



TECHNOLOGY TIMES

"Insider Tips To Make Your Department Run Faster, Easier and More Efficiently"

Expiration notice

If your department is currently running Windows Server 2003 or Exchange 2003, on any servers in your office, you need to know about a dangerous security threat to your department that must be addressed very soon. Please take a moment to read the important announcement.

We are aggressively reaching out to all Law Enforcement Agencies in the northern NJ area that use Server 2003 to alert you to this serious security risk to your department and inform you about what you need to do now to protect your department.

Windows Server 2003 and Exchange 2003 Replacements Must be Made by July 14, 2015

Microsoft has officially announced that it will retire all support on the Server 2003 operating system on July 14th, 2015. That means that any department with this operating system still running will be completely exposed to serious hacker attacks aimed at taking control of your network, stealing data, crashing your system, and inflicting a host of other crippling problems you do NOT want to deal with.

Free Windows 2003 Migration Assessment

At no cost, we'll come to your office and conduct a full analysis of your network to help you determine what specific servers will be affected by this announcement. Additionally we will provide a detailed analysis of all upgrade options available to you, along with the pros and cons of each option. While there, we will also assess other security, backup and efficiency factors that could be costing you in productivity. We will then put together a customized Server 2003 Migration Plan specifically for your office.

To secure your FREE Windows Server 2003 Migration Plan,

Call us today at 973-560-9050

Important: Due to the intensive one-on-one time required to conduct these Risk Assessments, we can only make them available for free for the first 4 requests.



"As a Police Chief, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"

- Shawn Butt
Police IT Support

February 2015

Whippany, NJ

Inside This Issue...

Windows Server 2003 End of Life...Page 1

Stay Secure While Using Public WiFi...Page 2

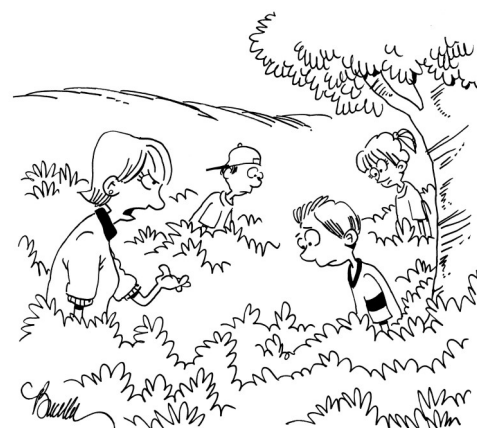
App of The Month...Page 2

Meet Prizm...Page 3

How To Grow Star Performers...Page 3

Protect Yourself From Online Credit Card Fraud...Page 4

Punch a Painting, Go to Jail...Page 4



"Sure, it's all fun and games until someone loses an iPhone."

How To Keep Your Laptop Secure When Using Public WiFi Hotspots

They are everywhere these days. WiFi hotspots for checking e-mail and hopping on the Internet can be found in airports, coffee shops and even most fast-food joints. But have you ever wondered, just how safe is it to connect? With the proliferation of hackers, viruses and identity theft at an all-time high, you are smart to be concerned. Unfortunately, it is easy for a hacker to set up a WiFi spot to access your laptop, called an "evil twin." An evil twin is a wireless hotspot that is used to lure people from a nearby, legitimate hotspot. For example, when logging in at your favorite coffee shop, you may have inadvertently logged in to an evil twin Internet connection set up by the person working on a laptop at the next table.

Just like legitimate sites, evil twins allow you access to the Internet, but in the background they record everything you are typing. Log on to your e-mail, investment web site or bank account, or buy something online, and they are recording your keystrokes.

Tip: Do you want an easy way to securely access your network and the Internet from anywhere? **Call us today at 973-560-9050** about setting up a VPN for your office!

You may be asking, "How do I protect myself at WiFi hotspots?" First you need to make sure the hotspot is legitimate. You can do this by asking someone who works at the WiFi location; in fact, some businesses will give you printed instructions that include the hotspot name. Even here you need to be careful. Many times, in an attempt to make you feel comfortable, the hacker will use an evil twin name that mimics the legitimate hotspot and, on some occasions, the fake site may even show up at the top of your network list by having a stronger signal than the legitimate site.

