

**In this Newsletter:**

- [North Chamber CIO Resource Book](#)
- [RFID - Privacy and Security \(Part 3\)](#)
- [Phishing and Pharming - Protecting Yourself in today's Wireless World](#)
- [Dell's Jeff Clark - Distinguished Speaker Recap](#)
- [The Wonderful Wizards of SBS](#)
- [Local News - Items of Interest](#)
- [Need more information?](#)
- [Contact Us](#)

 **No Technology Vendor Left Behind!**

In an effort to further increase our offerings to chamber members, The North San Antonio Chamber is creating the 'CIO Resource Book'. This is a directory listing of technology chamber members and the technology products/services they offer.

The CIO Resource Book will be made available at our monthly CIO Breakfast and is designed to give busy CIO's a quick and accurate resource listing of local chamber members who may be able to provide the specific technology products and/or services being sought.

We invite and encourage you to submit your information for this great resource! It's FREE and it will only take a moment!

The CIO Resource Book committed has created a preliminary listing of Vendor Types (or categories) for technology products and services. That list can be viewed at;

[www.northsachamber.com/CIO\\_vdr\\_types.htm](http://www.northsachamber.com/CIO_vdr_types.htm)

Once you've had a chance to go through the Vendor Types - send an email to [Billy Pitts](#), the chair of the CIO Resource Book, with the following information;

- Company Contact Information

- Vendor Type(s) from the list above (choose as many that apply to actual products and services you offer - please do not choose for anticipated or future offerings)

If there's a vendor type that you do not see and think should be included - let Billy know.

Don't be left behind!

[More Info](#) - [Top](#)

---

## RFID - Privacy and Security

**Author:** [Bede Ramcharan, FACHE, Instant Data Technologies \(Indatatech\)](#)

*This is the third of three articles on RFID (Radio Frequency Identification). The first article provided a basic foundation for what is RFID, and how it is being used today. The second article went into more depth about the various types of RFID technology and standardization issues. This third article deals more with some of privacy and security issue concerning RFID..*

In the last two articles, we have learned how RFID works and some of issues surrounding standardization. Supply chain networks have realized the importance and value-add services that RFID can bring. The biggest challenge facing RFID are the myths concerning privacy and security of the technology.

Imagine this scenario; you purchase a movie ticket to see the new Star Wars Movie. The movie ticket is embedded with a RFID tag to help the movie theater track ticket sales and customer movements. You don't like the movie, so you try and sneak in to see the latest horror flick. Soon after you are settled in, and usher comes to your seat and gently reminds you that you are in the wrong theater. Your RFID enabled ticket didn't match the movie theater you are in and notified management. So you leave embarrassed, and head to the mall. Once there, you enter the movie rental chain store to find a good movie to watch at home. A clerk approaches you, and asks – "How was Star Wars?", and offers to show you where the other episodes of Star Wars and similar movies are kept. Your RFID enabled ticket was read when you walked in the store, and the clerks knew how to approach you. Sound far fetched? Not really. All of these events are within the technological capabilities of RFID.

The Electronic Privacy Information Center (EPIC) published a set of guidelines which went before Congress. These guidelines focused on consent, third part access, and security. The EPIC is a public interest research center in Washington DC. It was created in 1994 to focus

on emerging civil liberty and constitutional freedom issues. The mandates focused on letting the consumer know that 1) RFID technology is being used, 2) Obtain consent from the consumer 3) Do not sell information to third parties without the consumer's consent. Toll tags currently scan your car as you pass through the gates to charge your account – they also record the time, direction and speed of travel. In a recent criminal case the prosecutor used this information to establish proximity to a crime for the suspect.

RFID technology is not inherently insidious. The technology is like any other technology, it will be used for both good and not so good purposes. It will remain up to the users to constantly demand and implement practices and protocols that will protect us from misuse.

[More Info](#) - [Top](#)

---

## **Phishing and Pharming - Protecting Yourself in Today's Wireless World**

**Author:** [Matt Reedy](#), [Armida Technologies](#)

A recent Wall Street Journal article described two new threats to wireless road warriors, supplanting last year's infamous round of "phishing" emails. You probably received some of those phishing notes, claiming to be from a bank, credit card company, Ebay, or a member of a wealthy royal family from a small African country wanting to use your bank account to transfer funds. Unfortunately, the bad guys are getting smarter, and are now using two new techniques to try to steal information about you when you are online: "**evil twins**" and "**pharming**."

Evil twins are wireless networks that pretend to be Internet connections like those available at coffee shops, hotels and other public places. On a laptop screen, an evil-twin hotspot can look just like the real thing, even to the point of copying the genuine provider's sign-in page. They are created by hackers who turn on an illegitimate wireless access point near a public one, and use their signal to overpower the legitimate one. Then they try to capture passwords or credit-card information that you might enter.

In pharming, crooks actually change an Internet address inside a server and redirect you to an imposter Web page, even though you may have typed the correct web site name in your browser. They use a technique known as "DNS poisoning" within Internet service provider servers. Some ISPs and business continue to use unprotected software on their servers that lets the bad guys in to do this dirty deed.

To protect yourself from accidentally accessing an evil twin, you should disable your laptop's wireless function when not in use. You can also go online at the office (or in another "wired" connection) to sign up for the hotspot service that you are planning to use – providing your credit card information over a wired connection is much safer than over a

wireless connection. Some hotspot providers, such as T-Mobile, provide free software for laptops that automatically ensures a Wi-Fi network's digital ID certificate is legitimate. One way to protect yourself from pharming is to make sure your browser address bar shows the special "secure" Web page address that uses encryption ("https" rather than "http") to protect data transfer. These sites are automatically sending a digital ID certificate to your browser to indicate they are certified; web browsers will warn you if the certificates are illegitimate.

