smart office CONNECT

October 2017
Tech News and Information

pcWorks Professional Solutions plus

Month's Focus

Understanding your back up strategy.

Do you know in your organization what data is being backed up?

Some people think that their workstation or laptop is being backed up each night, only to find out that when they accidently deleted that important file, it was actually on their desk top and was never backed up.

Most workstations are NOT backed up, unless there is some special software installed that is only located on that pc.

This is why it is important to store ALL your files into a secure folder on your server. The server might be an on-premise server or in the Cloud (O365 using SharePoint or OneDrive being the most popular).

This month ask yourself these questions:

1. Does my company have a policy for saving documents and critical data?
2. Is my workstation/Laptop on the back up list as a critical workstation?
3. Am I saving my documents to an area that will get backed up daily?
4. If I delete a file, how do I retrieve critical data?

If you cannot answer all of these questions, it is time to ask your employer or PC Works Plus about these questions. We have unfortunately run into situations where someone assumed their data was being back up, but when that one file disappears, it is gone for good.

Know your data location!

October is not just scary because of Halloween, it is also Cyber Security Awareness Month!

Myth#1 - I'm not a large Enterprise, so hackers won't attack me. NOT TRUE

61% of the data breach victims were businesses under 1000 employees. You might be well under this 1000 employee mark, but the hackers are looking for easy targets. No one is exempt from cyber-attacks. Security expert and Datto CEO Austin McChord told FOX Business that while small businesses are targeted every single day by ransomware, paying the ransom renders an entity more likely to get hit again.

Myth#2—I don't have the funds or the resources for Cybersecurity NOT TRUE

Some of the most basic implementations:

* Awareness training for your employees, can mean a huge savings in possible pay outs of ransomware or someone just clicking on the wrong thing. A simple Phishing Test can show you where your employees are with their awareness. (Did I mention that this phishing test is FREE???) See how much Alabama County paid in their Ransomware attack.

* Two factor authentication on your O365 and other critical software is not a big investment and is a great way to keep non-authorized people off of your network.

* Giving two log ins to those needing ADMIN rights to make changes to your network. They use their Admin rights log in for management purposes and their other log in of doing their day to day work. NEVER do daily tasks with ADMIN RIGHTS.

Myth#3—Technology will fix everything. NOT TRUE

Without policies and procedures, your employees are not aware of the do's and don'ts of the technology and what compliances your company fall under. This is where a Risk Assessment comes into play. Whether or not you fall under a larger federal compliance like HIPAA or you have regulatory compliances like PCI, it is all about your Policy. Make sure you have a clear and written policy.

If you have any questions or concerns on your Cyber security or would like your FREE Phishing Test, contact us at :

Compliance@pcworksplus.com

Don't make this a scary month because of a hacker attack.

Budgeting for 2018 Cyber Security

Is Cyber Security a line item on your 2018 budget? Gartner Research is showing security spending rising by 8% world wide.

√ Disaster Recovery Plan with a good back up plan

√ Risk Assessment for Compliance regulations

√ Mobile Device Management (MDM)

√ Cyber Security Awareness and Training

√ Policies and Procedures for data protection

These are the items we are seeing that have an effect on our customers. They need to think of these items to make sure they can keep their business running. Preventing and having a good strategy to protect your clients, employees and data are critical components of your Cyber Security strategy. It is time to start budgeting to PREVENT, rather than REMEDIATE a cyber attack or a mishandling of your important data.

Have you seen the HIPAA Wall of Shame? Something as simple as a loss of a laptop without encryption that contained patient information, can cause a breach and an investigation by the HHS Office of Civil Rights.

Having a good back up and policy can help deter the hackers

Let us help you with your budget numbers for your Security and Compliance concerns.

Email sales@pcworksplus.com for a consultation.

Using Microsoft O365 Forms

If you have an O365 subscription, there is a nice and easy way to create forms. Simply log in to http://forms.microsoft.com with your Office 365 school or work credentials, and you can start creating surveys, quizzes, and polls.

This is a very basic application, but if you are just looking for an easy way to survey your customers this is a great way to do it.

Check out this YouTube video on how to create forms.

Miss any of our Newsletters with important tech information from PC Works Plus?
Check out the archive of past newsletters and free reports.

http://www.pcworksplus.com/tech-tips-tricks-and-industry-news/newsletter-archive/