The best protection you can have is connecting via your company's VPN (virtual private network).

A VPN protects your online information by encrypting your data and activity even if you're connected through an evil twin. If you don't have a VPN, the best protection is to surf the net, but never type in password, credit card, social security, bank account or other sensitive information when connected to a public WiFi hotspot.

Police IT Support's App of the Month - Dropbox



Dropbox is a great storage App for all of your videos, pictures, documents and other files. Anything that you have stored in your Dropbox will automatically be shared to all of the devices that Dropbox is installed on. Dropbox is like a normal folder on your computer where you can store your files and documents. The great thing about it is that every file that you put in your Dropbox is automatically backed up to the cloud to keep it safe and secure.

Installing Dropbox

1. On your Computer - open up your web browser and go to www.dropbox.com and click the sign up button. Follow their instructions and download.
2. On your Portable Device - open your device and go to the App Store on your Windows, iOS or Android Phone/Tablet and search for Dropbox and press install.

Shiny New Gadget Of The Month:



Prizm

This month's gadget is so new, it isn't even off the assembly line. Meet Prizm — a small, pyramid-shaped device designed to make your home-audio experience as hands-off as humanly possible. The device was recently backed on Kickstarter this past November. The French company behind the audio device wanted to create an intuitive music experience that brings users new music, while learning what they really love to listen to.

The device streams music from cloud services such as Deezer, Spotify and SoundCloud, with more services planned in the future. It works by accessing your WiFi network. It doesn't contain any speakers, so you'll have to supply your own (it connects via Bluetooth, 3.5 mm stereo jack and optical audio). And despite being called hands-off, the device sports buttons to let you like or skip songs to customize your listening experience.

It can currently be pre-ordered from www.meetprizm.com for \$139.

HOW TO GROW STAR PERFORMERS

A study of computer programmers at Bell Laboratories showed that the star performers outperformed moderate performers by a margin of 8 to 1. If that holds true in your organization, the conversion of five of your moderate performers into star performers would be the equivalent of adding 35 moderate performers to your workforce. Where are you going to find the five additional star performers? You don't find them. You develop them.

The Bell Labs study identified nine work strategies that characterize star performers. All of them are qualities that can be inculcated through a good corporate education system. According to researchers Robert Kelly and Janet Caplan, these qualities are:

- 1) **Taking initiative:** accepting responsibility above and beyond your stated job, volunteering for additional activities and promoting new ideas.
- 2) **Networking:** getting direct and immediate access to coworkers with technical expertise and sharing your own knowledge with those who need it.
- 3) **Self-management:** regulating your own work commitments, time, performance level and career growth.
- 4) **Teamwork effectiveness:** assuming joint responsibility for work activities, coordinating efforts and accomplishing shared goals with workers.
- 5) **Leadership:** formulating, stating and building consensus on common goals and working to accomplish them.
- 6) **Followership:** helping the leader to accomplish the organization's goals and thinking for yourself rather than relying solely on managerial direction.
- 7) **Perspective:** seeing your job in its larger context and taking on other viewpoints, like those of the customer, manager and work team.
- 8) **Show-and-tell:** presenting your ideas persuasively in written or oral form.
- 9) **Organizational savvy:** navigating the competing interests in an organization, be they individual or group, to promote cooperation, address conflicts and get things done.

Star performers considered initiative, technical competence and other cognitive abilities to be core competencies. Show-and-tell and organizational savvy were on the outer edge of their circle of importance. Middle performers placed show-and-tell and organizational savvy at the center. While star performers were focused on performance, middle performers were focused on impressing management.

Star performers and middle performers also showed marked differences in their attitudes toward networking. The middle performers waited until after they had encountered problems before looking around for someone who could provide help and support. The star performers built a network of helpers and supporters in advance, so they could call on them immediately when needed.

