THE PILOT

"Insider Tips to Make Your Organization Run Faster, Easier and More Profitably"

No Victim Too Small – How Small Businesses Are Getting Cleaned Out By Cybercrooks

Think it would be easy to steal secret weapon plans from the Pentagon? Of course not! How easy would it be to penetrate the computers running Bank of America and deposit a lot of money into your account? Not very! These large enterprises have resources to protect their data and fight off hackers.

Now let's think about organized computer criminals breaking into your small company's computer which you also use to connect to your Facebook and Twitter pages. Social networks are one of the main methods of infecting computers with malware. Why? Only one reason, they want to take **YOUR IDENTITY AND MONEY**. These criminals want your personal information, passwords, software license activation codes, bank account numbers, Social Security numbers, contact lists, and more.

The criminals have discovered that small organizations have limited resources to protect their information and are easier to hack and defraud. The criminals also have less chance of being caught when they take small amounts from a large number of accounts than when they move large amounts of money.

Verizon's annual study of data loss for 2012 found one-half of the incidents involved small business. Symantec's annual report of cyber-attacks on small businesses found that companies with fewer than 250 employees accounted for 31% of the incidents compared to 18% from the previous year.

As cybercrime in small business grows, the Verizon study urges a return to the basics: Use good passwords, update your antivirus software, install and professionally manage a quality firewall and don't expose your essential business services to the Internet. See Page 4 and 5 for security strategies.

"As a business owner, you don't have time to spend on technical and operational issues. That's where we *shine*! Call us and put an end to your computer problems finally and forever!"

- Ed Becker, BeckITSystems, Inc.

AUGUST 2013
DULLES, VA

Inside This Issue…

A New Favorite Way Hackers Are Gaining Access To Your PC

Do you have Java turned on in your web browser? If your answer is "Yes" or "I'm not sure" then it's time to take action to find out. Why? The biggest threat to your computer systems in 2013 (and beyond) is no longer Microsoft Windows — it is now Oracle's Java.

After 20+ years as the poster child for insecure software, Microsoft's newest operating systems (Windows 7 and 8) have improved security. Cybercriminals like to get the greatest bang for their buck and therefore they're attacking the Java platform because of its huge market share and because it's an easier platform to hack than the Microsoft operating system. Java is now installed in over 1.1 billion desktops and 3 billion mobile phones. That's a big target that is very attractive to hackers. Hackers also love that Java is multi- platform, which means it's capable of corrupting computers and phones running Microsoft, Apple or Linux.

And since many Mac users should but don't have anti-virus, hackers were able to infect over 600,000 Macs with serious malware through the Java software.

Right now, cybercriminals are aware and exploiting any security flaws in Java that could lead to infections on your computer. There are even automated kits available to capitalize on any security hole found within days, if not hours of them becoming known. It's not unusual to see hackers use Java as a first attack to weaken the defenses before serving up an Operating System specific attack. Even the Department of Homeland Security suggested that "To defend against future Java vulnerabilities, their users should consider disabling Java in web browsers."

Here are 3 steps you can take today to minimize your risk:

1. Be sure your technology has a major firewall, anti-virus and malware protection installed and updated regularly.

2. If possible, use a separate web browser for Java based websites and be sure to update and patch Java regularly.

3. Have all staff report the first signs of slowness, possible infections and web browser popups to your technology administrator as soon as they happen.

Free Report Download: The Ultimate Guide To Setting Up A "Work From Home" System For Your Staff

If you are thinking about implementing a "work from home" program for your employees, or if you want to install a virtual network to allow your key employees to work seamlessly on the road or from a remote office, DON'T – until your read this eye-opening guide first!

We will mail your FREE copy today. To request it just tell us at http://www.beckitsystems.com/about-us/contact-us/ or call us at (703) 433-0730.

Shiny New Gadget Of The Month: Pebble E-Paper Watch

Pebble connects by Bluetooth to your iPhone or Android device. Setting up Pebble is as easy as downloading the Pebble app onto your phone. All software updates are wirelessly transmitted to your Pebble. **COMPATIBILITY:** iPhone 3GS, 4, 4S, 5 or any iPod Touch with iOS 5 or iOS 6. Android devices running OS 2.3 and up. Works great with Android 4.0. Unfortunately, Pebble does not work with Blackberry, Windows Phone 7, or Palm phones at this time.

Customize Your Perfect Watch. It's as easy as downloading an app. Pebble is the first watch built for the 21st century. It's infinitely customizable, with beautiful downloadable watch faces and useful internet-connected apps.

See more on the web:

http://getpebble.com

10 Ideas You Need if You Want to Succeed

1. Do what you need to do now so you will eventually get to do what you want to do later.

2. Discipline is the ability to get things done regardless of how you feel about doing them.

3. Passion only pays off when channeled into productive effort.

4. Others may believe in you, help you and support you, but ultimately nobody will do it for you. You are responsible for your own life.

