FREE

Tech Source News

FREE

First Edition

A FLICKERTRONICS TECHNICAL NEWS PUBLICATION

www.techsourcenews.com

Flickertronics MSP (Managed Service Provider)

+1 (904) 825-6708
+1 (800) 899-5350

Flickertronics is launching our free newspaper to help keep you informed of the latest computer security threats, provide helpful information relating to technology and computer related news as well as other interesting topics.

Here is how we are different!

Flickertronics, in business over 18 years, has a different philosophy and a radically different approach to Business IT Managed Services. We believe that a Managed Service Provider should respond to your needs in real time.

Our 24x7 local, live US based phone operators, all of whom are experienced technicians, are available all holidays as well as weekends. While others operate in a tiered level support system, where you get the "Cheapest" person (or answering machine) that can help you first, **Flickertonics'** live support phone operators are actually trained technicians with years of experience.

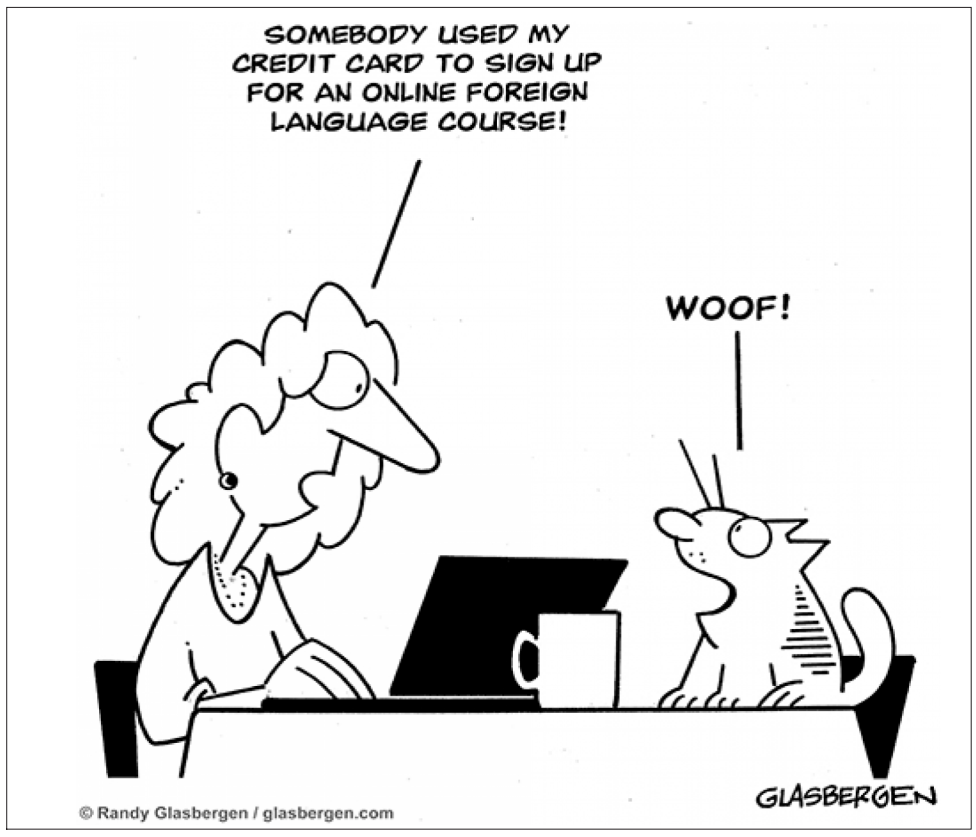
L**ive, 'Round the clock Human Support** from our local, in-house technical staff assures your problems are resolved, or **your questions answered**, promptly and **in Real Time** as they occur.

Flickertronics on-site service is focused mainly towards business support, allowing our technicians to be highly available for your on-site business needs.

With one of the largest walk-in repair depots in North East Florida, we offer flat-rate repairs geared for home users for $75.00 to $95.00 at our business location.

With Flickertronics you can "Grow as you Go."

You can choose from a menu of Managed IT Products & Services, allowing you to start with the ones that make the most sense for your organization, and add other products and services as needed.



Computer Workstation Ergonomics

Excerpts Compiled from OSHA
by Flicker, CEO , Flickertronics

Millions of people work with computers every day and pay little attention to computer workstation ergonomics, the study of how people work in their environment and the effects of such work on the human body.

While there is no single correct posture**,** furniture arrangement or working environment, with these few tips you will find your workplace more comfortable.

Here are the tips:

1. Keep top of monitor at or just below eye level.
2. Keep head and neck balanced and in-line with torso.
3. Keep shoulders relaxed.
4. Keep elbows close to your body and supported.
5. Keep lower back supported.
6. Keep wrists and hands in-line with forearms.
7. Have more than adequate room for keyboard and mouse.
8. Keep your feet flat on the floor.
9. Have good lighting and avoid glare from improperly shaded windows.

★10 Easy Tips to keep Your Computer Safe★

by Mandy, Vice President,
IT Tech, Flickertronics

TIP 1 - Update your Computer with the latest security updates and patches.

TIP 2 - Make sure Antivirus software is up to date & working properly. Also make sure Java, Adobe Flash-player as well as Shockwave are up-to-date and apply updates as released for your other programs.

TIP 3 - Always LOG OFF of your banking sites as well as remote programs, Email, Credit Card, Facebook and other sites requiring a password login.

TIP 4 - Use Mozilla Firefox as an alternative browser to **Internet Explorer**.

Tip 5 - Clean out your cookies, Internet history, searches, and temporary files.

TIP 6 - **Be CAREFUL** doing searches on the Internet. Some pages may try to change your Home Page. (*continued on Page 8*)

Securing Your Wireless Network

by Flicker, CEO , Flickertronics

If you don't secure your wireless network, strangers could use it and gain access to your computer, including your personal and financial information.

Any computer or wireless device within range of a wireless access point or a wireless router can connect to that device and use your Internet service unless you take certain precautions such as encrypting your wireless Internet connection by c.reating a "Wi-Fi" password.

