September 2015

TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

Cybercriminals Now Have A Bull's-Eye On Small Business… Is Your Company's Data At Risk?

In a December 2014 survey by the National Small Business Association, 61% of small businesses reported being victims of a cybercrime within the past 12 months.

The average cost to recover from a cyber-attack skyrocketed from $8,699 per attack in 2013 to $20,752 per attack in 2014. And, of the businesses targeted, 68% said they'd been hacked more than once.

Experts agree, as cybercrooks become ever more sophisticated, the threat to small businesses is going to get worse before it gets better…

So what can you do to beat the bad guys?

Here are three common ploys used by hackers – and how you can fend them off:

Phishing – A really legitimate-looking e-mail urges you to click a link or open a file that triggers a malware installation on your computer.

> **Best Defense:** Don't let anyone in your company open files or click links in an e-mail unless they're certain who it came from.

Cracking Your Password – Hackers can run programs 24/7 testing password combinations. The easier your password is to guess, the more likely it is they'll crack it.

> **Best Defense:** Consider using a password manager that generates and stores tough-to-crack passwords. For extra security, use unique passphrases for financial accounts in case the manager gets hacked.

Drive-By Download – You visit what appears to be an innocent site; yet when you click, your device gets hacked – and you may never know it, until it's too late.

> **Best Defense:** Make sure your browser is up-to-date, or use one that updates automatically, such as Firefox or Chrome. Internet Explorer users have been found to be most vulnerable to these attacks.

Unfortunately, these three examples are just a small sampling of the dozens of ever more ingenious ways cybercriminals are breaking down the doors and destroying unprepared businesses.

Let us help! Through September 30, call our office and receive a FREE 15-Point Cyber-Security Audit to uncover gaps in your company's online security.

Our highly trained team of IT pros will come to your office and conduct this comprehensive audit. We'll then prepare a customized "Report Of Findings" that reveals specific vulnerabilities and a Prioritized Plan Of Attack for getting any problems addressed fast.

To take advantage of this limited-time offer, just call our office at 701-364-2718.

"Enabling People to Provide Great Products and Services - Anytime, Anyplace, Anywhere"

- Rick Johnston, Information Management Systems

September 2015

Fargo, ND

Inside This Issue…

©Jeff Stahler/Distributed by Universal Uclick for UFS via CartoonStock.com

Why Managed Services Boost Productivity

For many small and medium sized business owners like yourself, Managed Services may be a confusing topic. You've likely heard that they can lead to greater productivity and profits, but are unsure as to just how they do this. If you've been confused for long enough, today you'll finally understand the process by which Managed Services can lead your business to increased productivity and a higher bottom line.

Managed Services essentially amounts to preventative IT maintenance. What this means for your business is that little IT problems are nipped in the bud as soon as they bubble up, and before they have a chance to compound into much bigger, more costly ones. But before we dive deeper into how this increases your business's productivity levels, it makes sense to look at the history of this service and the role of "preventative maintenance" in our culture.

Why preventative maintenance matters

Managed Services have been around for decades. But despite this, many businesses have been slow to catch on. And really, is it all that surprising? Preventative maintenance is not exactly a priority in mass culture. Whether you hire a mechanic to replace a catalytic converter, a plumber to repair a leaky pipe or doctor to correct your coronary heart disease, many of these oftentimes preventable problems have been culturally accepted as commonplace. Yet people are so used to the mindset of thinking "everything is okay until it's not", which is really where the true problem lies.

Additionally, when preventable problems are ignored long enough to the point they explode into emergency repairs, your wallet almost always suffers. This is just as true for a network crash to your business's IT infrastructure as it is for a trip to the emergency room for a neglected health problem.

Because Managed Services prevent catastrophic IT repairs that surprise you out of nowhere, your bottom line will enjoy long-term savings. Along with this, you'll also get a significant bump in your productivity levels.

How does Managed Services boost productivity?

To answer this question, it makes sense to look at a fundamental principle of productivity – focus. Imagine if you're trying to complete a new marketing strategy for the next quarter. You're doing some research, compiling a list upcoming networking events and trade shows to attend, when suddenly you're disrupted by an urgent phone call. After you're off the phone, you return to your research, and then your secretary bursts in with an handful of vendor invoices you need to sign off on. As these disruptions continue to pile up, what happens if your IT breaks down and you're unable to use your computer? Basically, you don't get anything done during the day. You become stuck.

