



April 2013

In this issue. . .

- ▶ Letter from the President
- ▶ Data Growing Pains
- ▶ What to Do If You're a Victim
- ▶ Tune Up Your Telephone Skills
- ▶ Business Continuity Tip
- ▶ Cartoon & Quote

Tune Up Your Telephone Skills

by Debra J. Schmidt



How do you sound to your customers and co-workers? First impressions are lasting impressions. That's why every telephone conversation counts. The impression you make on your co-workers and customers is based on your tone of voice, energy and attitude.

Because so many workplace transactions are conducted solely by telephone, it is extremely important to have an awareness

Letter from the President

Network security over the past five years has become an increasingly important need and service for both small businesses and large corporations. As a result of increased online technology, mobile hackers now have better opportunities to infiltrate mobile application systems and websites. Cyber hacking has become a growing security problem for countries, governments and businesses of all sizes.

Some recent examples of hacking include:

- Nissan
- Wells Fargo, Bank of America, Citigroup
- Fox News
- Time Warner
- Exxon, Shell & BP
- Australian, Thailand Government and business sites

One industry that utilizes outside network security services frequently is the financial and banking industry. This includes credit unions, credit card companies, money transfer centers and large banking institutions. Most of these businesses offer mobile financial applications for their customers and often need iPad security services. This service is designed to provide customers added protection while they perform mobile money transfers and other online financial transactions. Creating a secure passcode and using a safe connection are just a few of the tips recommended for enhanced iPad security.

So how do you prevent it? Although most businesses today have an in-house IT support team, most are not fully trained and equipped to handle all of today's network problems. Because of this, many businesses are contracting outside IT companies to assist them.

Recent events strongly illustrate that hackers are out there, and they're targeting businesses of all sizes and industries. In some cases, they're looking to steal product designs, intellectual property or other information. Others are flat-out looking to access account information and steal money! Either way, the threats continue. Please contact us to discuss proactive security options for your business.

Scott Huotari, Founder, President/CEO

of how you sound during these conversations.

[Read more](#)

Business Continuity Tip Stay Afloat

The Midwest was hammered with yet another snow storm recently. And with winter weather on everyone's mind, it's hard to believe that it's officially spring.

As the snow melts and temperatures rise, flooding becomes a major issue in many parts of the country. According to FEMA, floods are one of the most common and expensive natural disasters. All it takes is a few inches of water to cause thousands of dollars of damage. So what can you do to protect yourself, your family and your business? Check out Agility Recovery's [Flood Preparedness Checklist](#) and [Ready.Gov's Flood Awareness](#) page.

*No winter lasts forever:
no spring skips its turn.*

- Hal Borland

Laugh a Little



"Yep, that seems right."

Data growing pains?

used with permission from HP Technology at Work

Virtualization. Like other technology buzzwords, some users work this term into business conversations without really understanding its meaning or how its strategic application can streamline operational efficiencies, improve resource allocation, enhance network security and reduce costs.



It's worth learning. Careful evaluation of existing non-virtualized environments is the most vital first step toward choosing the best virtual server and storage solutions for any given environment. This evaluation should be done with an eye on present and anticipated computing and power requirements, as well as the number of existing and future users.

Growing data storage requirements are always a major concern of large corporations and institutions. But "big data" has become an issue for small businesses, too. Varying operating systems, a growing number of applications and the increased use of mobile, BYOD and other technologies threaten to overwhelm existing physical server and storage solution capacities.

Rather than allocating resources toward upgrading aging servers or buying new ones—the 'ol "throwing good money after bad"—more IT and other administrators see the benefits of "going virtual." Indeed, [Acronis' Global Disaster Recovery Index](#) found that 21 percent of surveyed small businesses planned to adopt virtualization last year, a number most likely to increase in 2013.

[Read more](#)

What to Do If You're a Victim

used with permission from Norton by Symantec

Introduction

There is a nonstop flood of Trojan horses, bots, and phishing attacks assaulting the Internet every day. Crimeware attacks and identity theft can happen to anyone. If you believe you have been a victim of crimeware or online fraud, there are a series of steps you can take in each instance to respond to and recover from the incident.



Crimeware

Disconnect immediately. Whether you're connected to the Internet via wi-fi or a phone or cable line, disable your connection as soon as possible. This can prevent data from being leaked back to the cybercriminal. Breaking your network connection is a sure-fire way to put a stop to the immediate damage. Aside from physically unplugging your Internet connection, you can disable your network connection by clicking on your PC's start menu, selecting "Settings," then selecting "Network Connections," and finally disabling your network connection by right-clicking on it and selecting the "Disable" option.

[Read more](#)

202 East Mill Plain Blvd | Vancouver, Washington 98660 | 360.944.5111 | www.ccsipro.com

