CE Tech Times

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

What's New

IMPORTANT REMINDER about the XP operating system… 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. If you need help figuring out what to do with your XP machines, give us a call at 585-729-8324.

Summer is upon us… Time for a stroll in the park… softball… fishing… a few rounds of golf…

Yet how could you possibly relax if some random bit of malware, software glitch or cyber-attack catches you off guard just as you're walking out the door? A well-designed secure computer network gives you the confidence that "all systems are go," whether you're having fun in the sun, or just getting things done with your team.

Here's a quick nine-step checklist we use to ensure that a company's computer network, and the data for that business, is safe and secure from disruption, if not absolute devastation:

1. **A written recovery plan.** Simply thinking through what needs to happen when things go south, and documenting it all IN ADVANCE, can go a long way toward getting your network back up and running quickly if it gets hacked, impacted by natural disaster or compromised by human error.
2. **Have a clear communication plan.** What if your employees can't access your office, e-mail or phone system? How will they communicate with you? Make sure your communication's plan details every alternative, including MULTIPLE ways to stay in touch in the event of a disaster.
3. **Automate your data backups.** THE #1 cause of data loss is human error. If your backup system depends on a human being always doing something right, it's a recipe for disaster. Automate your backups wherever possible so they run like clockwork.
4. **Have redundant off-site backups.** On-site backups are a good first step, but if they get flooded, burned or hacked along with your server, you're out of luck. ALWAYS maintain a recent copy of your data off-site.

Continued pg.2

5. **Enable remote network access.** Without remote access to your network, you and your staff won't be able to keep working in the event that you can't get into your office. To keep your business going, at the very minimum, you need a way for your IT specialist to quickly step in when needed.

6. **System images are critical.** Storing your data off-site is a good first step. But if your system is compromised, the software and architecture that handles all that data MUST be restored for it to be useful. Imaging your server creates a replica of the original, saving you an enormous amount of time and energy in getting your network back in gear, should the need arise. Without it, you risk losing all your preferences, configurations, favorites and more.

THE #1 cause of data loss is human error. If your backup system depends on a human being always doing something right, it's a recipe for disaster. Automate your backups wherever possible so they run like clockwork

7. **Maintain an up-to-date network "blueprint."** To rebuild all or part of your network, you'll need a blueprint of the software, data, systems and hardware that comprise your company's network. An IT professional can create this for you. It could save you a huge amount of time and money in the event your network needs to be restored.

8. **Don't ignore routine maintenance.** While fires, flooding and other natural disasters are always a risk, it's more likely that you'll have downtime due to a software or hardware glitch or cyber-attack. That's why it's critical to keep your network patched, secure and up-to-date. Deteriorating hardware and corrupted software can wipe you out. Replace and update them as needed to steer clear of this threat.

9. **Test, Test, Test!** If you're going to go to the trouble of setting up a plan, at least make sure it works! An IT professional can check monthly to make sure your systems work properly and your data is secure. After all, the worst time to test your parachute is AFTER you jump out of the plane.

Be certain that you have all 9 steps fully covered with our FREE Disaster Recovery Audit.

Contact us at 585-729-8324 or sbrumm@cetechno.com or visit www.cetechno.com to schedule our **Disaster Recovery Audit** FREE of charge, now through May 31. **Contact us TODAY to get scheduled!**

IT Security Tip of the Month

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 web sites 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 employer 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. (continued on next page)

Shiny New Gadget Of The Month:

Surface Studio: All Beauty, A Little Brains

"We want to move from people needing Windows…to loving Windows."

So said CEO Satya Nadella after taking over Microsoft. Their new Surface Studio takes a bold step in that direction.

In a bid to win over creative types, they designed the Studio with a gorgeous desktop screen that easily glides from vertical to almost horizontal, like an artist's sketchpad. With its Apple Computer-like brushed aluminum finish and ultra-thin screen, it's feels right at home in an open-plan office with microbrews on tap.

The guts of the machine are stuffed into a nine-inch-long base that's joined to the screen with an überslick hinge design, allowing it to fold nearly flat for stylus- or touch-driven design work.

Downsides? Well, you'll pay at least $3,000. And it's a bit underpowered to be in that price range. But all in all, even the graphically challenged will find this machine tantalizing.

