

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.

How Can Ransomware be Prevented?

It's Monday morning. You just sat down at your desk and you're determined to start the week with a clear inbox. That's when it happens. Without thinking, you download a seemingly innocuous attachment without double checking the sender. Suddenly, a popup flashes across your screen:

> ATTENTION! All your documents, photos, databases and other important files are encrypted. The only method of recovering files is to purchase a unique private key. Only we can give you this key and only we can recover your files.

Your heart sinks. You've been hit with ransomware. Questions race through your mind: How did they get through our firewall? What do we do now? How is this going to affect our operations?

Hopefully this situation hasn't played out in your office. If it has, take a deep breath—you're not alone. A June 2018 report from McAfee Labs identified over 16 million strains of ransomware. How many attacks is that? The subversive nature of ransomware makes it difficult to identify the exact number, but experts estimate that a business falls victim to ransomware every 14 seconds.

Four organizations have just fallen victim to ransomware in that minute, and the number is only expected to increase as new strains are introduced. What's more? SMBs are particularly vulnerable to this type of attack because they have smaller IT departments and/or fewer resources to invest in the latest prevention technology.

"So, what's the best way to avoid ransomware?"

Ransomware is a formidable opponent, but there are ways to protect your organization from attack. Like other issues of IT security, experts recommend a multi-pronged approach. The best defense for ransomware is a combination of:

1. Education – It's critical that your users understand how ransomware is spread, and the danger it poses to your organization. Share examples of ransomware emails and provide a clear process that outlines the steps a user should take if they identify a threat.

2. Software & Patches – Maintain up-to-date antivirus and anti-malware software. Double check that all business applications are current with the latest security patches.

3. Backup Management – Invest in a business continuity/disaster recovery solution (BCDR) that creates regular backups and data recovery points. A properly configured (and tested) BCDR program will allow you to roll-back your data to a point before the corruption occurred in the event of an attack.

Do you have questions about your organization's security preparedness? Schedule a comprehensive risk assessment with one of Knight's managed IT consultants and take the first step toward a more protected IT environment.

