GROVE BANK & TRUST

# 8 Simple Steps to Protect Your Company from Ransomware

July 2017

## What is Ransomware?

Ransomware is the digital version of extortion. It's as simple as that. It uses age-old tactics to carry out a modern day crime, but the elements behind it are as old as human criminal activity itself.

## 8 Simple Tips to Protect Your Data from Ransomware

**1. Back up your files regularly.**
The only way to ensure that you can immediately handle a ransomware attack is to implement a regular backup schedule so that your company can get access to the files it needs without dealing with cybercriminals. Your backup should have certain restrictions such as read/write permissions without an opportunity to modify or delete files.

**2. Check your backups.**
There are times when something can damage your files. Be sue to check regularly that your backups are in good shape.

**3. Protect against phishing attacks.**
Cybercriminals often distribute fake email messages that look like an official message from a vendor or bank, luring a user to click on the malicious link and download malware. Teach employees that they must never open attachments from an unknown sender or even suspicious attachments from a friend in case they have been hacked.

**4. Trust but verify.**
Malicious links can be sent by your friends or your colleagues whose accounts have been hacked. Let employees know that if they receive something out of the ordinary from a friend, they should call that person directly to verify that they sent it and find out if their accounts have been compromised.

**5. Enable 'Show file extensions' option in the windows settng.**
This will make it much easier to distinguish potentially malicious files. Because Trojans are programs, employees should be warned to stay away from file extensions like "exe", "vbs",

and "scr". Scammers could use several extensions to masquerade a malicious file as a video, photo or document.

**6. Regularly update your operting system.**
Cybercriminals tend to exploit vulnerabilities in software to compromise systems. With the right assessment and management tools you can rest assured that your system will be scanned and that patches will be distributed regularly in order to keep your system updated.

**7. Use a robust antivirus program.**
Protect your system from ransomware by using a multi-layered system of defense that checks malware from many different angles to ensure that it does not corrupt your system.

**8. If ransomware hits...cut off your internet connection immediately.**
If you discover ransomware, shut off your internet connection right away. If the ransomware did not manage to erase the encryption key from the computers in question, then there is still a chance you can restore your files.

**Frank Iglesias**
Senior Vice President
Chief Compliance & Risk Management Officer