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

What's New

Microsoft ended support for the XP operating system as of April 2014. What's new is anti-virus programs are doing the same. Sophos, for example, will no longer be updating virus definitions for the XP operating system starting 5/1/17. This means after May 1st any XP PC's, with Sophos, will not be protected by Antivirus software. Any XP computers that are connected to the Internet will be vulnerable to new threats as both Microsoft and many anti virus manufacturers are no longer providing updates for XP systems.

In addition, Microsoft is ending support for Vista on April 11, 2017. This means that Vista machines will no longer receive automatic updates. These security updates can protect your PC from harmful viruses, spyware and hackers.

Whether its XP or Vista, your best course of action is to retire this equipment.
If you have XP or Vista machines and you need assistance determining what to do, give us a call at 585-729 -8324. We can help you out!

7 Ways To Dodge A Data Disaster

You stride into the office early one Monday morning. You grab a cup of coffee, flip on your computer and start checking e-mail…
A note pops up that rivets your attention:
"Your files have been encrypted. Send $5,000 within five days or they will all be destroyed."
You start sweating as your throat constricts and your chest tightens. Sure enough, every time you try to open a document, the same message appears. Your phone rings. It's Bob in accounting, and he's having the same problem. All files across your entire network have been encrypted. You contact the local police.
They suggest you call the FBI. The FBI says they can't help you. What do you do next?
a) You pay the five grand, desperately hoping you'll get your data back, or…
b) You calmly call your IT pro, who says, "No problem, your backups are all current. No files were lost. Everything will be restored by noon, if not sooner."
If your answer is "b," you breathe a sigh of relief and get back to work as your backup plan kicks in…
Ransomware attacks are more common than ever, especially at smaller companies. That's because small companies make easy marks for hackers. The average small business is much easier to hack than high-value, heavily fortified targets like banks and big corporations. According to Time magazine, cybersecurity experts estimate that several million attacks occur in the US alone every year. And that figure is climbing.
So how can you make sure you never have to sweat a ransomware attack or other data disaster? One sure solution is having a solid

Continued pg.2

backup plan in place. When all your data and applications can be duplicated, you have plenty of options in the event of an attack. Here are seven ways to make sure you're in good shape, no matter what happens to your current data:

Insist on a regular, remote and redundant process. A good rule of thumb is 3-2-1. That means three copies of your data is stored in two off-site locations and backed up at least once per day.

Don't cheap out on disk drives. Less expensive arrays that save money can leave your data at risk. Get features like a redundant power supply and hot spare disks.

Guard against human error. Make sure people doing backups know exactly what to do. Take people out of the loop and automate wherever possible. And watch for situations where backups aren't a part of someone's regular duties.

Check backup software settings routinely. When new software or updates are put into service, a change in the way the settings are configured can cause incomplete backups, or backups that fail. Do the people who maintain your backups include this on their regular to-do list?

Make sure critical files aren't getting left out. As resources are added and priorities shift, documents and folders can get misplaced or accidentally left off the backup list. Insist on a quarterly review with your backup management team to make sure all mission-critical files are included in your organization's data recovery systems.

Data Recovery Review Reveals Backup System Vulnerabilities

Address network issues immediately. Any component in your network that isn't working properly can introduce another point of failure in your backup process. Every juncture in your network, from a misconfigured switch to a flaky host bus adapter, can hurt your backups.

Ask for help with your data backup and recovery system. You cannot be expected to be an expert in all things. Yet data is the backbone of your business – its protection and recovery should not be left to chance. Leverage the knowledge, skill and experience of an expert who stays current with all the latest IT issues.

Data Recovery Review Reveals Backup System Vulnerabilities

Don't let *your* company become yet another statistic. Just one ransomware attack can result in a serious financial blow if you're not prepared. Visit www.cetechno.com/datadisaster TODAY or call 585-729-8324 by April 30 for a FREE Data Recovery Review, ordinarily a $500 service. We'll provide you with a complete on-site assessment of your current backup system to check for and safeguard against any gaps that could prove financially lethal to your business.

IT Security Tip of the Month

IT Security Tip: How to spot a phishing e-mail

A phishing e-mail is a bogus e-mail that is carefully designed to look like a legitimate request (or attached file) from a site you trust in an effort to get you to willingly give up your login information to a particular web site or to click and download a virus.

Often these e-mails look 100% legitimate and show up in the form of a PDF (scanned document) or a UPS or FedEx tracking number, bank letter, Facebook alert, bank notification, etc. That's what makes these so dangerous – they LOOK exactly like a legitimate e-mail. So how can you tell a phishing e-mail from a legitimate one? Here are a few tell-tale signs…First, hover over the URL in the e-mail (but DON'T CLICK!) to see the ACTUAL web site you'll be directed to. If there's a mismatched or suspicious URL, delete the e-mail immediately. In fact, it's a good practice to just go to the site direct (typing it into your browser) rather than clicking on the link to get to a particular site. Another telltale sign is poor grammar and spelling errors. Another warning sign is that the e-mail is asking you to "verify" or "validate" your login or asking for personal information. Why would your bank need you to verify your account number? They should already have that information. And finally, if the offer seems too good to be true, it probably is.

