smart office CONNECT

July 2018
Tech News and Information

pcWorks Professional Solutions plus

Month's Focus

Ransomware is still a valid Hacking tool

According to Sonicwall, Ransomware attacks jumped 299 percent. This is staggering when you think of how much we hear in the news about the attacks, but people are still getting fooled.
Why? Because we live on the internet and our email these days. We get so much of our information and news online and we are still hungry for more information. This makes us perfect targets for the hackers.

Hackers are becoming laser focused in their attacks, due to the security solutions that companies are putting into place.

How can you try your best to keep hackers from getting to your company?

Here are a few tips:

1. Update your operating system on your PC, phones and servers- Do you have a computer or server that is over 5 years old? It is more than likely that you are out of the parameters of the security updates the vendors are providing. They may no longer be supporting the version you have, therefore making it very important to update your operating system, if your current hardware supports the upgrade. If not, it is time to replace hardware.
2. Education—One of your largest defense mechanisms is people. Knowledge is power over the hackers. With ongoing training on what to look for and news on the current hacks, people can be vigilant.
3. Back up your data—This is very important, so that if you do get hacked, you have a way to fall back on something that can make your life a lot easier. This goes with your home computers and smartphones, too. What would happen if you could not get to the data on your home pc that stores all your photo memories. That would not be a good day.
4. Anti-Virus and Anti-Malware—Keep these up to date on your PCs. The best security is a subscription based service. These are constantly updating and if there is a hack that is just discovered, vendors are usually pretty quick to find a cure.
5. Cisco Umbrella (which was OpenDNS)- The simplified definition of this tool is that it will block bad websites. You will get a warning that you should not proceed on that website, because there is malicious activity.
6. Firewalls— Older firewalls should be replaced and you should always have a current subscription that will keep your firewall up to date on all threats.

If you have any questions on any of these tips, please email compliance@pcworksplus.com We can analyze your security tools.

FREE

Did you know that we provide some freebies?

- One Free On-site Security Awareness training with David Wertz.
- One Free Phishing Test
- One Free Dark Web search
- Free site survey for phone system upgrades
- Free analysis of your phone and internet services (usually we can find some cost savings)

If you would like to take advantage of any of these free services, contact us today!

Call
814-742-9750

Email
compliance@pcworksplus.com

Visit
109 Stadium Drive
Bellwood PA

Safe Online Banking Tips

Today we use online banking to do almost all of our transactions. You can even deposit a check from your smartphone. That is amazing. Here are some simple tips to make sure that you are safe when using your banking apps or accessing it from a website.

1. Two Factor Authentication—This is a great way to make sure you have secured your account. You will be asked to verify your log –in with a number or additional password that is sent to you via a phone call, text or email.
2. Strong Passwords—This of course is a no brainer. Strong passwords or pass phrases are needed with ALL your online activities.
3. Keep your device and PC up to date - Security patches are always updating on your smartphones and pcs. Make sure you are regularly doing the updates.
4. Avoid clicking on links in emails—If you get an important message from your bank about your account, make sure you do not click on the link to take you to the bank website. This could be a phishing email that is trying to steal your passwords.
5. No public WIFI— This one is kind of a bummer, but one of the worst things you can do is bank on a public wifi. There are hackers that will use devices that spoof a wifi connection and you would really be using their internet. They can track all your moves and steal your account info.
6. Log out when finished—It is a good idea to always log out of your banking session when complete. This does not allow hackers to jump onto an open account.
7. Account Notifications—When you get that email that says you just transferred $10K from your banking account, but you didn't… Happy day that you set up the alerts. Some banks and credit cards will also send you text alerts, so you see that very moment that something happened.
8. Monitor your account—I know that reconciling your bank or credit card statement is not a fun task, but you could catch something that might have happened that month. A lot of banks and credit cards have insurances that will allow you to get a refund on a fraudulent transaction, but you would need to catch it quick.

Sneak Peak Updates in MS Office

Microsoft is doing some revamping of their interface. If you are not a big fan of all the tools, the new interface lets you do a simplified tool bar for the more used functions.

If you want to learn more about this new interface, check out this website with a brief video on the updates.

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/