CyberSecurity: Threat Awareness is your Best Defense

In the early days of the internet, most individuals and businesses considered themselves safe from hackers if they had reliable antivirus software. The occasional virus was a nuisance, but typically didn't involve the theft of confidential data. Because it was inconvenient to secure PCs and WiFi networks with passwords, many of us didn't bother. Similarly, when we created website accounts, we didn't think twice about using "Password" as our password because really, what was the risk?

If only internet security was that simple still today! Hardly a week passes now where we aren't hearing about yet another breach, often by companies that we thought we could trust and know had access to our personal data.

Unfortunately, whereas years ago, malicious internet activity was often motivated by technology "nerds" looking to prove that they were capable of breaching networks and releasing destructive viruses, today cybercriminals are most often motivated by money. The "dark web" provides a platform for criminals to exchange data, pass along trade secrets, and generally make their living.An entire industry now thrives making money illegally on the internet, often at our expense.

Many small businesses and nonprofits naively think they won't be targeted by cybercriminals.According to Verizon, 58% of malware attack victims are categorized as small business. Another sobering statistic from a 2017 Ponemon Cybersecurity Study indicates that 61% of small businesses experienced some type of cyberattack in the past 12 months. The reason? Small businesses and nonprofits lack the resources of larger organizations and often don't understand the risks or make it a priority to properly secure their data.

Fortunately, there are some basic precautions that all organizations can take to better secure their environment.

Be suspicious of every unsolicited email. According to the same Verizon study, an amazing 92% of malware is delivered via email. That doesn't necessarily mean a malicious attachment; often it is a less suspicious link within the email that starts the malware infection. Phishing emails (and a clever variation known as "spear phishing" which impersonate a known person to gain the trust of the recipient) have become increasingly more sophisticated and difficult to distinguish from legitimate messages. Office 365 users are particularly susceptible, not because Office 365 is inherently less safe, but because it has a massive user base attracting more sophisticated attacks.

Use complex passwords and change them regularly. If this seems cumbersome (it is!) you're not alone.Criminals count on the use of simple passwords (or the same one used across many websites) to easily gain access. Consider the use of password management software (such as LastPass or Roboforms) to create complex, unique passwords and save them to an encrypted vault. Even better, if offered by your software vendors, enable multi-factor authentication.

Backup data offsite. Ransomware (whereby a virus encrypts network data and demands a ransom payment to release the encryption) is still one of the leading forms of malware.

Often ransomware is able to "crawl" the network and infect all available files including backups. Ensuring an offsite copy (that has been verified and tested) is a proven method to recover from ransomware.

Control access to data. Because end user PCs are the most common sources of malware, controlling access to data may help contain a virus' spread. If a user does not have a business need to access customer or other confidential data, use security controls to restrict their access. For instance, in QuickBooks, assign only permissions that correlate to the person's responsibilities; on a server, assign folder share permissions only as needed.

Secure remote access to your network. Criminals can silently attempt to exploit any available access point into your network. Thus, poorly secured remote access is a common vulnerability. Consider blocking all unattended remote access (especially external vendors who access PCs or other devices in your network) and use virtual private networks which provide additional protection.

Educate your employees. Good cybersecurity "hygiene" starts by having employees who understand the company's expectations, are aware of the risks, and are vigilant about potential cyberthreats. Have employees acknowledge your organization's IT security policy (or create a policy if one doesn't already exist). Regularly review threats with employees and consider implementing recurring phishing and training programs.

Because threats are constantly evolving, internal cybersecurity reviews should be a regular part of your business processes. For stronger protection or a more thorough assessment, ask an IT expert to evaluate your network.

If you have any questions about the cybersecurity, please give us a call at 509.433.7606 or submit a service request online at http://support.simplepowerit.com/

 Last update: 05/24/2019