Password Thefts Have Not Prompted Users To Change Password Habits

The newest big problem with data security is the same as the old big problem with data security. It's the users. Specifically, it's the fact that most people don't bother to change their passwords more than once a year, if that frequently.

Data security is a major headache for all business owners, no matter the size of your company.

You can spend hundreds of thousands or even millions of dollars on a top-notch, state of the art system, and still watch it all come tumbling down around you because someone used a dead-simple password or didn't bother to change it periodically.
How bad is this new/old problem?

According to the most recent survey, fully 53% of users only change their passwords one a year or less. More than a quarter only change them when a system administrator instructs them to.

This is crazy, especially in light of the rapid increase in major security breaches in recent years. With all the high-profile hacks, often affecting hundreds of millions, if not billions of users at a time, you'd think that the message would have sunk in by now. Password security matters. It's important. It's your first, best line of defense against a major security breach, and none of that seems to matter. Users just aren't responding.

It's uncertain whether this is an education issue, or something else. At this point, it could come down to simple apathy. Since most users won't be personally impacted by the consequences of a breach, there's limited interest in working to prevent one.

To date, no one has come up with a good solution to this problem. But, based on the statistics, you can be almost certain that a significant portion of your workforce hasn't changed their passwords in a while, and many of them are likely using passwords that would be child's play for a hacker to work out.

That puts your company at risk, and it's a ticking time bomb. If you need help implementing password policies, please give us a call at 585-729-8324.

IT Security Tip of the Month

Continued from Page 2

One thing you can (and should) do is configure your firewall to document and monitor which web sites users are visiting. Almost all commercial-level firewalls have this ability built in; you simply need to configure it and monitor the reports (something we can certainly help you with). If you are a client of CE-Technologies we take care of this for you! 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. We can help on all fronts, contact us at 585-729-8324.

Will Your Laptop Battery Last As Long As They Say?

If you have a laptop, you've probably noticed that your laptop's battery doesn't seem to last as long as the manufacturer says it will. Maybe you just figured you were a power user, or maybe you thought it was just your imagination. It isn't.

A company called "Which?" that runs a popular website offering expert advice on numerous topics, including technology, recently completed a year-long survey into laptops made by a variety of manufacturers. Their findings support what users have been saying all along.

With one notable exception, laptop manufacturers overstate the expected battery life of their equipment, sometimes by as much as 50 percent! Here are some of the key findings, broken out by manufacturer:

- Acer Equipment – According to the manufacturer, their batteries should last an average of seven hours and 53 minutes. In independent tests, the actual battery life was found to be five hours and 59 minutes.
- Asus Equipment – Manufacturer's claim: 10 hours and 12 minutes. Independent test results: six hours and 53 minutes
- Dell Equipment – Manufacturer's claim: nine hours and 15 minutes. Independent test results: five hours and 12 minutes.
- HP Equipment – Manufacturer's claim: nine hours and 48 minutes. Independent test result: five hours and 2 minutes.
- Lenovo Equipment – Manufacturer's claim: six hours and 41 minutes. Independent test result: four hours and 34 minutes.
- Toshiba Equipment – Manufacturer's claim: seven hours and 58 minutes. Independent test result: four hours and 45 minutes

The one bright spot in the report? Apple equipment actually lasted longer in independent tests than the company claimed (ten hour claim vs. ten hours, 15 minutes in independent testing).

Unfortunately, this means that unless you're using an Apple laptop, the manufacturer's data on expected battery life is essentially worthless and should not be factored into your decision-making process.

Which? researchers reached out to the manufacturers of the equipment they tested for an explanation and were told that the company must have used a different testing paradigm to measure expected battery life.

Who Else Wants To Win A $25 Gift Card?

The Grand Prize Winners of last month's Trivia Challenge Quiz are Tracy Glass from Quintel and Lindsey Pacitto from the Town of Hamlin They were the first two people to correctly answer my quiz question from last month: **Roughly what percentage of the world's money exists only in computers?**

a) 10% b) 27% c) 62% d) 95%

The correct answer was **d) 95%**.

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.)

Which technology, developed in the 1940s, was inspired by Morse code?

a) ZIP code b) Bar codes c) Braille d) Tickertape

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