CCSI Essential Stream

CREATIVE COMPUTER SOLUTIONS
INCORPORATED
"Creating Clients For Life!"
15th Year Anniversary

February 2013

In this issue. . .

Business Continuity Tip

Flu Update

The influenza outbreak has reached epidemic proportions in the United States according to the Centers for Disease Control and Prevention. The number of states reporting widespread activity rose from 41 to 47 in one week. Click here for a snapshot of flu activity in your state.

In response, Agility Recovery hosted a free webinar featuring Dr. Michael Jhung, lead medical officer in the CDC's Influenza Division who will update us on the current status of the outbreak and the severity throughout the nation. Join us as we discuss how to reduce risk, prevent transmission of the virus and maintain a healthy work environment.

Letter from the President

The following information regards data integrity, backup and recovery of your critical systems. I try to have conversations with all our clients on a regular basis, but there is some extremely important news I would like to share with you. Many of you use USB drives and or Network Attached Storage to back-up your computer networks, so please:

- Verify you're taking a full backup of your data offsite each day. If you're not the person responsible for that task, have a conversation with the responsible party regarding the importance of having the disks taken offsite every day.
- Test backups regularly, both offsite and on another computer other than your server.
- Increase the number of drives you're taking offsite each day, I recommend (4) FULL copies minimum moving forward; one at your office and (3) FULL copies offsite. How far back would you like to go if all your data disappeared tomorrow? How much would it cost to reproduce all your information?
- Allocating money in your budget to replace your USB based backup system with an automated offsite system, which requires no user intervention, should be a strong consideration.

Why this information now? There is a new variant of a well-known virus called Ransomware or Citadel that has been released. When a server becomes infected, it encrypts all files on the server and all files on any attached drives, including your data and any backup drives attached to the server. It may also be a dormant attack where all files are encrypted, and the virus waits for a time and date to activate. This would cause all of your backups to be useless after that date. It is imperative you have a conversation regarding your backup system with us immediately if you have a USB or NAS based backup system. There is NO recovery from this threat. All data will be gone and all attached backups will be destroyed.

If you're taking drives off-site, you need to increase the number of drives you're using for backup, and ensure a backup is taken off site each day. This particular virus is extremely virulent, there is nothing short of a full backup set recovery and server rebuild to recover from this threat. Your server and all of your data will be destroyed if infected.

There is no 100 percent protection against computer based threats, malware and data destruction. It's about mitigation of risk, and how much risk you're willing to allow your company to be exposed to.

Scott Huotari, Founder, President/CEO

Laugh a Little

"This?! Oh please!
It's not even mine!"

The Future of IT

Used with the permission of http://thenetwork.cisco.com, by Padmasree Warrior

What an exciting time to be in the tech industry. We are at the beginning of a major transition to the Mobile-Cloud era. Trends like bring your own device (BYOD), access anywhere, virtualization, and machine-to-machine connections have given way to a new breed of applications. We estimate that approximately 50 billion devices will be connected by 2020. In 2010 alone, more than 350, 000 applications were developed with more than three million downloads. A 44-fold increase in data creation is predicted from 2010 to 2020, with 34 percent of it in the cloud. All of this leads to a world of intuitive connections between people, processes, data and things on the network – the Internet of Everything.

Read more

Password Dos and Don'ts

used with permission from Norton by Symantec
by Marian Merritt

There have been some well-publicized news stories of hacked websites where millions of user accounts and passwords were posted publicly. Can you imagine if you were one of those users affected? They likely had to hurry to change their credentials and make sure they didn't use the same combination of email address and password on any other websites. Chances are these people, like many others, did use the same password for other accounts. Many people not only use the same password all over the Web, but they also choose weak and foolish passwords.

Here's a list of some of the top password choices for millions of computer users:

Read more

Writing better business emails

used with permission from HP Technology at Work

The way you use language can say a lot about you. Especially in the online world, where your words are often all you have to make a lasting impression. Here are some tried-and-true tips to keep in mind when crafting business emails that might help improve your professional image.

Consider these basic tips before you start to write:

Read more