Most modern wireless devices have the wireless network name and a security, or encryption key, already pre-configured for you.
If that is the case you will be able to locate that information on your wireless router or access point.

You will see something called the the SSID (service set identifier), and the password or key will be under that.

The SSID is what you see on your laptop when you "Search fo Available Networks"

Limit Access to your network
Allow only specific users to access your wireless network.

Turn off your wireless network when you know you won't use it.
Unauthorized users cannot access your Internet when it is powered off.

Do not assume that Public Wi-Fi networks are safe and secure.
Be careful when using public wireless networks. While airports, hotels, cafes and other public places offer **Wi-Fi** to their customers, these **HotSpots** often may not be secure, and sometimes hackers will set up a "**Fake Hotspot**" to steal data from your computer and infect it with hidden Keyloggers or **Trojan Viruses**!

The Microsoft Imposter Scam (among others)
story page 2

Cryptolocker Ransomware Virus
story page 2

Let's Talk Trash
Great article by Mandy on recycling, reduce, reuse topics
story page 8

7.8 Million Deadly Airbags Recalled
story page 7

The Microsoft Imposter Scam (Among Others)

by Flicker, CEO , Flickertronics

The Microsoft Impostor Scam is Targeting the Saint Augustine, Florida area especially hard in recent months.

We have a number of people each month who let impostors access their computer remotely.

Note: ***We have had 5 customers who actually came in to our store after they had received a phone call and had allowed an impostor remote access to their machine during the week it took me to compose and edit this newspaper*****. (Flicker)**

We have been receiving increased calls from local consumers who have been targeted by the Microsoft Imposter Scam and similar others - a number of them have allowed the impostor to access their computers remotely, and even paid, the impostors!

The scam, which involves people pretending to be employed by **Microsoft**, **Cisco**, **Linksys**, **HP** or other recognizable technology names offering to fix computer **Viruses**, is thought to have ripped off tens of thousands of people in six countries.

We will use Microsoft as an example, but this applies to any such suspicious caller since none of those companies ever call people in such a manner.

The Impostor will make an unsolicited phone call, send a letter, e-mail or text coming "out of the blue" pretending to be a **Microsoft** employee. The targeted victim is told that it ha been detected that their computer is infected with **Viruses** and the caller offers to help to fix the problem.

The fake Microsoft employee will try to "**Hard Sell**" their targeted victim regarding all sorts of bad things that will happen to their computer if they do not sort out the problem immediately.

To try to gain the targeted victims trust, the caller may sometimes direct them to the ***Event Viewer*** in Windows which shows details about various hardware and Windows software issues.

The *Event Viewer* is <u>always</u> full of some type of error messages, even on a healthy computer, but the caller will convince them that these are the warning signs of the impending disaster.

When the caller has their trust, they ask the targeted victim to go to a website and download a remote control program that will help them fix the problem.

After downloading the remote control program, the caller will take control of the computer, the targeted victim will see their mouse pointer move around while various programs and folders are opened. The caller will claim that they know exactly what the problem is and how to fix it.

Then the caller will ask for credit card details for a piece of software that will supposedly remove the '**Virus**'.

The software that they sell to fix the computer will do nothing except tell you every now and then that everything is fine, all viruses have been removed. But in reality, it could be downloading all sorts of **Malware** to your computer.

However, part of the scam's damage may already have been done when the customer downloaded the remote control software. This software could well have the capability to sit in the background for months or years, stealing personal information from the computer like bank login details and other personal details that could be used for identity theft purposes. (*continued above right*)

ShopGenie.me

Flickertronics offers a safe shopping site for your **online shopping**. We are affiliated with many familiar brands among others at **www.ShopGenie.me**. **Flickertronics** has long, well established financial relationships with everyone listed at **www.ShopGenie.me** so you can be assured of a safe, secure online shopping experience..

<u>Quote</u> <u>from</u> <u>Microsoft:</u>

"Microsoft takes the privacy and security of our customers and partners personal information very seriously. We are advising customers to treat all unsolicited phone calls with skepticism and not to provide any personal information to anyone over the phone or online. Anyone who receives an unsolicited call from someone claiming to be from Microsoft should hang up. We can assure you Microsoft does not make these kinds of calls."

(*continued from below left*)

These callers could also be using this software to infect your computer with real viruses and Malware.

If you receive one of these unsolicited phone calls hang up and do not download anything they ask you to download.

And definitely don't hand over your credit card details, just because someone mentions the well known names **Microsoft** or **Windows**.

If you have allowed them to take control of your computer, or you have downloaded their 'fix' software, it is possible they have infected your computer with a Virus or other nasty **Malware**.

At **www.techsourcenews.com** we have a number of tools to verify that your computer is safe and secure.

To scan and remove **Viruses**, **Rootkits** and **Malware** for **FREE** from your computer, click on the ***Free Do it yourself Virus Removal Tools*** link at the top of the page.

What is Ransomware?

by Flicker, CEO , Flickertronics

Ransomware is a type of **Malware** which blocks access to the to the computer system that it infects , and demands a ransom be paid to the creators of the **Malware** via an on-screen alert in order for the victim to regain access to their computer or files, typically in the $100 to $300 range.

Some forms of ***Ransomware*** will put up an alert that the FBI has blocked your computer and tell you to buy a MoneyPak Card and put in the redemtion code to access your computer - those are all bogus and simply take your money.

Some forms of ***Ransomware*** encrypt the files on the systems's hard drive (***cryptoviral extortion***). The ***Cryptolocker Virus*** is particularly nasty, and I will discuss that in the article below.

Cryptolocker Ransomware Virus

A user's computer typically becomes infected by the ***Cryptolocker Virus*** by opening a malicious attachment from an email. This malicious attachment contains ***uptare***, a downloader, which infects the user with ***Gameover Zeus***.

