THIS BROWSER IS PROTECTED.
START BROWSING

Did You Know?

If you're using any kind of cloud application (and these days, who isn't?), you are right to be concerned about data privacy and security.

Here's one quick tip you can easily do to improve security in the cloud:

"Reverse"-backup your data. If the data in a cloud application is important, make sure you're downloading it from the application and backing it up in another safe and secure location. That way, if your account is hacked or the data is corrupted, you have a copy.

June 2021

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."

Breaking Bad Habits
4 Ways Your Employees Are Putting Your Business At Risk Of Cyber-Attack

Your employees are instrumental when it comes to protecting your business from cyberthreats. But they can also become targets for hackers and cybercriminals, and they might not know it. Here are four ways your employees might be endangering your business and themselves — and what you can do about it.

1. They're Not Practicing Safe And Secure Web Browsing. One of the most basic rules of the Internet is to not click on anything that looks suspicious. These days, however, it can be harder to tell what's safe and what isn't.

A good rule of thumb is to avoid websites that do not have "https" in front of their web address. The "s" tells you it's secure – https stands for Hypertext Transfer Protocol Secure. If all you see is "http" – no "s" – then you should **not** trust putting your data on

that website, as you don't know where your data might end up.

Another way to practice safe web browsing is to avoid clicking on ads or by using an ad blocker, such as uBlock Origin (a popular ad blocker for Google Chrome and Mozilla Firefox). Hackers can use ad networks to install malware on a user's computer and network.

2. They're Not Using Strong Passwords. This is one of the worst IT security habits out there. It's too easy for employees to use simple passwords or to reuse the same password over and over again or to use one password for everything. Or, worse yet, all of the above.

Cybercriminals love it when people get lazy with their passwords. If you use the same password over and over, and that password is stolen in a data breach (unbeknownst to you), it becomes super

easy for cybercriminals to access virtually any app or account tied to that password. No hacking needed!

To avoid this, your employees must use strong passwords, change passwords every 60 to 90 days, and not reuse old passwords. It might sound tedious, especially if they rely on multiple passwords, but when it comes to the IT security of your business, it's worth it. One more thing: the "tedious" argument really doesn't hold much water either, thanks to password managers like 1Password and LastPass that make it easy to create new passwords and manage them across all apps and accounts.

3. They're Not Using Secure Connections. This is especially relevant for remote workers, but it's something every employee should be aware of. You can find WiFi virtually everywhere, and it makes connecting to the Internet very easy. A little too easy. When you can connect to an unverified network at the click of a button, it should raise eyebrows.

And unless your employee is using company-issued hardware, you have no idea what their endpoint security situation is. It's one risk after another, and it's all unnecessary. The best policy is to prohibit employees from connecting to unsecured networks (like public WiFi) with company property.

Instead, they should stick to secure networks that then connect via VPN. This is on top of the endpoint security that

> **"Education is a powerful tool and, when used right, it can protect your business and your employees."**

should be installed on every device that connects to your company's network: malware protection, antivirus, anti-spyware, anti-ransomware, firewalls, you name it! You want to put up as many gates between your business interests and the outside digital world as you can.

4. They're Not Aware Of Current Threats. How educated is your team about today's cyber security threats? If you don't know, or you know the answer isn't a good one, it's time for a change. One of the biggest threats to your business is a workforce that doesn't know what a phishing e-mail looks like or doesn't know who to call when something goes wrong on the IT side of things.

If an employee opens an e-mail they shouldn't or clicks a "bad" link, it can compromise your entire business. You could end up the victim of data breach. Or a hacker might decide to hold your data hostage until you pay up. This happens every day to businesses around the world – and hackers are relentless. They will use your own employees against you, if given the chance.

Your best move is to get your team trained up and educated about current threats facing your business. Working with a managed service provider or partnering with an IT services firm is an excellent way to accomplish this and to avoid everything we've talked about in this article. Education is a powerful tool and, when used right, it can protect your business and your employees.

Shiny New Gadget Of The Month:

Cancel Stress With Cove

Wouldn't it be nice if you could just press a button and your stress would melt away? Well, now it's possible, and it's thanks to Cove. The first of its kind, Cove is a wearable device (like a pair of headphones) designed with "stress cancellation" in mind.

Cove rests on your ears and wraps around the back of your neck. It uses subtle vibrations behind your ears to soothe your stress. Over 90% of those who participated in clinical trials reported a marked decrease in stress, and 91% reported sleeping better.

If you're looking for a new and innovative way to help manage your stress, Cove may be the answer. Due to its compact, lightweight design, it can be used anywhere, anytime. Learn more at **FeelCove.com**.

Why You're Not Rich Yet

Recently, Petra Coach presented a webinar, Why You Aren't Rich Yet, *with David Waddell and Teresa Bailey of Waddell & Associates. The webinar is aimed at helping entrepreneurs identify key biases that may be preventing them from maximizing their net worth and also shows them how they can change things to actually make a substantial profit. You can see the full webinar at* PetraCoach.com/why-you-arent-rich-yet-with-david-waddell-teresa-bailey

Why You're Not Rich Yet Reason #1: Because You're An Entrepreneur

But you're also human. So, you have many tremendous attributes, but you also have some communication and thinking biases (bias as in being an illogical preference or prejudice). This gets in the way of your pursuit of wealth.

