CE Tech Times
"Insider Tips to Make Your Business Run Faster, Easier and More Profitably"

What's New

Starting in February, we began rolling out additional Anti-virus called Sophos Intercept X. This product is a new approach for virus protection. Sophos Intercept X is designed to stop the most difficult viruses and ransomware before it takes your files hostage.

With traditional anti-virus (AV) protection, once a virus is reported, an AV manufacturer has to write a pattern to protect against that specific virus. Then every computer must be updated. At best, that can take a few days leaving computers at risk and vulnerable.

With Sophos Intercept X, its goal is "0 day" meaning it finds suspicious activity and stops it immediately. Another way to look at this is proactive protection versus reactive. CE-Tech is continually working to provide the best security protection for our clients. To learn more about this and our other services, please call us at 585-729-8324.

"Lucky Charm" Keeps Hackers Out

Ralph's been a good employee for you. Shows up on time. Gets the job done. Doesn't hassle anybody.

He's also a porn addict. When nobody's looking, he's visiting sites – on your network – that you'd be appalled to see. IF…you knew about them. Without careful monitoring and filtering, this kind of Internet use on your network can remain hidden. Shocking? Hard to believe it could happen at your company? A survey by International Data Corporation (IDC) revealed that 70% of all web traffic to Internet pornography sites occurs during the work hours of 9 a.m. to 5 p.m. Ralph's little visits may seem harmless, but they're adding a serious level of risk to the financial health and security of your company.

Here's how. A visit to an adult website can be tracked. And if a logged-in user's identity is leaked, it can be embarrassing, to say the least, to that user. The user may even become a victim of "sextortion" or blackmail. Just ask any of the people who used Ashley Madison, a dating site for illicit affairs. When the site was hacked, users were suddenly at risk of having their indiscretions revealed. This gives cybercriminals a powerful lever to pressure an employee into revealing sensitive company data. Considering that 60% of security breaches start from within the company, you have to wonder what someone at risk of being exposed might do to keep their little secret, well…secret.

Let's face it, if you're not carefully monitoring and managing how your network is being used, your company's data could be in serious jeopardy.

Content Filtering In Today's Web 2.0 World

Whether you're already monitoring user activity on your network or not,

Continued pg.2

you need to stay vigilant about evolving risks. And content filtering is key. If your business is like many, you may already be doing some filtering. But is it enough? As technology evolves, hackers drum up ever stealthier ways to invade your network.

Cloud-based filtering, for example, becomes a must when mobile devices tap into your network. The old concept of a static, location-based "firewall" just doesn't cut it anymore when your staff goes mobile.

Then there's social media. It's like a big window into the personal lives of your personnel. It lets cybercriminals "case the joint" before breaking in. For instance, when users log in to a personal Facebook account at work and talk about vacations, favorite hangouts or weekend activities, hackers can use that information for social engineering and other ploys.

The number of ways your network is exposed to potentially damaging content grows daily. It's no wonder that 90% of companies and government agencies surveyed by IDC detected computer security breaches within the previous 12 months. Eighty percent of those organizations acknowledged financial losses due to these breaches. With odds like that against you, an up-to-date content filtering system could well be THE "Lucky Charm" that keeps your company, and your data, safe from all kinds of harm.

FREE Web And E-mail Usage Audit Instantly Reveals If You Have A Problem

FREE Web And E-mail Usage Audit Instantly Reveals If You Have A Problem

If you'd like a snapshot of where your employees are going online and how much time they're spending surfing the net on non-work-related activities, I'd like to offer you a FREE Internet And E-mail Usage Audit worth $500. At no cost or obligation on your part, we'll come by and install a special diagnostic program that will expose lurking threats due to inappropriate employee use of websites, e-mail and instant messaging.

I'm making this offer because I'd like to give you a bite-sized sample of our extraordinary customer service and proactive approach for protecting you and your organization. And to be perfectly clear, no matter what we may find during your audit, you are under no obligation to buy anything or ever use our services again. However, there is a catch: we'd like to help every company in the Western NY area eliminate this risk, but we're only able to perform 10 audits. Call 585-729-8324 or visit www.cetechno.com now, while you're thinking of it. The five minutes you invest could save your company thousands of dollars in lost productivity, potential lawsuits and company resources.

Let's not let your company become yet another statistic, hemorrhaging cash as a result of a destructive cyber -attack. Call me TODAY at 585-729-8324 or e-mail me at sbrumm@cetechno.com and let's make sure your systems are safe. I'll provide you with a Cyber Security Risk Assessment to check for and safeguard against any points of entry for an attack. This service is FREE, but DO NOT RISK WAITING: contact me NOW before the next scam puts your network at risk.

IT Security Tip of the Month

IT Security Tip: How to foil ransomware

Not too long ago, the CryptoLocker ransomware virus was all over the news, infecting over 250,000 computers in its first 100 days of release (at least that's the number reported – the real numbers are probably MUCH higher). The threat was fairly straightforward: Pay us or we'll delete all your data.