Gameover Zeus is a variant of the ***Zeus Trojan*** that ***steals banking information*** and is also used to steal other types of data. Once a system is infected with ***Gameover Zeus***, ***uptare*** will also download ***Cryptolocker***.

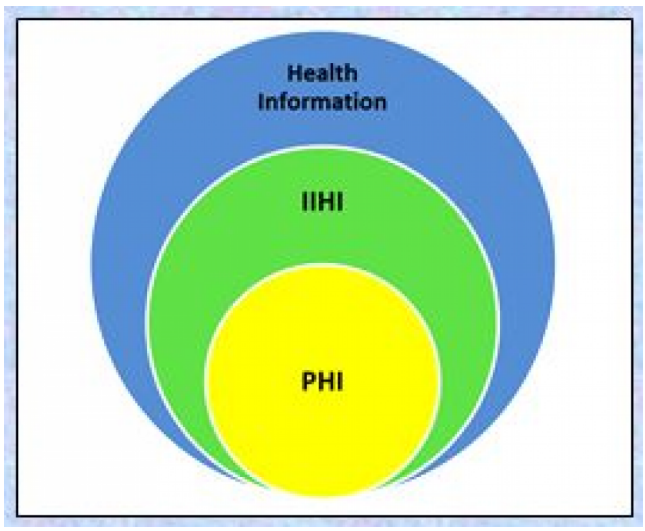
Finally ***Cryptolocker*** encrypts files on the infected computer and requests that you pay a ransom.

Ransomware does not only target home computers, thousands of businesses have been infected as well, resulting in millions of dollars in losses.

Paying the ransom does not guarantee your encrypted files will be unencrypted, and rarely does paying the ransom work..

However, if paying the ransom does work that will start the decryption process. When you pay the ransom you will be shown a screen stating that your payment is being processed and may take several hours to complete.

Once the payment has been verified, it will begin decrypting your files, which can take quite a while depending on how many files were encrypted, and you most likely will not recover many files!



Taino Consultants, Inc , *a Flickertronics Partner*

SAMPLE HIPAA SECURITY REMINDER

Nov 2014 VOL #1 ISSUE #10

Electronic Protected Health Information (e-PHI)
45 CFR 160.103, 45 CFR 164.514

The HIPAA Security Rule establishes national standards to protect individuals electronic protected health information **(e-PHI)** that is created, received, used, or maintained by a **HIPAA** covered entity. The Security Rule requires appropriate , physical, administrative, and technical safeguards to ensure the confidentiality, integrity, and security of **ePHI**.

These safeguards, when applied well, can help you avoid some of the common security gaps that lead to cyber attack or data loss. They can protect the people, information, technology, and facilities that you may depend on to carry out your primary mission: helping your patients.

The HIPAA Security Rule requires covered providers to implement security measures, which help protect patient's privacy by creating the conditions for patient health information to be available but not be improperly used or disclosed.

Actions in Case of a Breach
A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of **e-PHI** such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

The Breach Notification Rule requires covered providers to promptly notify individuals and the Secretary of the **HHS** of the loss, theft, or certain other impermissible uses or disclosures of unsecured **e-PHI**. Health care providers must also meet additional requirements if any breach affects 500 or more individuals.

Remember that Failure to comply with HIPAA can result in civil and criminal penalties.

Civil Penalties
• The U.S. Department of Health and Human Services Office for Civil Rights **(OCR)** is responsible for administering and enforcing the **HIPAA** Privacy and Security Rules and conducts associated compliance investigations as well as compliance reviews, and audits. **OCR** may impose fines on covered providers for failure to comply with the **HIPAA** Rules.
• State Attorneys General may also enforce provisions of the **HIPAA** Rules.

Criminal Penalties
• The U.S. Department of Justice **(DOJ)** may enforce criminal penalties for **HIPAA** violations.

The Dangers of Technology

by Dr. Jose Delgado, Ph.D.

My intention is not to scare but to create awareness about the realities of our times. Even thinking about this topic I think that rather than a one-time article we could create a series of articles where we cover each aspect of the new technologies and how the same could endanger us.

The funny thing about all this is that I can say that I make my living by relying on technology and pushing new developments and how the same could benefit us. For example, just yesterday I was speaking to a couple of healthcare professionals in terms of how to use camera phones and similar technologies to consult peers about a patients condition.

I have also seen applications that normally require rather specific diagnostic equipment that can now be deployed using cellular phones.

On the other hand, this same technology makes us extremely vulnerable as more and more information is downloaded into those devices and as we increase remote operations. For example, it is no longer enough to hack into your system, but for a while now individuals have been able to commandeer your system from remote sites to do their bidding (**BOTS, BOTNETS**).

(*continued on Page 5*)

A Sustainable St. Augustine

Story on page 8

Pictured above Steve Satterfield, Flickertronics, Kip Case from the City of St Augustine and Olivia Smith St Augustine Recycling Coordinator

What is a Computer Virus *by Flicker*

A Computer Virus is a program or piece of binary code that is loaded on to your computer without your knowledge and can cause malicious damage. All Computer Viruses are man-made.

Some Computer Viruses can also replicate themselves (Polmorphic Virus), and some types of viruses are capable of transmitting themselves across networks and bypassing security systems.

Computer Viruses are often spread through downloads on the Internet or by attachments in Email or instant messaging messages. They can also be disguised as attachments of funny images, greeting cards, or audio or video files. That is why it is essential that you open email attachments unless you know who it's from and you are expecting it.

What is a Bot? a Botnet? a Zombie?

compiled from the FBI by Flicker

You have probably heard such terms as "**Bots**", "**Zombies**", and "**Botnets**" in recent news stories about data breaches and other cybersecurity risks.

A "**Bot**", short for robot, is a type of software application or script that allows an attacker to take complete control remotely of an affected computer. The compromised machine may also be refered to as a "**Zombie**" and a collection of thes infected computers is known as a "**Botnet**".