The answer may be behavioral coaching – changing the way you think about wealth management. When it comes to investing, you have the investment return (what your return should be), as well as what your return *actually* is. Then there's the behavioral gap – the difference between the investment return and the investor return (based on the human aspect). Coaching helps close the gap.

Why You're Not Rich Yet Reason #2: Because You're Too Busy To Be Rich

You're too busy with your business. Too busy in the weeds, so to speak. If you place priority here (delegate, shift focus, etc.), change will happen.

Why You're Not Rich Yet Reason #3: Because You Don't Have A *Coordinated* Strategy *Implemented Across All* Of Your Professional Service Providers

Anna is an entrepreneur with $200,000 in cash. She needs to decide what to do with it, so she calls her bank. The bank offers to increase Anna's overall deposit interest rate (as well as a few bonuses) if she deposits the cash.

Then she calls her tax preparer. The tax preparer suggests that Anna should open an investment account with the firm.

Lastly, Anna calls her financial advisor, who tells her to think about retirement and to purchase a whole life insurance policy or a variable annuity.

What should Anna do? She pays off her condo and avoids the 3.5% interest on the mortgage. It made sense.

Here's the problem: none of Anna's providers reviewed Anna's balance sheet (and life, in general). They didn't consider possible factors like family, lifestyle, debt or liquidity. It's possible Anna's only liquidity was the $200,000 or her only debt was the condo (some would argue the mortgage with a 3.5% rate was an asset).

Why You're Not Rich Yet Reason #4: Because You Don't Have A Strategy Outside Of Your Business Strategy

Have you done the math? What does your balance sheet look like? It comes down to this: know thy balance sheet.

~David Waddell & Teresa Bailey

IT Security Tip: The #1 threat to your security is…

YOU! And your employees. Like it or not, human beings are our own worst enemies online, inviting hackers, viruses, data breaches, data loss, etc., through the seemingly innocent actions taken every day online. In most cases, this is done without malicious intent – but if you as a manager or owner aren't monitoring what websites your employees are visiting, what files they're sending and receiving, and even what they're posting in company e-mail, you could be opening yourself up to a world of hurt.

That's because employees' actions can subject the company they work for to monetary loss, civil lawsuits, data theft and even criminal charges if they involve disclosure of confidential company information, transmission of pornography or exposure to malicious code.

One thing you can (and should) do is configure your firewall to document and monitor which websites users are visiting. Almost all enterprise-level firewalls have this ability built in; you simply need to configure it and monitor the reports (something we can certainly help you with). But it's up to you to set the rules, write it into an Acceptable Use Policy (AUP), TRAIN employees on what is and isn't acceptable and then get them to sign the AUP.

pcplus networks
better people, better solutions

1010 Lakes Pkwy
Lawrenceville, GA 30043

Inside This Issue:

- Breaking Bad Habits: 4 Ways Your Employees Are Putting Your Business At Risk Of Cyber-Attack
- Why You're Not Rich Yet

Eliminate Workplace Distractions To Maximize Your Productivity

While most of us accept that distractions will be a part of our day, if your intention is to get things done and to stay productive and focused, you'll need to minimize those distractions. No, we'll never be able to eliminate them 100%, but we can certainly try. Here's what you can do to cut distractions.

Block Time On Your Calendar (And Stick To It). Use your calendar to its full advantage. Mark time off for e-mails, for all projects, phone calls, Zoom calls, you name it! If it's part of your normal day, put it on your calendar. Even throw on time for miscellaneous stuff. Then share it with all relevant parties and stick to it. If you're working on a project between 1:00 p.m. and 3:00 p.m., that's the word.

Use Sound To Your Advantage. A common source of distraction is sound: it can be office chatter in the background or even neighborhood sounds (for those working from home). Find a sound that complements your workflow. It might be chill music or the sounds of rain or a babbling brook. Find the right sound that helps you zone in and blocks disruptive sounds. *Forbes, March 15, 2021*

The 2 Best Investments You Will Ever Make

Practically every successful person has something in common with every other successful person. Millionaires and billionaires share these habits – habits that are absolutely crucial if you want to achieve the success that's on your mind.

1. Read, Read And Read Some More. Warren Buffett and Bill Gates are prime examples of this, but it's one of the most common traits among the most successful businesspeople in the world ... They are constantly reading: books, blogs, newspapers, magazines and anything else that enriches their personal and professional lives.

2. Get Educated. Whether you hire a private coach, take courses (like continuing education) or hire consultants, there are pros who can teach us more about what we do (or want to do) and how to improve ourselves or our businesses. While we may be good at what we do, there is always room for improvement – you just have to be open to it.
Inc., Feb. 24, 2021