LAN Infotech
YOUR TECHNOLOGY IS OUR BUSINESS

WHITE PAPER

5 STEPS TO BETTER SECURE YOUR NETWORK

We all know that there are viruses out there, but just how expansive is the threat landscape, exactly? Well, according to Verizon's 2015 Data Breach Investigations Report, 317 million new pieces of malware were created in 2014, and that total is expected to be even higher for 2015.

That's a lot of threats... but why should you care?

The effect that a malware infection could have on your bottom line should grab your attention, as the financial consequences of an online security breach are absolutely devastating. Losing other people's sensitive information that's stored on your network could cost you millions through class-action lawsuits and regulatory fines (healthcare organizations have HIPAA, financial organizations face SEC and FDIC audits, anyone who accepts credit cards must comply with PCI DSS, etc.).

There's also your reputation to consider: a breach will ruin many of your current relationships and drive away potential clients. It's nothing personal; they just don't want to risk compromising their data by trusting it to a network that's known to be vulnerable.

Following these **5 steps** will make your network better protected from all the threats that are out there:

1. Keep Up with the Latest Updates and Patches

With hundreds of millions of new pieces of malware introduced every year, it's getting harder and harder for those fighting the cybercriminals to keep up. The major software companies do try though, and they're always releasing updates and patches for their products that correct vulnerabilities and protect users from the latest known threats.

The problem is that oftentimes these updates aren't automatic, so it's up to you to seek them out and download them yourself. Doing so will go a long way towards protecting your sensitive data.

2. Long and Strong Passwords

There's a reason why some sites won't even let you create a password unless you throw in some numbers and special characters. It's for your own good, as there are programs out there that run through dictionaries at incredible speeds and can find any simple password by trial-and-error, so you need more than just letters.

Length is another factor: generally, you want to shoot for at least 8 characters. And do something more creative than just adding "1" to the end of a normal word, because many password-cracking programs are on to that, too.

In addition to good length and using a mix of letters, numbers, and special characters, you should also make sure that your password isn't inspired by any information that could be found publically on your Facebook or other social media accounts. Favorite movies, music, quotes... your password shouldn't be anything that you've ever mentioned online. Don't use anything that can be found outside your head.

3. Only Open Attachments and Follow Links from Emails you're Entirely Sure Are Legitimate

One of the most popular ways for malware to spread is through deceptive emails. We've all heard about Nigerian princes and know to avoid such obvious schemes, but many phishers are more sophisticated with their craft and can be reasonably convincing, tricking their victims into following a link or downloading an attachment that actually infects their computer with a virus.

For example, recently there's been an email floating around that offers a free upgrade to Windows 10. Although Microsoft does offer free upgrades to Windows 10 (on the condition that you're already running Windows 7 or Windows 8), they're not sending anyone emails about it.

No, when people follow that link for the "free upgrade", they end up infecting their computer instead of getting that promised upgrade, in this case with ransomware. That's a particularly frustrating problem, as ransomware will encrypt your most important files (documents, photos, videos, databases, the works) and offer to decrypt them only if you send over some money, usually totaling somewhere between a few hundred to a couple thousand dollars. If you don't pay up, your files are gone forever.

You can avoid these threats by simply not opening any attachment or following any link from a source you're not 100% sure about.

4. Stay Safe on Public Wi-Fi

There are many benefits to cloud computing, with one of the most valuable benefits being that the cloud mobilizes your workforce. Employees can access their tech tools and business data anywhere they can find an internet connection instead of being limited to the office, and more availability means they can get more work done, finish projects faster, and produce more revenue.

But if you're not careful, the convenience of the cloud can open you up to some serious security risks. Especially if you're using unsecured public Wi-Fi at a coffee shop, hotel lobby, or wherever else you find it, as anyone else could be using that connection, too. Maybe even a cybercriminal who knows how to turn a shared connection into a golden opportunity by using it to intercept your data, and we already warned you about the consequences of data loss (class-action lawsuits, regulatory fines, etc.).

Using strong encryption protocols and virtual private networks (VPNs), among other mobile security technologies and techniques, will allow you to take advantage of the benefits of the cloud without putting your sensitive data at risk.

5. See a USB Stick in the Parking Lot? Don't Pick It Up

Not all attacks are web-based.

One of the more clever breach methods we've seen pop up recently is for a cyber-criminal to strategically place a USB stick, loaded with malware of course, between your parking lot and your entrance.

More often than not an employee will notice the thumb drive, pick it up, and then plug it into a work computer just to see what's on it. And once that drive is in, your network is infected. This trick is even more effective if the perpetrator goes through the effort of printing your company logo on the thumb drive.

They say curiosity killed the cat. Well, turns out it can also lead to a security breach. Train your employees to think critically about what they introduce to work computers, whether it is USB sticks or the phishing links and attachments we mentioned earlier, in order to avoid such social engineering attacks.

Give us a call at 954-717-1990 or send a mesage over to Info@LANInfotech.com for more information about our IT security services.