November 2020

CSU Connection

Be sure to check us out on Facebook each week to vote for your favorite "Wacky Wednesday" team member.

REMINDER:

CSU will be closed November 26th & 27th for Thanksgiving

Our Mission
is to deliver outstanding IT support to your practice in order to improve uptime, productivity, and profitability.
You take care of running your hospital. We'll take care of your technology.

This monthly publication provided courtesy of Michelle Sherman, President of Computer Services Unlimited

Redefining What it Means To Be a

What is a Human Firewall?

Whether you know it or not, you are a human firewall. That is not up for debate. It's just a matter of how good you are at being one. A good human firewall has strong situational awareness, uses common sense to spot potential threats, and applies street smarts to information security. Just like actual firewalls on our networks that can control much of the incoming and outgoing data, you control what is allowed to come in and out of our organization, your computers, your devices, and your home (in both the cyber and physical domain).

But being a human firewall is more than just avoiding security incidents; it also means reporting security incidents. It means knowing what kind of data you have access to and what needs to be protected. It means asking for clarification whenever you're in doubt. As a human firewall you have a lot of responsibilities. The good news is that those responsibilities don't require strong technical or computer skills. They simply require common sense, good decision making, and a commitment to fighting cybercrime!

Personal Human Firewall Upgrades

The battle is not yours alone. Here are five tools that upgrade your security and your ability to be a strong human firewall. Always check organizational policy before installing any third-party software on work devices and computers!

Continued on pg.2

Continued from pg.1

PASSWORD MANAGERS

How many online accounts do you have? Ten? Twenty? Maybe fifty? It's impossible to remember every password and login for each account we own. Thankfully, with password managers, we only have to remember one master password. They store your passwords and login credentials across all (personal) devices, so signing in is simple and secure! They are one of the top security tools available to us.

VIRTUAL PRIVATE NETWORKS (VPNS)

Public WiFi is a blessing that we all use almost daily. But public WiFi is also a blessing for cybercriminals who jump at the opportunity to steal information being exchanged on public networks. VPNs, short for virtual private networks, prevent thieves from stealing your sensitive data, like logins, passwords and credit card numbers, by encrypting your traffic. They are a must-have for every personal device.

"It means knowing what kind of data you have access to and what needs to be protected.

ANTI-MALWARE

Antivirus software is a default standard in computer security. You already know this. But anti-malware is just as important. Anti-malware software routinely scans your devices and improves your security by alerting you to any potential infections. The key word here is "devices." Anti-malware (and antivirus) should be installed on every personal device from desktop computers to mobile phones.

CL OUD BACKUP

Stolen data isn't the only risk we face. It's just as easy to lose data due to system or hard drive failures. A cloud backup is a great option to ensure you'll always be able to recover in the event of an emergency. Redundancy is a major part of information security! Do your research before choosing a personal cloud backup option.

SYSTEM CLEANERS

Much like household appliances and motor vehicles, computers require maintenance. Using your internet-connected devices builds up clusters of log and system files, temporary downloads that you'll never use, cached data, expired preferences, etc.— some of which may pose a security risk. System cleaners scan your hard drives to remove all of that unwanted junk and keep your machines clean! Always research and compare products before choosing a personal system cleaning tool.

Shiny New Gadget Of The Month: Arlo Pro 3 Floodlight Camera

In the era of porch pirates, more people are investing in outdoor security cameras. The Arlo Pro 3 Floodlight Camera delivers security and practicality. It features an ultrahigh-definition camera delivering 2K HDR video and color night vision combined with a 2000 lumens light. Nothing goes undetected!

Plus, the Arlo Pro 3 is wireless. It connects to WiFi and doesn't need a power cord (it just needs to be plugged in for charging periodically). Because it's on WiFi, you can check the feed anytime from your smartphone. You can even customize notifications so you're alerted when it detects a car or person. And it has a speaker and microphone so you can hear and talk to anyone near the camera. Learn more at: **Arlo.com/en-us/products/arlo-pro-3-floodlight.aspx**

4 Steps To Move Your Business From Defense To Offense During Times Of Disruption

"Everyone has a plan until they get punched in the mouth." –Mike Tyson

As business leaders, we've all been punched in the mouth recently. What's your new game plan? Since COVID-19, the annual or quarterly one you had is now likely irrelevant.

You have two options:

Sit and wait for the world to go back to the way it was, a place where your plan may have worked (and let's face it, that's not happening).

Create and act upon a new game plan. One that's built to overcome disruption and transform your business into something better and stronger.

Option Two is the correct answer! AND, we at Petra Coach can help.

At Petra Coach, we help companies across the globe create and execute plans to propel their teams and businesses forward. When disruption hit, we created a new system of planning that focuses on identifying your business's short-term strengths, weaknesses, opportunities and threats and then creates an actionable 30-, 60- and 90-day plan around those findings.