Hundreds of millions of computers worldwide are infected with **Bots** and under the control of hackers as part of a **Botnet**. The owners of these computers typically do not experience any signs that the machine is infected and continue to use it, unaware they are being controlled by a cybercriminal. In fact, the infected machine could be sending multiple spam emails, including to all contacts in the compute, making it appear that the email is legitimate and from someone they know. They can steal banking passwords and can be used infect other computers on the Internet as well

Flickertronics Business Telecommunications and Internet Service

Ever used an Insurance Broker, or a Real Estate Broker? Why not a Telecom Broker? Let an unbiased broker work on your behalf to find the optimal services for your company.

Flickertronics, an Independent Telecom Broker with over 18 years experience, represents over 30 different Satellite, Telecommunications and Wireless Internet Service providers as well as Colocation Spaces available in over 60 SSAE Hardened Data Centers including **Level3**.

We can often lower your Telephone or Internet bill and keep your existing phone numbers.

Since we don't work for the Telecom Carriers, we don't have any bias towards them. We give you impartial advice.

Call (904)825-6708 for a **FREE, Consultative Review** of your current Telephone & Internet bills. We can even evaluate your internal network!

Business Class DSL
Plans Starting at $49.00/mo.

Business Class Broadband
Plans Starting at $69.00/mo.

Business Class Satellite Broadband
Plans Starting at $79.95/mo.

Business Class 3GWireless Broadband Backhaul
Plans Starting at $189.00/mo.

Ethernet over Copper
Starting at $295.00/mo.

Business T1
Plans Starting at $219.00/mo.

Integrated T1 Voice & Data
Plans Starting at $399.00/mo.

Full DS3 (Equivilent to 28 T1's)
Plans Starting at $4,496.00/mo.

OC-3 (Equivilent to 100 T1's)
Plans Starting at $15,900.00/mo.

Business Class Phone Service

Business Hosted Voice (Business VoIP) starting at $19.00/mo. per line (Satisfaction Guarantee)

This High-Performance, no-maintenance Hosted PBX solution gives your small business the edge.

Hosted Voice works harder and smarter to meet your unique needs, and is used by **Flickertronics** as our in-house phone system. It's a complete solution that includes your choice of business class connectivity, employee calling plans, long distance options, phones, and many key IP features for mobility and productivity with no inhouse, on premise phone system to maintain and repair.

Our Hosted PBX solution gives you unprecedented power and flexibility with significant cost savings - and we stand behind our service with customer support that's intelligent and empowered to help you 24x7x365.

Here's how Hosted Voice helps you take control of your phone service:
Lower Start-Up Costs - No PBX (an on-premise phone switching system) required and to maintain.
Flexible Calling Plans Available - Unlimited & shared minutes
Work Smarter - Advanced IP features for productivity and mobility, Hunt Group and Three Way Calling included!

Switching Phone and Internet Service providers - How The Process Works

Ok, you have decided to switch Phone and/or Internet service providers. Here is how the process typically works.

1. After you place the order for the phone and Internet services you wish to transfer with your new carrier, make sure to give a **valid Email address that you will be monitoring** to your new provider, commonly referred to as a carrier - I will use those terms interchangeably. If **Flickertronics** is your sales agent simply forward those emails to us and we will take care of everything at no cost to you.

a. IMPORTANT - DO NOT CONTACT your current phone or Internet provider - your new carrier will make all the arrangements, and contacting the carrier you wish to switch from yourself may delay the process.

2. You will receive important instructions and notifications via the email address you provided. It is important to monitor that email address and to follow those instructions to ensure a smooth transition.

If you have Flickertronics as your Telecom Sales agent simply forward the emails to Flickertronics and we will coordinate the entire process at no charge to you.

Business Class Cable TV

Basic Cable T.V.	- 30 Channels in a bundle -	**$ 4.95**
Variety T.V.	- 50 Channels in a bundle -	**$29.95**
Standard T.V.	- 80 Channels in a bundle -	**$59.95**

Additional T.V. outlets $9.95 each

Flickertronics usually provides the fastest switchover times on your internal network, and since your new carrier/provider is paying your Independent Flickertronics Telecom Agent for the sale, our on-site networking is done by us at no cost to you!

Unlike all the other local Telecom and Internet "resellers", as an **Independent Telecom Agent Flickertronics** represents the carriers directly, just like your **Independent Insurance Agent** with his products, offering you **MORE** savings, more reliable service and better benefits than the local **"resellers"** are able to offer!

3**. Once the order has been placed**, the new carrier you are switching to will contact the engineering department of your present carrier and let them know to prepare for "Porting" or transferring your existing phone numbers to your new provider, and that they will be your new carrier.

Technicians from your old and new provider may be periodically checking and running outside wiring, and examining and prepping your equipment room up to the point where their services tie into your existing phone or network.

4. At the scheduled time, when the switch from the old carrier to the new carrier is occurring, you will need to have your Telecom Vendor (phone man) and your network technician present when the installer from your new carrier is ready for the switchover.

Here are two confusing industry terms:
Your **Telecom Provider** provides you with phone or Internet service.

Your **Telecom Vendor** is the agency or person responsible for working on your internal phone system and wiring. In other words your **"phone man"**.

Your "phone man" will make sure your in house phone wiring and phone switching system is prepared for connecting to the new carrier's equipment. If you do not have your own "phone man", we can take care of that for you as well.

The new provider's technician will call their engineering department who will coordinate the switchover to your new carrier. The switchover process usually occurs almost instantaneously.

If you are switching Internet service in addition to switching phone service , while the new carriers technician and your phone man have been coordinating the telephone service switchover, the network IT tech has been preparing to switch over to the new network.

On average it can take a technician about 30 minutes to one hour per machine, depending on how your network is configured. **Flickertronics Technicians take about 30 minutes total time for all computers and servers due to our proprietary, well used and proven switchover technique's!**

Flickertronics Managed Services

by Flicker, CEO , Flickertronics

Our Business Managed IT Services are built upon monthly subscription based offerings that can be "assembled" into the products and services that make the most sense for your organization.

