pcplus networks
better People, better Solutions

Real World Tech Tips

making your business IT reliable & more secure than ever

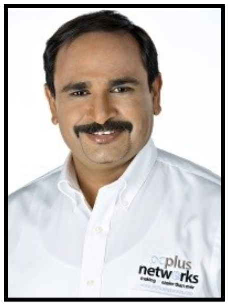
What's New

Using a Passphrase For Security
As a cybercriminal's skills evolve, so too must our passwords. Experts are putting an emphasis on creating strong passphrases to keep accounts as secure as possible. A passphrase is a collection of random words. If done correctly, a passphrase is much harder for a cybercriminal to crack but should be easier for you to remember. An example: Instead of using "There's no place like home." Change it to "There's no place like home or Alaska." Another method is to really make the passphrase random by merging four unconnected words. An example of this is "Itsy, bitsy spider man." So try it.

Quick Tips

1. Try merging four unconnected words to create a strong passphrase.
2. A passphrase is designed to be much harder for a cybercriminal to crack.

March 2020



This monthly publication provided courtesy of Shan Dholaria, CTO of PcPlus Networks

"As a business owner, you don't have time to waste on technical and operational issues plus security is a BIG concern too. That's where we shine! Call us to put an end to your IT problems finally and forever."

5 Signs You're About To Get Hacked — And What You Can Do To Prevent It

Hackers love to go after small businesses. There are many businesses to choose from, and many don't invest in good IT security. Plus, many business owners and their employees have bad cyber security habits. They do things that increase their risk of a malware attack or a cyber-attack. Here are five bad habits that can lead to a hack and what you can do to reduce your risk.

1. Giving out your e-mail Just about every website wants your e-mail address. If you share it with a vendor or e-commerce site, it's usually not a big deal (though it varies by site – some are more than happy to sell your e-mail to advertisers). The point is that when you share your e-mail, you have no idea where it will end up – including in the hands of hackers and scammers. The more often you share your e-mail, the more you're at risk and liable to start getting suspicious e-mails in your inbox.

If you don't recognize the sender, then don't click it. Even if you do recognize the sender but aren't expecting anything from them and do click it, then DO NOT click links or attachments. There's always a chance it's malware. If you still aren't sure, confirm with the sender over the phone or in person before clicking anything.

2. Not deleting cookies Cookies are digital trackers. They are used to save website settings and to track your behavior. For example, if you click a product, cookies are logged in your browser and shared with ad networks. This allows for targeted advertising.

Continued on pg.2

Continued from pg.1

There's no good way to tell who is tracking online. But you can use more secure web browsers, like Firefox and Safari. These browsers make it easy to control who is tracking you.

In Firefox, for example, click the three lines in the upper right corner, go into the Options menu and set your Privacy & Security preferences. Plus, every web browser has the option to delete cookies – which you should do constantly. In Chrome, simply click History, then choose "Clear Browsing Data." Done. You can also use ad-blocking extensions, like uBlock Origin, for a safe web-browsing experience.

3. Not checking for HTTPS Most of us know HTTP – Hypertext Transfer Protocol. It's a part of every web address. However, most websites now use HTTPS, with the S meaning "secure." Most browsers now automatically open HTTPS websites, giving you a more secure connection, but not all sites use it.

If you visit an unsecured HTTP website, any data you share with that site, including date of birth or financial information, is not secure. You don't know if your private data will end up in the hands of a third party, whether that be an advertiser (most common) or a hacker. Always look in the address bar of every site you visit. Look for the padlock icon. If the padlock is closed or green, you're secure. If it's open or red, you're not secure. You should immediately leave any website that isn't secure.

> **"Good IT security can be the best investment you can make for the future of your business."**

4. Saving passwords in your web browser Browsers can save passwords at the click of a button. Makes things easy, right? Unfortunately, this method of saving passwords is not the most secure. If a hacker gets your saved passwords, they have everything they could ever want. Most web browsers require a password or PIN to see saved passwords, but a skilled hacker can force their way past this if given the chance.

Protect yourself with a dedicated password manager! These apps keep passwords in one place and come with serious security. Password managers can also suggest new passwords when it's time to update old passwords (and they remind you to change your passwords!). LastPass, 1Password and Keeper Security Password Manager are good options. Find one that suits your needs and the needs of your business.

5. You believe it will never happen to you This is the worst mentality to have when it comes to cyber security. It means you aren't prepared for what can happen. Business owners who think hackers won't target them are MORE likely to get hit with a data breach or malware attack. If they think they are in the clear, they are less likely to invest in good security and education for their employees.

The best thing you can do is accept that you are at risk. All small businesses are at risk. But you can lower your risk by investing in good network security, backing up all your data to a secure cloud network, using strong passwords, educating your team about cyberthreats and working with a dedicated IT company. Good IT security can be the best investment you make for the future of your business.

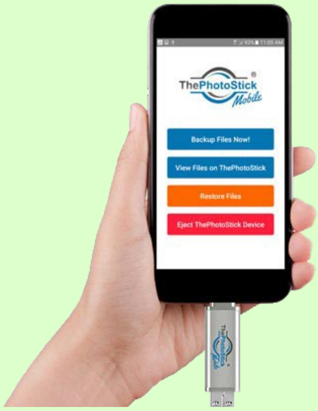
Free Cyber Security Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now

At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber security audit to uncover loopholes in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eye-opener for you, since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.

To get started and claim your free assessment now,
call 678-523-5599.