Ransomware, like the CryptoLocker attack, works by encrypting your files to prevent you from using or accessing them. After your files are compromised, the hackers behind the attack then pop up a demand screen asking for payment ($400 to $10,000) within a set time frame (e.g., 72 hours or three days) in order to get the key to decrypt your files. The last CryptoLocker virus forced many business owners to lose data or pay up since there was no other way to decrypt the files. (Continued on next page)

Shiny New Gadget Of The Month:

Handheld? Console? No, It's...Switch!

Nintendo's long-awaited new gaming platform Switch should be available any day now, if it isn't already. It combines the best elements of handheld games with a home console. Handheld, the gamepad is the screen. Slip it into its dock and it plays on your TV.

The gamepad comes with two detachable "Joy-Cons." One player can hold a Joy-Con in each hand, two players can each take one, or bring in more Joy-Cons and multiple people can play.

If you're on the go, pull out the "kickstand" on the back of the gamepad and prop it up on an even surface for easy viewing. There's a slot on the side for game cards and a USB-C port for quick charging.

Because it has greater processing power than the Wii U, you'll have no trouble playing Legend of Zelda: Breath of the Wild, Super Mario and a host of your other favorite Nintendo games.

Using Android Pattern Lock May Not Be Best Phone Security

If you use an Android device, and since they are the most popular devices on the planet these days, you probably do, then you may also be using a pattern locking mechanism to secure it.

On the face of it, that seems to make a lot of sense. After all, given the number of high profile data breaches we've seen in recent years, it seems clear enough that standard text-based passwords have real issues. That's the entire reason that new security schemes like two-factor authentication and the like have risen in prominence.

Unfortunately, new research from a consortium of universities including Lancaster University, northwest University in China and the University of Bath have concluded that pattern locking is, in most cases, significantly less secure than a text-based password.

Based on their research, which included secretly videotaping people unlocking their phones, they discovered that most people tended to use the same basic patterns.

What this means from a practical standpoint is that if you use pattern locking, your supposedly secure pattern can be successfully guessed 95% of the time within five tries or less.

Everyone in the industry understands the pressing need for better and more advanced security, which, again, explains the rise of new password protection schemes that we've seen in recent years.

Unfortunately, this is essentially a process of trial and error. Some new ideas will work well, and others will backfire and wind up being less secure than what we have right now.
That certainly seems to be the case with the pattern locking. This seemingly great idea looked like it would be more secure on paper, but in the real world, it turned out to be significantly less secure.

The bottom line is that if you're currently using the pattern locking mechanism to secure your device, it isn't as well protected as you probably think it is.

IT Security Tip of the Month...Continued from Page 2

Obviously the best way to foil a ransomware attack is to be incredibly diligent about IT security; but with hundreds of thousands of new attacks being created daily, there are no guarantees that you won't get infected. Therefore, it's critical to maintain a full, daily backup of your data OFF-SITE so that IF you do get whacked with ransomware, you can recover all your files without having to pay a thin dime; and don't forget to back up off-site PCs, laptops, remote offices and third-party software data stored in cloud apps as well!

Gmail No Longer Supports Windows XP and Vista

If, for some reason, you're still running Windows XP or Vista, you probably already know that it's well past time to upgrade. Microsoft officially ended support months ago, even for critical updates, which means that your computer is essentially a ticking bomb. Sooner or later, a hacker is going to find it, and when he does, he's going to be able to crack it open like an egg and do whatever he pleases with any data inside it.

If that computer also happens to be connected to your company network, you've potentially handed hackers the keys to the kingdom. This could wind up being a very costly mistake.

This is probably not new, or even news, to you. You know you're racing against the clock. You know you've got to hurry before the worst happens, and now, you've got one more reason to upgrade sooner rather than later.

Google is the latest company to take action, pulling the plug on continued Gmail support for Windows XP and Vista users.

The day's coming when literally no vendor will continue to offer support for those old operating systems.

Even if you've got legacy systems that absolutely depend on the continued existence of an old Windows XP or Vista box, it's just a risk you can no longer afford to take. Sure, there's going to be a certain amount of pain involved in making the switch. It would be better by far to do that on your terms, rather than be forced into a situation where you're reacting to a breach and stuck in damage control mode.

If you're feeling trapped and like your existing IT staff is so overwhelmed that they just can't do anything about the problem, give us a call and speak with one of our talented team members. We'll be happy to work with you to construct a roadmap and outline how we can help to get you out from under that old legacy system and onto something safer, more secure and more robust.

Who Else Wants To Win A $25 Gift Card?

The Grand Prize Winners of last month's Trivia Challenge Quiz are Pat Zubil from Natcore Technology and Robin Hansel-Kruger from the Town of Hamlin! They were the first two people to correctly answer our quiz question from last month: **Who was the classic Hollywood film star and avant-garde composer who helped invent WiFi?** a) Hedy Lamarr b) Arnold Schwarzenegger c) Clint Eastwood d) Judy Garland

The correct answer was a) Hedy Lamarr. Now, here's this month's trivia question. The first two winners will receive a $25 Amazon gift card.

Daylight Savings Time was originally dreamed up by whom?
a) Sir Isaac Newton b) Franklin Delano Roosevelt c) Benjamin Franklin d) Thomas Edison

Email us at jstanton@cetechno.com or call at 585-729-8324 with your answer!