Dr. Delgado, of Taino Consultants, and I have been working on packages especially geared toward "Manged Medical Compliance" and the Healtcare industry for the last 5 years, and have come up with our "Modular" approach to Business and Healthcare Managed IT Services.

Flickertronics covers the complete gamut of IT Manged Service and Security Products , while Dr. Delgado provides all the tools you need to comply with **HIPAA** rules and regulations through Taino Compliance's Dashboard. A very good presentation is located at **www.tainoconsultants.com/compliance-software.**

Daily Health Checks

For less than the price of a cup of coffee, we'll conduct a thorough check each and every morning before you start to work. **We'll check:**

Your backup is complete to make sure your data is safe

Your Antivirus pattern file to make sure your protection is always up-to-date

Your disk space to ensure your system won't crash and your workers aren't left unproductive while you recover

Your hard disk and memory health to ensure your system is always in peak operating condition

Your Critical Event logs to spot other developing problems that could cause downtime during the day

The service is performed automatically - so it's guaranteed to happen even if staff are sick or on holiday, If we find problems, we will immediately alert an engineer so he can act fast to cut potential downtime. **We'll even send you a report every morning to confirm the checks carried out and their results.**

The Antivirus report is especially important in proving compliance and ensuring the security and health of your computer systems and network, as mentioned by Dr. Delgado in the article above right.

What would you do if the auditor asked you this one question right now, this very minute?

Auditor's Question: How secure are your computers from attack, how are they protected, and what is the status of that protection at this moment?

Most have answered similar to this:
Answer: " I Don't Know" is the most common in over 75% of practices queried by **Flickertronics** staff.

If you have no logs or reports then, in the auditors presence you can go to each machine, open the Antivirus program, make sure it is updating automatically, make sure all of the protection settings are correct and that the subscription is current for every computer and Server.

To be truthful, I really don't know what you would tell them when you are put on the spot by the auditor, whether it is for HIPAA or an investigator on a cybercrime or data breach case involving your company if you do not have a compliance package.

(*Daily Health Checks continued above right...*)

The Dangers of Technology cont'd

by Dr. Jose Delgado, Ph.D.

Continued from Page 3

Consider this; do you know if someone is using your computer or camera phone to spy on you? What about using your computer to access your accounts or even worst, to use your computer's processing power and connectivity to hack other person's or organizations data banks? **(BOTS)**

There are multiple schemes that are being used by programmers and hackers where they either penetrate your systems or use your systems to penetrate others. The thing that should not surprise you is not that these actions are taking place but of the frequency of the same.

The beauty of technology is that for every problem there may be one or more solutions.

So while technology continues to change, and while even people like me try to stay current with the same, reality is that there are only so many hours in a day. So in my case I decided that the best recourse is to have trustworthy expert, my partner, use his software to monitor my systems.

So every day I receive a report telling me if there are any viruses in my systems, attempts of penetration and a number of potential activities that could indicate suspicious activities, along with a Daily Health Check Report of my computer.

In summary, technology is great, yet understand what you are doing and your vulnerabilities before you implement or release access to your systems. Even better, if you are going to use the new toys, find someone to help protect your assets.

Daily Health Checks continued

With Flickertronics Daily Health Checks, or any of our **Managed Service** offerings, you get email reports of the security staus of each machine in your network, along with the status of your backups, which you can print out and put in your compliance folder or Email archive.

Since all of our offerings include these basic checks and more, you can simply hand the auditor the daily, weekly or monthly printouts from your your compliance folder in your office, or retrieve them from wherever your archive are located.

If you have on of Dr. Delgado's (Taino Consultants) Compliance packages, you can simply, and with virtually no effort, check the boxes for network security compliance and verification of backups in his monthly report log. See **www.tainoconsultants.com/compliance-software.**

Managed Antivirus

Our Managed Antivirus is a highly effective Virus protection based on the award-winning **VIPRE Enterprise Software (ICSA and VB100 certified)** with very low impact on system resources.

Laws such as HIPAA (Health Insurance Portability and Accountability Act), **GLBA** (Gramm-Leach Bliley Act) and the **Sarbanes-Oxley Act** mandate strict protection for data in use, in transit, or in storage.

Our Managed Antivirus, Daily Health Checks and Managed Services generate reports that you simply show the auditor to document your compliance.

Managed Antivirus along with Managed Network Security offers the most reliable protection for your important company data, Network and computers.

As a Microsoft Partner and Microsoft OEM, Flickertronics not only combats, bots, viruses, worms and cybercriminals, our publications demonstrate our intimate knowledge of how these cybercriminals work as well as the tools of their trade!

US_CERT Security Tip (ST06-003)

Staying Safe on Social Network Sites

What are social networking sites?

Social networking sites, sometimes referred to as "friend-of-a-friend" sites, built upon the concept of traditional social networks where you are connected to new people through people you already know.

The purpose of some networking sites may be purely social, allowing users to establish friendships or romantic relationships, while others may focus on establishing business connections.

What security implications do these sites represent?

Some social networking sites rely on connections and communication, so they encourage you to provide a cetain amount of personal information. When decicing how much information to reveal, people may not exercise the same amount of caution as they would in person because

1. The Internet provides a sense of anonymity
2. The lack of physical interaction provides a false sense of security.
3. They tailor the information for their friends to read, forgetting that others may see it.
4. They want to offer insights to impress potential friends or associates

While the majority of people using these sites do not pose a threat, malicious people may be drawn to them because of the accessibility and amount of personal information that's available. The more information malicious people have about you, the easier it is for them to take advantage of you. Predators may form relationships online and then convince unsuspecting individuals to meet in person leading to potentially dangerous situations.

The personal information can also be used to conduct a social engineering attack. Using information that you provide about your location, hobbies, interests, and friends, a malicious person could impersonate a trusted friend or convince you that they have the authority to access other personal of financial data.