Shiny New Gadget Of The Month:



ThePhotoStick Mobile

Never worry about running out of memory on your smartphone again! It happens to all of us – you're trying to take a picture or record a video and you get a message saying your phone's storage is full. You don't want to buy another new smartphone, so what can you do besides delete old photos?

This is where ThePhotoStick Mobile comes in. It's a memory stick compatible with most Android and iPhone devices and will boost your phone's memory without your having to buy a new phone. ThePhotoStick Mobile is an insurance policy against lost photos and videos.

ThePhotoStick Mobile gives you more control. While most smartphones work without a hitch for years, you never know if something might happen or if you'll run out of memory. ThePhotoStick Mobile plugs into your device and allows you to copy photos over. You can keep them on ThePhotoStick or transfer them to another device. Learn more at GetPhotoStickMobile.io!

Who Is Responsible For Your Corporate Culture?

"Corporate culture" is the fundamental character or spirit of an organization that influences the loyalty and general behavior of its employees. When you learn how to combine the right corporate culture with the right core values, your organization will thrive regardless of the challenges it faces.

One problem I see in most companies today is they create a mission statement only because it's fashionable to do so … but they stop there. Some may even go so far as to create a list of core values to help guide their leadership and employees … but they fail to follow them. I see lots of mission, vision and value statements on corporate websites, but the majority of employees in any company cannot recite any of them.

Several months ago, one of my clients wanted me to work with their senior management team to identify ways they could create better employee engagement. An anonymous survey was conducted, and it turned up some alarming comments. Over 50% of their employees stated that the company:

- Isn't results-oriented
- Doesn't celebrate accomplishments
- Doesn't have training for growth
- Doesn't allow them to generate ideas
- Isn't empowering them
- Has leaders who play favorites
- Has leaders whose actions do not match their words
- Doesn't involve them in the decisions that affect their jobs
- Doesn't keep them informed about changes or important issues

This company has five excellent "Guiding Principles" (core values) that address all these issues, but they weren't being followed. What most companies don't understand is that their "corporate culture" is in the hands of local middle management. In other words, your corporate culture is your LOCAL BOSS. They are responsible for making sure your guiding principles, core values, and mission and vision statements are being followed.

Last week I did a program for Herr Foods. Herr Foods understands the importance of living their core values. They have been in business for over 70 years and have over 1,500 employees. Their formula for success is based on the acronym L.O.V.E., which stands for:

L - Live
O - Our
V - Values
E - Every day

A recent Gallup poll found that only 34% of workers are committed to their company and are enthusiastic about their work. That means 66% are NOT engaged; they are just going through the motions, collecting a paycheck. As you look to the future, recognize that the principles that are instrumental to your success must be communicated throughout your organization on a constant basis. They should not only be part of your new employee training; they should also be part of every meeting, deeply rooted into every decision you make.

When your corporate culture is right, employees working for you no longer have jobs; in their minds, THEY HAVE CAREERS. ~Robert Stevenson

IT Security Tip: Lie, lie, lie!

Social engineering is big business. What is it? Figuring out who you are and then using that information to make money off of it. People list password challenge and identity verification publicly or at least freely on their Instagram, Twitter and Facebook pages and feeds without giving it a second thought. Maiden name? Check. Favorite pet? Check. High school? Check. Town they grew up in? Check. Favorite or first car? Check. Throwback Thursday is a social engineer's dream! They love this stuff. Combat it by always giving false password and identity challenge and verification information to the sites and services that require it. Keep the answer file offline or at least in a format that's not easily guessed. Remember, if it's a handwritten list, you can still take a photo of it.

pcplus networks
better people, better solutions

1010 Lakes Pkwy
Lawrenceville, GA 30043

Inside This Issue

How People Spy On You When You're Traveling

Long security lines. Crowded airports. Cramped airplanes. Tight connections. Traveling, whether for business or pleasure, blends a hectic mix of physical discomfort and emotional distress. It's in these situations where security awareness becomes even more important. Imagine that you have a 90-minute layover in a busy airport. It's just enough time to grab a quick meal and knock out some work. You find a seat at an overwhelmed café and open your work laptop.

But did you notice...the person sitting behind you? They can easily see your laptop screen. Known as "shoulder surfing," any sensitive data on your screen will surely catch the eye of a social engineer.

But did you notice...that everyone else is using the same WiFi? Connecting to public networks essentially makes anything you access on the network also public. Cybercriminals use public WiFi to steal information.

But did you notice...the person sitting next to you eavesdropping on your conversation? Whenever you find yourself in a public setting, discretion is key. You wouldn't want someone overhearing your private conversation with a client or business associate.

Public WiFi: What's The Big Deal?

Order a coffee. Grab a seat. Connect to the public WiFi. Get hacked. Surely, it's not that simple, right? Believe it or not, stealing data over unencrypted connections (as most public networks are) takes no special hacking skills. Instead, all it takes is data-stealing software (such as packet analyzers) and a motivated cybercriminal. The technical details of how packet sniffing or WiFi hacking work aren't important, though we encourage you to research it and watch a few real-world attacks. What's important is understanding the vulnerabilities of public WiFi.

Login credentials, credit card information, email conversations—anything you send over an unencrypted internet connection can be intercepted and captured. There are two ways to avoid this type of attack.

ONE: Don't connect to public WiFi. It's not ideal, but it's also not paranoia. Security first!

TWO: Always use a virtual private network (VPN) on every device. VPNs provide encrypted connections that help prevent criminals from stealing your data. But even with a VPN enabled, it's still wise to avoid logging into sensitive accounts or making purchases online.