3008 Dawn Drive #106 Georgetown, Texas 78628

Ransomware

What you can do to protect yourself, your clients and ultimately your business reputation!

1st let's examine our natural behavior. We've become so used to getting every important document or communication sent via email, a link, or a text message that we are actually numb to the all the info that we open.

For example, let's say you are in Human Resources, well of course you're going to need to open that PDF resume, it's part of your daily job function. Or let's assume you work in the shipping department of your company and you use FedEx and UPS to ship packages every day. Of course you will have to click on the tracking link because you need to know if your shipment was signed and delivered successfully. Or maybe you are in marketing and you are constantly on LinkedIn and Facebook creating and updating posts for your online business presence. So when you receive that LinkedIn "accept this invitation" button, it's normal that you automatically click it.

If you have employees in mind right now that you think this applies to, or if this sound like you, then you need to be armed with information on how to protect yourself and hopefully you can prevent this from happening to you:

1. Have a Backup Offsite and Test It

   Some people balk at this because maybe they fear that having an offsite backup may put too much of their information in "the cloud" or maybe it just seems like it's expensive and that can't quantify or justify they costs. That is, until they need it. Having a backup off-site, disconnected from your computer is the single biggest thing that can defeat ransomware. If you are attacked this morning, you may lose the document from 30 minutes ago, but if you can go back to last night, it gives you a huge sigh of relief.

   Make note that ransomware like Cryptolocker will encrypt your USB thumb drives, your cloud files you have assigned as a drive letter, your mapped network drives and any external drive you have physically plugged in. It will crawl across your network and hose all of your data. Having a snapshot of your system and a backup regimen that is regularly tested is a must, and it's been proven to be the only true way out.

2. Invest in a Firewall with Advanced Threat Protection

If you run a small business and accept credit cards or use financial accounting software, the residential router/ firewall boxes you can pick up at the local big box store are really not sufficient. You don't have to have 400 employees to still have the need for a commercial firewall box with advanced threat protection.

If you are a small accounting firm with only 5 employees, you still need the protection that the 400 employee company has, the modem/router/firewall combo box that your ISP gave you isn't enough. The threats out there aren't customized by the size of your business… they are all the same. The big guys only have an advantage because they usually have a staff of IT pros trying to protect their network and investing in equipment. You can invest in similar equipment with the right amount of protection and if its all too confusing, you don't have to navigate the waters alone. At Computek we will guide you and help determine what protection best fits your business and your budget!

3. Train Employees

Cyberthreats are often totally blamed on outsiders and malicious code designed to penetrate your network and pilfer your confidential information and we addressed what we can to do mitigate that in item **# 2 above**. However, sometimes the threat actually originates from ***within*** your organization. Training your employees on what to watch for and what to do if they are uncertain, or what to do ***after*** they have erroneously clicked on a link has an enormous impact on how well you are able keep your company data safe.

One company we support recently decided to send a rogue, but somewhat convincing social email throughout its organization. They wanted to actually see how many users could be duped. The click through rate (meaning it tricked the users) was 39%. Cybercriminals know this tactic works too and that's why they use it! This is a topic that is more in-depth than we can cover in just a few paragraphs here, so if you feel like you need assistance or would like us to do a lunch and learn to help your organization, just give us a call. We like to educate not alienate your users, and we like to encourage cooperation, not just compliance!

4. Use a Comprehensive Antivirus Security Suite

If your current IT company is allowing you to use a free security suite… fire them! You get what you pay for and don't you think your information and your network are more valuable than free? Hackers do too!

5. Patch and Update Your Systems Regularly

This is the easiest to do on the list. On our Computek Managed IT service plans we automate your patches and updates so that all users are regularly maintained across your organization, but if you are a home user this is something you can do as well. Just keep your Windows updates turned on and update Java and Adobe products directly from their respective websites.