Additionally, because of the popularity of these sites, attackers may use them to distribute malicious code. Sites that offer applications developed by third parties are particularly susceptible. Attackers may be able to create customized applications that appear innocent while infecting your compute or sharing your information without your knowledge. (High Security Risk for business networks - Flicker)

How can you protect yourself?

Limit the amount of personal information you post - Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing. Also be considerate when posting information , including photos, about your connections.

Remember that the Internet is a public resource - Only post information you are comfortable with anyone seeing. This includes information and photos in your profile and blogs and other forums. Also, once you post information online, you can't retract it. Even if you remove the information from a site, saved or cached versions may still existon other people's machines.

Hello, My name is Flicker. I am the second graduate of the St Augustine Technical Center's Electronics Technology Program in 1976.

I have been technically involved in the Satellite, Telephone and Cable TV industries for over 38 years, and the computer industry since 1981.

I was employed from 1977 to 1983 at the local Cable TV company, working my way up from installer to **Chief Technician**, and was responsible for supervising and maintaining the entire technical operation of **Jones Intercable**, the local cable TV company at that time, and have held many such positions over the years.

Jones Intercable also used me as a troubleshooter for Cable TV systems in Georgia and South Carolina as well as Florida, and I was the leading troubleshooter for the company.

I started Flickertronics 18 years ago and am happy to give back to the community with my new publication. I hope you enjoy, and find use in, my articles, and the Glasbergen cartoons, which you can also purchase from his site.

US-CERT TIP (ST06-003) Continued

Be wary of strangers - The Internet makes it easy for people to misrepresent their identities and motives. Consider limiting the amount of people who can contact you on these sites. If you interact with people you do not know, be cautious about the amount of information you reveal or agreeing to meet them in person

Be Skeptical - Don't believe everything you read online. People may post false or misleading information about various topics, including their own identities. This is not necessarily with malicious intent; it could be unintentional, an exaggeration, or a joke. Take appropriate precautions, though, and try to verify the authenticity of any information before taking action.

Evaluate your settings - Take advantage of a site's privacy settings. The default settings for some sites may allow anyone to see your profile, but you can customize your settings to restrict access to only certain people. There is still a risk that private information could be exposed despite these restrictions, so don't post anything ou would not want the public to see.

Be wary of third-party applications - Third-party applications may provide entertainment or functionality, but use caution when deciding which applications to enable. Avoid applications that seem suspicious, and modify your settings to limit the amount of information the applications can access.

Use strong passwords - Protect your account with passwords that cannot easily be guessed. If your password is compromised, someone else may be able to access your account and pretend to be you.

Check privacy policies - Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam. Also, try to locate the policy for handling referrals to make sure that you do not unintentionally sign your friends up for spam. Some sites will continue to email messages to anyone you refer until they join.

Keep software, particularly your web browser, up-to-date - Install software updates so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.

Use and maintain Antivirus software - Antivirus software helps protect your computer against known viruses, and some offer added protection from "Viruses in the Wild", or unknown viruses, using Heuristics. Because attackers are continually writing new viruses, it is important to keep your definitions up to date.

"Before we make a hiring decision, we'll be checking your Facebook page for bad behavior. We're looking for someone who would be fun at our office parties."

Flickertronics Featured Customer
Cheshires Customs & Collision
(904)687-5062
23 Pacific St.
St Augustine, Fl 32084

URGENT Consumer Advisory: Vehicle Owners with Defective Airbags Urged to Take Immediate Action

Washington, D.C. - The National Highway Traffic Safety Administration urges owners of certain Toyota, Honda, Mazda, BMW, Nissan, Mitsubishi, Subaru, Chrysler, Ford and General Motors vehicles to act immediately on recall notices to replace defective Takata airbags. Over seven million vehicles are involved in these recalls, which have occurred as far back as 18 months ago.

Department of Transportation Vehicle Safety Hotline at 1-888-327-4236

The message comes with urgency, especially for owners of vehicles affected by regional recalls in the following areas: Florida, Puerto Rico, limited areas near the Gulf of Mexico in Texas, Alabama, Mississippi, Georgia, and Louisians, as well as Guam, Saipan, American Samoa, Virgin Islands and Hawaii.

Consumers that are uncertain whether their vehicle is impacted by the Takata recalls, or any other recall, can contact their vehicle manufacturers website to search, by their vehicle identification number (VIN) to confirm whether their individual vehicle has an open recall that needs to be addressed. Owners that have been contacted by their manufacturer should contact the dealer's service department and make arrangements for repair.

7.8 Million Affected U.S. Vehicles, by Manufacturer, impacted by Recalls

Involving Takata Airbags *compiled by Flicker from www.nhtsa.gov*

The list below was compiled October 20, 2014. Owners should check their VIN periodically as manufacturers continue to add VIN's to their databases.

Once owner recall notices are available, owners can retrieve a copy from **safercar.gov/vinlookup** or **www.techsourcenews.com/recall**, or will receive one by US mail and are advised to carefully follow the enclosed instructions,

BMW
2000 - 2005 3 Series Sedan
2000 - 2006 3 Series Coupe
2000 - 2005 3 Series Sports Wagon
20000 - 2006 3 Series Convertible
2001 - 2006 M3 Coupe
2001 - 2006 M3 Convertible

Chrysler
2003 - 2008 Dodge Ram 1500
2005 - 2008 Dodge Ram 2500
2006 - 2008 Dodge Ram 3500
2006 - 2008 Dodge Ram 4500
2008 - Dodge Ram 5500
2005 - 2008 Dodge Durango
2005 - 2008 Dodge Dakota
2005 - 2008 Chrysler 300
2007 - 2008 Chrysler Aspen

Ford
2004 - Ranger
2005 - GT - 2007 Mustang

General Motors - GM
2003 - 2005 Pontiac Vibe
2005 Saab 9-2X2005

Honda
2001 - 2007 Honda Accord
2001 - 2002 Honda Accord
2001 - 2005 Honda Civic
2002 - 2006 Honda CR-V
2003 - 2011 Honda Element
2002 - 2004 Honda Odyssey
2003 - 2007 Honda Pilot
2006 - Honda Ridgeline
2003 - 2006 Acura MDX
2002 - 2003 Acura TL/CL
2005 - Acurs RL

