19 scams, many of which seek to obtain personal information or money for bogus treatments or testing.

4. Work on the Network. To maintain security and ensure work is backed-up, work-from-home personnel should work in the company network environment. This typically means using remote-desktop software or VPN networks.

5. Do Not Use Personal Email. To maintain security and ensure confidentiality, work-from-home personnel should not be using personal email accounts for business purposes.

6. Use Secure WiFi. Work-from-home personnel should be using secure Wi-Fi connections. It is relatively easy to configure a home router for security and encryption, and those who need help should contact the IT department.

7. Log Off Computers and Install Updates. Work-from-home personnel should remember to log off and shut down computers and devices. This allows IT to push important security updates to such devices. Users should also install updates when prompted; if they are not sure an update is legitimate, they should contact IT to check.

8. Keep Company Information Confidential. When working from home, it sometimes takes special effort to keep company information confidential and secure. If possible, work-from-home personnel should find separate areas in which to work. They should also do their best not to let family members see confidential materials in electronic or hard copy form.

9. Guard Conversations. Work-from-home personnel should be careful when participating in telephone conferences and on-line presentations, especially when using a speakerphone.

10. Dispose of Hard Copy Information Securely. Finally, work-from-home personnel should be careful to dispose of hard copy information in a secure way. For paper documents, this means shredding the document, and not just throwing it in the trash. Employees can also try to minimize this issue by printing on-line materials only when necessary.

Click here to go to our COVID-19 Resource Center for more advisories, articles and other content related to the coronavirus pandemic.

Related People

Charles W. Cohen

Seth D. Rothman

Related Areas of Focus

Data Privacy & Cybersecurity