



Frequently Asked Questions:

Cyber Security Risks in Today's Work from Home Environment



You mentioned that if using a Virtual Machine, you could potentially download viruses and it wouldn't infect your Physical PC. If you get ransomware in a VM, will that only encrypt the VM?

The malware would most likely infect the Virtual desktop operating system. Ninety-nine percent of the time you can expect ONLY the Virtual Machine to be infected. A hacker would have to use an incredibly sophisticated attack to affect the host machine.



If we log into a work network, do we need to abide by the same Home Network Security protocols?

If you are logged into a work network from home, you should follow your organization's security protocols. However, when working from home you should always turn your computer off after you are done with a work session and make sure any physical files are locked up at the end of each day. It might not be a bad idea to implement some home network security protocols in your work environment if you notice a gap in the cyber security (for example using multi-factor authentication or frequently changing passwords.)



WINONA

ROCHESTER

SAINT PAUL

LA CRESCENT

WALiveBIG.com

The information contained herein is for informational purposes only. It may not be appropriate for your particular situation and should not be taken as legal advice. You should contact an advisor or legal professional for advice about your situation.