Mazda
2003 - 2007 Mazda6
2006 - 2007 MazdaSpeed6
2004 - 2008 Mazda RX-8
2004 - 2005 MPV
2004 B-Series Truck

Mitsubishi
2004 - 2005 Lancer
2006 - 2007 Raider

Nissan
2001 - 2003 Nissan Maxima
2001 - 2004 Nissan Pathfinder
2002 - 2004 Nissan Sentra
2001 - 2004 Infiniti I30/I35
2002 - 2003 Infinity QX4
2003 - 2005 Infiniti FX35/FX45

Subaru
2003 - 2005 Baja
2003 - 2005 Legacy
2003 - 2005 Outback
2004 - 2005 Impreza

Toyota
2002 - 2005 Lexus SC
2002 - 2005 Toyota Corolla
2003 - 2005 Toyota Corolla Matrix
2002 - 2005 Toyota Sequoia
2003 - 2005 Toyota Tundra

Information on NHTSA's Investigation 06/11/2014

identification numbers10537899, 10568848, 10585224

Excerpts from www.safercar.gov compiled by Flicker

ODI (Office of Defect Investigation) RESUME

Investigation: PE 14-016
Date Opened: 06/11/2014
Investigator: Peter Ong Reviewer: Scott Yon
Approver: Frank Borris
Subject: Air Bag Inflator Rupture

ODI is opening this investigation in order to collect all known facts from the supplier and the vehicle manufacturers that it believes may have manufactured vehicles equipped with inflators produced during the same period as those that have demonstrated rupture events in the field.

MY = Model Year **VOQ** = Vehicle Owner Questionnaire

Manufacturer & Product Information
Manufacturer: Takata Corporation, Honda (American Honda Motor Co.), Nissan North America Inc., Mazda Motor Corp., Chrysler Group LLC., Toyota Motor Corporation
Products: MY 2002-2006 models with air bag modules supplied bt Takata
Population affected: 1,092,000 (Estimated)

Action/Summary Information **Action:** Open This Peliminary Evaluation (PE)

Summary: In **August 2013,** the **Office of Defects Investigation (ODI)** received a complaint of a driver's bag inflator rupture in a **Model Year (MY)** 2005 Honda Civic (VOQ 10537899). In March 2014, ODI received a VOQ alleging a passenger's bag rupture on a MY 2003 Toyota Corolla (VOQ 10568848)
In April 2014, ODI received a third VOQ alleging a driver's bag rupture in aThere were three alleged injuries from these three incidents and all appeared to be minor in nature. ODI discussed these incidents with TK Holdings, Inc. (Takata), the supplier of airbags involved and with the affected vehicle manufacturers. In the course of its review, MY 2005 Mazda 6 (VOQ 1058224).

Takata identified two other incidents, one involving a passenger bag rupture on a MY 2004 Nissan Sentra vehicle, and another a driver's bag rupture on a MY 2006 Dodge Charger vehicle. Toyota also provided another passenger's bag rupture on a MOf note, all six incidents occurred in a high absolute humidity climate (Florida and Puerto Rico.) By way of background, several manufacturers in recent years have conducted safety recalls of vehicles for rupturing airbags. In calendar years 2008 through 2011, Honda conducted a series of recalls concerning driver's bag inflator ruptures on various MY 2001 through 2004 vehicles. In calendar year 2013, Honda, along with Toyota, BMW, Nissan and Mazda, initiated safety recalls to address passenger bag ruptures in certain MY 2001 through 2004 models. **None of these recalls were regional in nature or attributable to atmospheric conditions in field use.Y 2002 Toyota Corolla.**

Manufacturers recall search by VIN pages

www.techsourcenews.com/recall

All major light vehicle and motorcycle manufacturers are required to provide VIN search capability for uncompleted recalls on their websites. This data must be updated at least weekly.

Consumers can find their vehicle identification number, or VIN, by looking at the dashboard on the driver's side of the vehicle. or on the driver's side door post where the door latches when it is closed.

Vehicle owners can call the Department of Transportation Vehicle Safety Hotline at 1-888-327-4236

NHTSA Vehicle Recall Look-up by VIN

www.safercar.gov/vinlook

NHTSA's new search tool lets you enter a Vehicle Identification Number (VIN) to quickly learn if a specific vehicle has not been repaired as part of a safety recall in the last 15 years.

This tool covers:
Safety recalls that are incomplete on a vehicle.
Safety recall conducted over the last 15 calendar years.
Safety recalls conducted by major light automakers, including motorcycle manufacturers.

Parents Central

www.safercar.gov/parents

From Car Seats to Car Keys Keeping Kids Safe

This is the Gateway to Information and resources for keeping your kids safe when they are on the move. You will find the answers to the most common questions you may have - whether buying their first car seats or handing your teen their first sets of car keys.

This site covers thing such as car seats, teen driving, school bus , walking and biking safety It also covers such dangers as Backover accidents, Heatstroke, Power window dangers, and many other safety items and concerns.

ODI is opening this investigation in order to collect all known facts from the supplier and the vehicle manufacturers that it believes may have manufactured vehicles equipped with inflators produced during the same period as those that have demonstrated rupture events in the field.
The ODI reports cited above can be reviewed online: **http://www-odi.nhtsa.dot.gov/owners/SearchNHTSAID** under the following identification numbers: 10537899, 10568848, 10585224

Easy Tips

(Continued from page 1)

... or trick you into thinking they are an official site and fool you into downloading a bunch of junk to your computer.
Some sites may impersonate tech support for **Microsoft** or others so beware. Always look to un-check add-ons and toolbars on installations when downloading useful software.

Tip 7 - Go to the Official Web Site if a download file pops up and says it needs to update or you need this program to view info.