It's our DSRO pivot planning process.
DSRO stands for Defense, Stabilize, Reset and Offense. It's a four-step process for mitigating loss in your business and planning for intentional action that will ensure your business overcomes the disruption and prepares for the upturn — better and stronger than before.

Here's a shallow dive into what it looks like.
Defense: A powerful offensive strategy that hinges on a strong defense. Identify actionable safeguards you can put in place. The right safeguards act as the backbone of your company, giving you a foundation you can count on.

Stabilize: The secret to stabilization is relentless communication with everyone. That includes internally with your teams AND externally with your customers. Streamline communication and eliminate bottlenecks through a visual dashboard.

Reset: By completing the first two steps, you'll gain the freedom to re-prioritize and focus your efforts on the most viable opportunities for growth.

Offense: Don't leave your cards in the hands of fate. Shifting to offense mode gives you the power to define the future of your business. Equip yourself with the tools and knowledge to outlast any storm.

Interested in a deep dive where a certified business coach will take you (and up to three members from your team) through this process? Attend Petra's DSRO pivot planning half-day virtual group workshop. (We've never offered this format to non-members. During this disruptive time, we've opened up our coaching sessions to the public. Don't miss out!)

When you call a time-out and take in this session, you'll leave with:

An actionable game plan for the next 30, 60 and 90 days with associated and assigned KPIs

Effective meeting rhythms that will ensure alignment and accountability

Essential and tested communication protocols to ensure your plan is acted upon

I'll leave you with this statement from top leadership thinker John C. Maxwell. It's a quote that always rings true but is crystal clear in today's landscape: "Change is inevitable. Growth is optional."

Let that sink in.

Andy Bailey is the founder, CEO and lead business coach at Petra, an organization dedicated to helping business owners across the world achieve levels of success they never thought possible. With personal experience founding an Inc. 500 multimillion-dollar company that he then sold and exited, Bailey founded Petra to pass on the principles and practices he learned along the way. As his clients can attest, he can cut through organizational BS faster than a hot knife through butter.

Do These Things To Protect Your Business From Getting Hacked

1. Train Employees. Your team needs to know how to identify and handle today's IT security threats. Cybercriminals often rely on your employees' lack of training to break into your network. Ongoing training gives employees tools and resources to overcome this and many other IT security challenges. Make training a top priority!

2. Hold Employees (And Yourself) Accountable. Training and company guidelines don't mean much without accountability. When you set rules, follow them, just as you follow industry and government rules and regulations when operating your business. Be willing to hold anyone who does not accountable.

3. Have A Disaster Recovery Plan. Things happen. When you store sensitive data, you need to have a plan in place to recover and restore that data should anything happen. This doesn't just include data loss from malicious attacks but other types of disasters, including hardware failure, fire and flood. How is your data being backed up and saved? Who do you notify in the event of a breach? Who do your employees call in the event of disaster? *SmallBiz Technology, Dec. 26, 2019*

4 Tips To Get Projects Done On Time With A Small Team

Is Working From An Office More Secure Than Working Remotely?

It may come as a surprise, but working remotely can be just as (or more) secure than working in the office. *If* done right.

Those are the three operating words: *if done right*. This takes effort on the part of both the business and the remote employee. Here are a few MUST-HAVES for a secure work-from-home experience:

Secure networks. This is nonnegotiable. Every remote employee should be connecting to a secure network (at home, it should be WPA2 encrypted), and they should be doing so with a VPN.

Secure devices. All devices used for work should be equipped with endpoint security – antivirus, anti-malware, anti-ransomware and firewall protection. Employees should also only use employee-provided or approved devices for work-related activity.

Secure passwords. If employees need to log into employer-issued programs, strong passwords that are routinely updated should be required. Of course, strong passwords should be the norm across the board. *Entrepreneur, June 17, 2020*

Top Tips On How To Prevent Your Smart Cameras From Being Hacked

Smart cameras have been under attack from hackers for years. In fact, one popular smart camera system (the Amazon Ring) had a security flaw that allowed hackers to get into homeowners' networks. That issue has since been patched, but the risk of being hacked still exists. Here are three ways to keep your camera (and your network) safe from hackers:

1. Regularly update your passwords. Yes, passwords. This includes your smart camera password, your WiFi network password, your Amazon password – you name it. Changing your passwords every three months is an excellent way to stay secure. Every password should be long and complicated.

2. Say no to sharing. Never share your smart camera's login info with anybody. If you need to share access with someone (such as a family member or roommate), many smart camera systems let you add a "shared user." This will let them access the camera, without the ability to access the camera's configuration or network tools.

3. Connect the camera to a SECURE network. Your smart camera should only be connected to a secure WPA2 encrypted, firewalled WiFi network. The more protection you put between the camera and the rest of the digital world, the better. *Digital Trends, May 7, 2020*