5. If you don't do your job any differently from anybody else who does it, you won't get paid more than anybody else.

6. More often than not, you succeed in spite of, not because of, your circumstances.

7. If you think a little better and work a little harder you will always accomplish more than others.

8. If you can't control it; get over it.

9. If you don't appreciate where you are, you won't appreciate where you are going.

10. Get clear on what really matters to you and then get busy pursuing it.

If you want more insights into how to turn the ordinary into the extraordinary, go to Mark's site at www.marksanborn.com

Mark Sanborn, CSP, CPAE, is president of Sanborn & Associates, Inc., an idea studio dedicated to developing leaders in business and in life. Mark is an international bestselling author and noted authority on leadership, team building, customer service and change. Mark is the author of eight books, including the bestseller *The Fred Factor: How Passion In Your Work and Life Can Turn the Ordinary Into the Extraordinary* which has sold more than 1.6 million copies internationally. Learn more about Mark at www.marksanborn.com

Protect Your Small Business from Cybercrime

How secure are your digital assets from fraud, identity theft and cybercrime? Studies have found that small businesses have a higher fraud rate than larger companies. One of the most frequent sources of fraud is credit card abuse – largely due to the fact that few business owners take time to review every charge on the bill. Cybercrime also results from a lack of proper security including inadequate network and computer security and the failure to perform background checks when hiring employees. Try these strategies:

Protect Your Credit Cards and Bank Accounts: First be sure to separate personal banking and credit cards from the business accounts. At the very least, crooks will not get all of your money in a single act. Separating your accounts makes it easier to report business expenses and deductions on tax returns. Check bank accounts every day for suspicious activity.

Credit Cards: Use credit cards cautiously. Switch to online bill pay or make sure you store paper bills securely. Use a secure mailbox for receiving and sending bills. If there is not a secure mail box, drop the mail directly at the post office. Follow this practice for any mail that contains sensitive information. Leaving sensitive mail in an unsecured mailbox is a recipe for disaster.

Continued on page 5 --

Who Else Wants To Win A $25 Gift Card?

The Grand Prize Winner of last month's Trivia Challenge Quiz is Emma Olsen of Long and Foster. She was the first person to correctly answer my quiz question from last month: **The Pagans used the term ____???____ for the first full moon in June because they drank fermented honey as part of summer wedding celebrations.**

The correct answer was b) Honeymoon. **Now, here's this month's trivia question. The winner will receive a gift card to Starbucks.**

Which musician died in August of 1977, leaving behind a huge following of fans who still adore him to this day?
a) Jerry Garcia b) Jim Morrison c) John Lennon d) Elvis Presley

Call us right now with your answer!
703-433-0730

The Lighter Side:

Did You Know?

- A can of Diet Coke will float to the top of water, but a regular Coke will sink to the bottom. (Try it.)
- The fourth richest man in the world (Warren Buffett) still lives in the house he bought for $31,500 in 1958.
- The Munich Technical University has a 3-story slide used for students to get to class faster. (See photo above.)
- The "I'm Feeling Lucky" button costs Google $110 million each year.
- There are already more than 250 cryopreserved (frozen people) in the hope that someday technology will be invented to revive them and extend their lives.
- Peanut butter, under high (very, very high) pressure has the probability to turn into a diamond.

Secure the Network: Every network needs to be protected by a firewall. This includes field offices and home offices that connect to the corporate computers. Every computer needs to have anti-virus, malware and spyware detection software installed and updated frequently. Creating backup copies of the data and storing it in a secure center over 500 miles from your location will make it a lot easier for you to continue working in the event of a cyber-attack.

Use a Dedicated Computer for Banking: Use a dedicated computer for all your online financial transactions and restrict it from use in other online activity such as social media, email, and web-surfing which can open up the machine to vulnerabilities. Avoid mobile banking. This may seem to be overly cautions, until your systems are hacked and your bank accounts are compromised

Have a Password Policy: Another easy step you can take to protect your technology and systems is to institute a password policy that includes the following:

- Make sure passwords change regularly - every 60 to 90 days.
- Require complex passwords that contain one upper case letter, one number and must be a minimum of eight characters in length. Phrases are good, too!
- Use different passwords for different online and system accounts.

Educate Everyone: Employees are the greatest vulnerability when it comes to fraud, but they are also your first line of defense. Hold regular training sessions on recognizing and responding to security threats as well as prevention measures. This applies to new hires and seasoned staff. Enforce the training by instituting policies that guide employees on the proper use and handling of confidential company information, including financial data, personnel, and customer information. Randomly reward those who follow the guidelines. A little appreciation goes a long way in gaining compliance!

Perform Employee Background Checks Before and After Hiring: One of the first steps to preventing fraudulent employee behavior is to make the right hiring decisions. Pre-employment background checks are a good business practice for any employer, especially for those employees who will be handling cash, high-value merchandise, or have access to sensitive customer or financial data.

Consider drug tests, past employer verification, criminal background, and driving records especially if the job requires driving on the public highways. If your employees work with children or in other care positions, it may also be required to check the sex offender registry.

Stay within the Law by Working with a Screening Firm Many private screening firms will offer complete background checks while helping you stay compliant with the law.

Do Your Own Research There are background checks that you can do yourself and are important.

Verify what's on the Resume – Call colleges and universities to verify the degree earned and ask previous employers to confirm the applicant's work history.

Use the Web – Search for the applicant's Facebook, LinkedIn, and other social media sources as well as a Google search.

Insure Your Business: Fraud and cybercrime happens. Cover the damages by purchasing an insurance policy that protects against losses that may occur from crime or fraud. Likewise, find out what your bank is willing to do to help you out if your credit card or business account is compromised. See the insurance checklist in the April newsletter.

Don't wait until it is too late!