Tip 8 - You should not open suspicious Emails or links in Emails unless you are sure of the source and it was sent by them intentionally. Some email viruses are usually sent disguised under a familiar company name such as **UPS** or **FEDEX**, or they are sent from hacked Email to all contacts in your address book. Some try to collect info called **Phishing** and can be destructive and encrypt your pictures or documents.

Tip 9 - Block your camera with a sticker or cover of some sort when you are not using it.

Tip 10 - Important - Always back up important data including pictures, documents, favorites, tax info, Quickbooks, music and anything important so your files are in at least two places.
Backup media includes DVD's, Flash (USB) drives, USB Hard Drives, NAS Drives(Network Attached Storage) and Cloud Media.

A Sustainable St Augustine

Dream Green-Single Stream

The City of St Augustine's Solid Waste Department is working diligently on expanding recycling efforts and diversion rates. This is proving successful due to **Single Stream Recycling (SSR)**. **SSR** is a method of collection for materials which can be mixed together in one bin. This type of curbside and commercial collection is on the rise Nationwide and offers more efficient recycling.
With the implementation of **SSR** in the city wide over the past few months, now making it easier.

Continued above right next column

(*Cont'd from below left*)

Recycling tonnage has increased overall, while the volume of material going to our landfills has decreased significantly. The reason for this transition is due to broadening the residential and commercial awareness of the city wide recycling programs currently in place. Thus boosting the commodities that can be co-mingled, as well as the value created in sustainability for the entire city. Not only are there more materials that can now be collected with proper resources, there are new programs coming in to place to divert additional items.

One substantial program that has taken off is the **E-Waste Program** (electronic and battery waste such as appliances and computer components.) The units are being streamed away from our landfills for adequate dismantling and recycling.

Another focus is to target high tourist volume areas such as St. George St., Castillo de San Marcos Fort and The Visitor Center. The expansion of our commercial recycling program and the participation is growing daily.

Some changes to look forward to will be cardboard dumpsters, and three drop off locations in various parts of the city, receiving revised decal signage. These, with the aid of pictures, create education as to what "Co-Mingled" and "Single Stream Recycling" entails. Also, Solid Waste will be painting these bins over the next few months green to assist in recognizing these as free, multistream recycling collection points.

The Solid Waste Department has implemented mandatory recycling at Francis Field for special events. This has proved both positive and effective in reducing the amount of recyclable material going to the landfill. This has also created further recognition of the city's continuous endeavors to be clean and green! For a list of recyclable material, please visit **www.ci-st-augustine.fl.us**.

We appreciate everyones participation as being part of the solution!

For additional information, Please contact:
Olivia Smith
City Recycling Coordinator at Solid Waste
904-825-1049 osmith@citystaug.com

LET'S TALK TRASH!

by Mandy, Vice President, IT Tech, Flickertronics

According to Keep America Beautiful, in 2009, we filled U.S. landfills with trash equivalent to the weight of 88 million cars. In one of the EPA'S most recent e-waste reports it shows that we got rid of (trashed or recycled) 142,000 computers and over 416,000 mobile devices every day! In 2012, we generated 3.42 million tons of electronic waste in the U.S. Of this amount, only 1 million tons or 29.2% was recycled, according to the **EPA** (up from 25% in 2011) The rest was trashed in landfills or incinerators.
The benefits of keeping electronic waste and other trash out of the landfills are numerous. These items are filled with hazardous chemicals that pollute our environment. These toxins will effect the water we drink, food we eat and the air we breathe. According to the **EPA**, for every million cell phones we recycle, 35 thousand pounds lbs. of copper, 772 lbs. of silver, 75 lbs. of gold and 33lbs. of palladium can be recovered. Recycling metals from e-waste uses a fraction of the energy.

RECYCLE

In talking with Olivia Smith for just a few minutes, you know she has a passion for recycling. Before being hired as the City's first St. Augustine Recycling Coordinator, Olivia worked in California in the industry for many years. She is now working for the City implementing new recycling opportunities and protocols such as organizing the new **free drop off only** facility for **Electronics nd Battery Recycling** at **601 Riberia St.** For more information call **904-825-1049**

REDUCE

Reduce Waste, trade your unused or partially used art supplies and materials with other artists! **Melissa**, Owner of the **Red Sable Art Supply** at **107 King Street** (inside St. Johns Printing) will be hosting an **Artist Swip-Swap Event** the last Saturday of every month from12:00pm- 2:00pm. Just bring your art supplies you haven't used in a while and trade with other artists for materials you will use. This is a great way for reducing waste of art supply materials! For more information call **904-707-2861** or on the web **www.theredsable.com**

REUSE

St. Augustine has a number of artists in the community that work with found objects. **Steve Marrazzo**, artist and owner of **Simple Gestures** on **Anastatsia Blvd at 4 White St. E**, has been assembling found object art pieces for years including sculpture and jewelry which he displays and sells at his gallery gift shop.
He once had a heart shape, on a recycled board, made from old keys. His latest show is called **Lost and Found** and features all recycled materials including sculptures made from gears, nuts and bolts, door knobs, rifle butts and antique car lights. For more information call **904-827-9997** or check out their Facebook page.

REFURBISH

When you drop off your unused and unwanted computers and laptops to **Flickertronics** their techs will wipe your personal information at no charge. The computers will then be processed and it will be determined if the computers can be recycled or refurbished, and if any parts are usable to sell at a low cost or for charitable donations.
Flickertronics, in business over 18 years, has always had a concern for the environment and has worked with organizations such as the Guana River Preserve and the ST Augustine Technical Center ***(Flicker was the second person to graduate their Electronics Technology program in 1976)*** For more information call **904-825-6708**. **Flickertronics recycling efforts has kept over 20,000 pounds of lead (10 Tons) out of the landfills**, not to mention all the other poisonous metals and substances kept from poisoning the Earth.

In conclusion, recycling is easy. It can also be creative and fun and every item that is recycled will help leave a smaller imprint and make a difference for future generations.