Shiny New Gadget Of The Month:

Thought Oculus Was King? Think Again

Once upon a time, Oculus Rift ruled the world...

The virtual reality (VR) world, anyway. Not so much anymore. Now that VR heavyweights Sony, HTC and Samsung have entered the ring, there's a whole new reality in, well...VR.

Sony's PlayStation VR was recently crowned "Editor's Choice" by PC Mag. And, if you happen to own a compatible Samsung Galaxy smartphone, such as the S7 or S7 Edge, you can get "untethered" VR for just $100. You'll pay four times that for the Rift, HTC's Vive or Sony's PlayStation VR – all tethered sets, requiring a clunky cable from headset to hardware.

Vive has the most advanced technology, but Rift is nearly as sophisticated and sells for $200 less. You could shell out that much for the Rift's hand controllers, but, according to PC Mag, they're well worth it. So while Oculus may not be king, it's still a serious contender.

The Guardian Pocket

Rochester's premier custom clothiers, Omero's Custom, Ltd, provides top of the line custom suits, shirts, ties and other accessories. Walter (Wally) Piccone and son Matt Piccone own and operate Omero's. Their mission is to bring passion to fashion. You don't necessarily think of fashion and technology together but Wally recently blogged about an interesting topic...The Guardian Pocket.

Written by Wally Piccone, used with permission:
"As technology continues to evolve, I get excited when I modify my "old-school" and utilize the "new" to make my life easier and better.

We are now easily capable of running our businesses and private lives from our cell phones. We can pay bills and manage all of our banking, communicate with anyone in the world, get our news... even our most private information is accessible with a mere few presses on the keypad. The problem becomes that with all this power at our finger tips, the "CROOKS" are becoming more adept at Cyber-pickpocketing that information without you knowing until it's too late.

They could be standing close to you at the airport for instance, looking like they're texting, all the while gathering all your personal information like SS #, account #, banking information, etc. With the info you have connected to your cell phone, they can steal your identity causing you years of anguish and BIG money getting it back to the way it was. It's called "Cloning your phone".

You may be wondering to yourself: why is Omero's suddenly so concerned with cyber security? That's because we're excited about an ingenious creation from Hickey Freeman this spring called the ***"GUARDIAN POCKET".*** Now your custom made suit and custom jackets can be manufactured with this special pocket, which makes cyber-intrusion impossible. You can put your cell phone and credit cards in that pocket and via it's special material, it prevents those "CROOKS" from accessing your information.

Matt and I would be happy to help you secure your world just a little, with this special detail from Hickey Freeman's new spring 2017 collection now available, Custom Made, exclusively from OMERO'S Custom, Ltd.

We have always saluted Hickey Freeman for their American craftsmanship and American pride but now we add American ingenuity to their legacy which now is helping to protect us and helps us all to…*DRESS Passionately!"*

We have supported Omero's, Wally and Matt, for 12 years and counting. If you want to know anything about fashion and to look good check them out! They do an amazing job! Www.omeroclothes.com or 585-392-2939.

Lip Reading Technology May One Day Replace Traditional Typed Passwords

There's a new technology being developed by researchers at Hong Kong Baptist University (HKBU) that stands to be a game-changer. Dubbed "lip password," the new tech utilizes machine learning to recognize lip motion, shape and texture for each user when you speak your password.

Of significance, your voice has nothing to do with the password you set, it is entirely based on the movement of your lips. This matters because while a voice print would be difficult to mimic, it would not be impossible, given time and the right tools. The precise movement and shape of your lips would be virtually impossible for a hacker to duplicate, and the system would be even more robust if paired with facial recognition software.

The new tech is important in another way, too. One of the key drawbacks to current biometric password schemes, the two most common being retinal and fingerprint, is that they cannot be changed. If your fingerprints or retinal scans are ever hacked and released, there's no way for you to "change your password."

That's not the case here. Simply speak a different word, and it's done. Once testing has been completed and the new system is rolled out, it will give you the best of both worlds. The more robust security comes with biometric technology coupled with the flexibility and ease of use of current text-based passwords, including the ability to change them when and as needed.

Research and testing are ongoing, but the scientists applied for and got a patent on the technology in 2015. They expect that it will be ready for rollout later this year. Initial plans call for it to be deployed to the financial sector first, with other industries to follow after a trial period.

It may not be an ironclad, hack-proof system, but the early indications are that it's the most robust password protection scheme we've seen to date, and that is good news indeed.

Who Else Wants To Win A $25 Gift Card?

The Grand Prize Winners of last month's Trivia Challenge Quiz are Rika Stroller from Regional Distributers Inc. and Pam Fiegl from George and Swede Sales & Service, Inc. They were the first two people to correctly answer our quiz question from last month: **Daylight Savings Time was originally dreamed up by whom?** a) Sir Isaac Newton b) Franklin Delano Roosevelt c) Benjamin Franklin d) Thomas Edison. The correct answer was c) Benjamin Franklin

Now, here's this month's trivia question. The first two winners to respond will receive a $25 Amazon gift card. (One winner per company per quarter.)

Roughly what percentage of the world's money exists only in computers?
a) 10% b) 27% c) 62% d) 95%

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