The study concluded that "Individual productivity... depends on the ability to channel one's expertise, creativity and insight into working with other professionals."

Star performers emerge from educational systems tailored to the individual company and the individual job. They don't want to become clones. Too many companies today are content with training programs that provide people with knowledge and expertise, but skimp on educational processes that teach them to apply what they learn. You can't train them to seek excellence. You change that attitude through consistent input that appeals to an individual's self-interest and organizational spirit.



Dr. Nido Qubein is president of High Point University, an undergraduate and graduate institution with 4,300 students from 40 countries. He has authored two dozen books and audio programs distributed worldwide. As a business leader, he is chairman of the Great Harvest Bread Company, with 220 stores in 43 states. He serves on the boards of several national organizations, including BB&T (a Fortune 500 company with \$185 billion in assets), the La-Z-Boy Corporation (one of the largest and most recognized furniture brands worldwide) and Dots Stores (a chain of fashion boutiques with more than 400 locations across the country). As a professional speaker, Dr. Qubein has received many distinctions, including the Golden Gavel Medal, induction into the International Speaker Hall of Fame and as the founder of the NSA Foundation in Arizona. To learn more about Dr. Qubein, go to: <http://www.nidoqubein.com/>

Protect Yourself From Online Credit Card Fraud



The past couple of years have been a rough ride for anyone who relies on a credit card to make purchases. Data breaches have plagued retail stores in the U.S. and Canada. Credit card providers are set to roll out new, more secure credit cards to consumers this year, catching up to Europe and

much of Asia in terms of credit card security. The U.S., in particular, has lagged behind in credit card security due in part to the cost of upgrading both the cards themselves and the pay terminals.

If you are concerned about your credit card information falling into the wrong hands, there are several steps you can take to protect yourself:

Only give your credit card information to secure and trusted web sites.

Never enter any personal or financial information on a non-secure web page. If you don't see "https" in the web address, move along.

Monitor all activity. Regularly check your credit card and bank statements. The simplest way to spot fraud is to monitor all your financial activity. Many credit card providers have custom alerts you can set to notify you if certain purchases are made.

Never save credit card information. Many online retailers and shops now ask if you would like to save your credit card information for future use. While it may seem convenient, skip it.

Delete your cookies and auto-fill data. When you enter information on a web page, that data is stored in your web browser. After you complete a transaction, go into your browser's options, settings or history tab and delete the data.

Who Else Wants To Win A \$25 Gift Card?

The question from last month's trivia was: **To ring in the New Year in Spain, it is traditional to do what on each chime of the clock?**

a) Eat a grape b) Take a sip of wine c) Clap your hands d) Light a candle

The correct answer was a) Eat a grape. **Now, here's this month's trivia question. The winner will receive a \$25 Amazon Gift Card.**

Which country consumes the most chocolate per person at 26 lbs. or 11.9 kg per year?

a) Belgium b) Switzerland c) United States d) Germany e) Brazil

E-mail Us Right Now With Your Answer!

Stefan.Bilanych@policeITsupport.org

The Lighter Side:

Punch a Painting, Go to Jail



In 2012, Andrew Shannon punched a Monet painting valued at \$10 million. The incident occurred at the National Gallery of Ireland, located in Dublin. The painting, entitled *Argenteuil Basin with a Single Sailboat*, painted in 1874, apparently represented something much greater to the man who decided to attack it.

Right after his initial arrest, Shannon said the attack represented his way of "getting back at the state." Later on, when he appeared in court, he changed his tune. Instead of an "attack against the state," he said the whole thing was just a big misunderstanding. He said he didn't punch the painting, he "fell into it." He told the court he had felt faint and fell. The painting just happened to be in his way.

Fortunately, the National Gallery has plenty of CCTV cameras and the whole thing was recorded. What did those cameras see? Andrew Shannon very deliberately thrusting his fist through the Monet painting. In December of 2014, he was sentenced to five years in prison, and *Argenteuil Basin with a Single Sailboat* is back on display after being fully restored.