

Donovan Rhone is a Senior Account Manager for Knight Office Solutions and has been in the office equipment industry for over 25 years, specializing in working in the AEC Industry for the past 15 years. Along with Managed IT Services, Mr. Rhone also helps companies by providing printers, MFPs, plotters and document workflow solutions. He is passionate about customer service and bringing the latest technology to all of his customers.

Security Best Practices: Working from Home

The world is changing, and nowhere is this more apparent than in the workplace. As cloud technologies empower mobility like never before, many organizations are considering work-from-home as a permanent option for their employees. Unfortunately, cyber criminals have taken note of this. Protect your organization from attack with these best practices for working remotely:

Be aware

Stay especially mindful of phishing attempts when you work from home. If you receive a suspicious email, report it to your IT department before you click on any link or open any attachment. Keep an eye out for emails that seek to capitalize on the current pandemic.

Another popular tactic used by criminals: Posing as your boss. If you receive an unusual email from someone purporting to be a superior or colleague, verify its legitimacy by phone before you engage with the email. Typically, these messages will include an urgent appeal for help. Don't be fooled—this is merely a strategy to keep you from taking a second look at the request.

Be proactive

Double check that all hardware and software have received the latest updates and patches, especially your antivirus program. Additionally, enable two-factor authentication on any accounts that allow it.

Be safe

Never connect to a Wi-Fi network that is not secured with a password, and do not access sensitive information from any public network. Similarly, make your Bluetooth devices undiscoverable when in public places. Criminals can use Bluetooth as a way to gain access to your devices. Need to access data stored on-premises? Be sure to use a trusted VPN with a valid security certificate. Finally, report lost or stolen devices as soon as possible.

