M&M CONSULTING | Partners in Risk Management

To our Clients:

Many of our client's employees are working at home during the health emergency. The ability to work remotely can be a big advantage but also comes with increased risks including COVID-19 phishing attacks, malicious code disguised as COVID-19 information, denial of service attacks, exposed passwords and credentials, device theft and many others. We are advising our clients and employees who are working remotely during this period to consider the following:

1. Follow the latest FFIEC Interagency Statement on Pandemic Planning.
2. Have a remote access policy which includes connectivity requirements and is enforced.
3. Multi-factor authentication should be used for remote access.
4. Ensure that employees are trained to recognize spear phishing.
5. Wherever possible, employees should not use their personal devices for access. If not possible, there should be endpoint anti-malware protection on each device, at minimum.
6. Use an encrypted virtual private network with a time-out. If a remote desk top protocol is used, transmissions should be encrypted.
7. Use mobile device management software.
8. Stress test the network for remote users.
9. Home network should use WPA2 wireless encryption.
10. Change the router default password then periodically change your password.
11. Remote access server should be placed on the network perimeter; there should be one remote access point.

We at M&M, our clients, and employees endeavor to work safely and securely during this difficult time. Please contact us if we can be of assistance during this period.

Respectfully,

Dean Stockford

President & CEO
M&M Consulting, LLC