[More Info](#) - [Top](#)

---

## ★ Distinguished Speaker - Great Success

Contributed by : [Debby Zucker](#), [North SA Chamber](#)

On May 24th, the North SA Chamber hosted Jeff Clarke, Senior VP with Dell, as part of our Distinguished Technology Speaker Series.

Mr. Clarke engaged the over 250 attendees with his personal experiences and thoughts on leadership. He offered a rare insider's view of Dell's growth and challenges as it transformed from a \$79 million company called PCs Limited to the \$50+ billion Dell of today.

We'd like to thank our event sponsor, Rackspace, for their support. We'd also like to express sincere appreciation to our volunteers, table sponsors, and attendees who helped make this a great event!



[More Info](#) - [Top](#)

---

 **The Wonderful Wizards of SBS**

Contributed by : [Larry Lentz](#) , [Lentz Computer Services](#)

When you go out to your car, you put your key in the lock and start your engine.

Why don't you turn on the spark, put it in neutral, put in the hand crank and crank it to get it going instead?

Because you've learned to use the 'wizard' the car manufacturer provided for you in the form of the starter and ignition system. With Windows Small Business Server 2003®, Microsoft has provided a wonderful set of wizards for starting up (configuring) SBS. Unfortunately not everyone uses these wizards, at least at first. The main culprits are MCSEs (like me) and folks who are used to large (Enterprise) systems. Somehow they feel they know better and using the wizards is 'beneath them'. Luckily I learned at an early age (SBS 4.0 in 1997) to use the wizards. James Fogg, a contributor to the [SBS List newsgroup](#), recently stated;

"As someone coming from enterprise Windows environments I had a hard time accepting the advice I received about how "SBS is different", and the advice to "always use the wizards". I was not so stupid as to ignore the advice, so I didn't have to learn the hard way, but I can now say it's all true."

The wizards take care of all the 'little things' that make SBS such a great package. Ignore them at your peril.

I recently had the opportunity to work on a Small Business Server where the original installer had not used the wizards. The individual users and computers had been joined to the domain manually instead of using the Set Up Computer Wizard. Of course all appeared to work. But, when you add computers manually, their accounts are by default placed in the Computers container in Active Directory. When using the wizard, they are placed under the My Business organizational unit (OU), actually a few levels deeper in the OU hierarchy. This may be a subtle nuance but it can have big consequences.

I installed ISA Server on the SBS server. Having done that, I now needed to install the ISA Firewall Client on the users' workstations. Normally I create a Group Policy Object (GPO) and link it to the My Business OU. This way it is automatically installed on all of the network computers except the SBS server itself. The SBS server is in the Domain Controllers OU. However since all the computers were in the Computers *container* and you can't link GPOs to a container, I linked it at the domain level. This worked fine for the

workstations. However I noticed that it took for-e-ver to log onto the server. I mean an hour! I eventually figured out it was because the GPO also installed the Firewall Client on the server. A big no-no I learned. I won't do that again. I reconfigured the workstations using the wizards and moved the GPO to the appropriate OU. Then the server logged on fast and the workstations had their Firewall Client so they could access the Internet. Had the wizards been used in the first place, I wouldn't have had this problem.

When you first install Small Business Server 2003, the installation process ends with the To-Do List. This provides a handy way to work your way through the primary wizards to properly configure your server. They are presented in the recommended order but can be run in the order that best suits your needs. Once you've used the wizards, you may go back and make your own adjustments if you must. But run the wizards first.

[More Info](#) - [Top](#)

---

## Local News - Items of Interest

### **TxCAP - Economic Development Forum & Networking Reception**

Is your company looking for funding?  
Are you interested in networking with emerging businesses in Texas?  
We invite you to the Texas Coalition for Capital's

#### **ECONOMIC DEVELOPMENT FORUM & NETWORKING RECEPTION**

Wednesday, June 29, 2005

3:00 p.m. – 6:30 p.m.

San Antonio , Texas

- Join key policy makers as they give you a legislative overview of the CAPCO Program and the Emerging Technologies Fund
- Learn how Texas can stay at the forefront of emerging technologies
- Be briefed on the CAPCO Program and how it works
- Participate in a discussion with representatives of venture capital firms interested in participating in the CAPCO Program on when the funds will be available, and how your company can qualify

Please contact [Elizabeth James](#) for more information or call (512)476-4403.

[More Info](#) - [Top](#)

---

## **Need More Information?**

If you would like more information on any of the articles in this newsletter the following options are recommended;

- Discuss the article with your IT professional.
- Contact the Author of the article (contact info is available within the article)
- [Contact us](#) and we will help you find the resources you need.

If you would like information on a topic not included in the eNewsletter - please let us know and we'll do our best to find the information you need and have it included in the next eNewsletter!

This newsletter is a combined effort of the North Chamber Tech Committee and The Montopolis Group. All input is provided by Chamber members. [Top](#)

---

## **Contact Us**

### **Technology Chair**

[John Dickson](#)

Partner

[Denim Group, Ltd.](#)

### **North Chamber Contact**

[Debby Zucker](#)

Director of Finance/IS

[North SA Chamber](#)

### **Editor**

[Katrina D. Mukherjee](#)

Vice President

[The Montopolis Group](#)