smart office CONNECT

May 2018
Tech News and Information

pcWorks Professional Solutions plus

Month's Focus

This month's Certifications

David Wertz, Joe Pyzowski and Tim Sheehan have just finished their training and certification to become a Certified HIPAA Security Professional (CHSP). The certification shows that they are trained in Healthcare Technology and Regulatory Compliances.

Have you taken advantage of the FREE Security Awareness Training given by David Wertz at your office?

If you want to learn more about

- WHY Cyber Criminals do what they do.
- HOW Cyber Criminals do what they do.
- WHAT you can do to avoid being a victim.

Call 814-742-9750 or email compliance@pcworksplus.com to set up your training.

Employee Security Awareness Training is your best defense

In this day and age, we know that the hackers are trying their best to outsmart us in every way. With all the ways we try to keep our networks, computers and phones safe, there is a hacker in the waiting. One of our best defenses is the "human firewall" - training your employees what to look for and not to be a victim of a hacker's ploy to get you to click or act on something that will get your data in trouble.

One of the ways that we tell clients to keep their data safe, is using 2 factor authentication (2FA). This it the process of using your smartphone or a website that will generate a random number or one-time password to log into important software and help to save your data. With more people using 2FA, the hackers have decided to target these users. Not that this is not a good security measure, but it always falls back to the training of our employees.

Here is a hack…
You receive an email from someone that you *think* you know or a company that sounds legit. They ask you to sign up for a service or if it is a social media ploy, they want to connect. If you accept their offer and you click the "connect" or "interested" button from within the email, it will direct you to the website you would expect, but before this, malware is working in the background to collect your email and password you just used to log into the website. Read this article and watch the video on how this is all done.

One of the best way to keep your employees up to date on all the hacks and what to look for, is Security Awareness Training (SAT). There are many inexpensive ways to keep your employees up to date with the training they need to keep you and your clients data safe.

We can start with a FREE Phishing Test today. I know many of you have seen this offer for the FREE Phishing test, but just have not done it, because maybe deep down inside, you do not want to know how easy it would be for you or your employees to fall for a hackers attack. Don't worry, you are not alone.

Email compliance@pcworksplus.com today to get your educational training started, before it is too late. We would much rather get the call the you want to do a serious training plan than the call that you have just been hacked and you need our services to restore your network.

PS—Ask for the free Dark Web Search to show how many of your employee's emails have been compromised and are being sold on the dark web. Shocking

Could Hackers be using a back door to get access to your data?

You may remember the big Target hack of 2013. Cyber forensics showed that the HVAC company had access to Target's network and was used as the back door to their network.

Healthcare is a big target when it comes to hackers using ways to get into, not only data, but devices. Insulin pumps, pacemakers, MRI and CT scanners are some devices that are targeted by hackers. If a hacker can use the network to access a device, they can take control of the device and change insulin doses, change pacemaker rhythms and give an extra dose of radiation to a patient in an MRI. In August 2017, the FDA and Homeland Security recalled 456,000 pacemakers over the fears that they may have be hacked.

Here are a couple of tips on how to help prevent hackers from accessing sensitive devices:

1. Start with a good Security policy. Do you have a written guideline when it comes to the security of our network and data? If you have a Security Risk Assessment (SRA) you probably have a good written Security Policy. This is a must if you have HIPAA compliances.
2. Have an acceptable use policy, so that all employees know what is acceptable to attach to your network. Do you allow BYOD (bring your own device) cell phones, iPads, or laptops? Are employees allowed to stream music from their personal music subscriptions (Amazon music, iHeart Radio, iTunes)? Do you allow social media to be viewed during the work day? These are some things to consider for not just security reasons, but network performance issues … streaming music can take a lot of bandwidth.
3. Have a training program for your employees. As mentioned before, you need a Human Firewall between you and the hackers. Knowledge is power. The rule for cyber security training is train, retrain and repeat.

Need help with getting your policies written or training plan set up?
Email compliance@pcworksplus.com

Text messaging notifications in Outlook Web App for Office 365

If you are like most people, you use text messaging as a primary mode of communication. Would you like to get text notifications for things in your email and calendar that you want to stand out from the rest of the alerts on your phone? There is a way. Check out this "How to" article on setting up text messaging for calendar events, email rules, and, if you are a Skype user, missed calls and voice mails.

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/