When it comes to IT, Managed Services take preventative measures to ensure your IT is always running at its optimal level, so that you don't suffer technology breakdowns or distractions that blow your focus – preventing you and your staff from getting any work done. Smooth running IT won't resolve all your productivity problems, such as your staff focusing more on Facebook or their phone rather than their work, but it will resolve all of those that relate directly to technology. No longer will your business be held down by daily computer disruptions and associated repairs, and instead you and your staff can move forward and focus on growing your business. That is the beauty of Managed Services. More productivity, focus and growth for your entire organization.

Have more questions about Managed Services? Give us a call today. We're happy to provide you the information you need.

This entry was posted in General Articles C, Productivity—General and Tips and tagged 2015Jul30_Productivity_C, Emergency, IT, Managed Services, Preventative Maintenance, Productivity, QS_3, Technology http://www.techadvisory.org/2015/07/why-managed-services-boost-productivity/

Shiny New Gadget Of The Month:

Nest Cam: Keeping An Eye On Things While You're Away

Have you ever worried about what's happening at home when you're away? The Nest Cam can keep you informed. This wide-angle camera streams sound and video to your smartphone. It will even warn you about any unusual activity.

If the Nest Cam detects sudden movement or loud noises, it instantly alerts you by phone. The video feed lets you see what's happening and even scold kids, pets or burglars through a speaker.

This product integrates with other Nest equipment. For example, smart smoke alarms can activate the Nest Cam. It also saves alerts and footage in a convenient archive. The camera even makes it easy to share fun video clips online.

If you already have WiFi, setup is a breeze. This gadget comes with a stand that lets you put it on any flat surface. It also sticks to metal objects or screws onto a regular camera tripod.

Do You Accept Credit Cards? Watch Out For These 5 Pitfalls That Could Lead To Lawsuits

If your company is not fully compliant with Payment Card Industry (PCI) Security Standards, you could be at risk of a serious tangle with attorneys. Technically, PCI guidelines are not a hard-and-fast set of laws. However, merchants can still face hefty liabilities for not meeting them. Avoid these mistakes to keep your company out of hot water with attorneys:

1. Storing Cardholder Data In Noncompliant Programs

Many states have laws regarding data breaches and, depending on where you accept cards, you may be subject to many of them. For example, Massachusetts has 201 CMR 17.00, which requires companies keeping any personal data from Massachusetts residents to prepare a PCI-compliant plan to protect that data. If a company then fails to maintain that plan, the business may face state prosecution.

2. Fibbing On The Self-Assessment Questionnaire

If you have considered tampering with the reports from your company's Approved Scanning Vendor, think again. Time invested now to fix any holes in your data security system could save you big-time from the penalties your company could suffer if there's ever a data breach.

The same thing applies to simply "fudging the truth" on self-prepared compliance reports. Even if you think it's a harmless stretch of the truth, don't do it.

3. Not Using The Right Qualified Security Assessor

Many companies use Qualified Security Assessors to help them maintain their PCI compliance. Every QSA does not necessarily know as much as another, however. It's important to select someone who both understands your business and stays up-to-date on the latest version of PCI Security Standards.

4. Trying To Resolve Data Compromises Under The Radar

You may be tempted to fix a customer's complaint yourself if they inform you of a data compromise. Not informing credit card companies of data breaches, however small, can lead to you no longer having access to their services. Those credit card companies can then file suit against your company, costing you big bucks in the end.

5. Not Checking ID For Point-Of-Sale Credit Card Use

Sometimes it seems like no one checks IDs against the credit cards being used, so merchants tend to be lax about doing so. Unfortunately, running just one unauthorized credit card could cost you a lot in the long run. Even if the state in which you do business does not have specific laws regarding PCI compliance, a civil suit may come against your company for any data breaches. The court will not favor you if you have not been PCI-compliant.

All in all, it pays to pay attention to PCI compliance – a little time invested today could save you big-time tomorrow.

4 Different Types of Malware: Explained

Over the decades of the internet's existence, cyber threats have evolved at a rapid pace. When once there were only viruses and malware to watch out for, now you have to protect your business from worms, trojans, ransomware and dozens of other online threats. But what's the difference between all of them? Let's take a look. Here are today's most common cyber threats and the tips you need to protect your business from them.

Malware

Malware is the short version of the word malicious software. And this is a general term that encompasses many types of online threats including spyware, viruses, worms, trojans, adware, ransomware and more. Though you likely already know this, the purpose of malware is to specifically infect and harm your computer and potentially steal your information.

But how do the different types of malware differ from one another? How can you protect your business from them? Let's take a look at four of the most common forms of malware below.

Virus – like a virus that can infect a person, a computer virus is a contagious piece of code that infects software and then spreads from file to file on a system. When infected software or files are shared between computers, the virus then spreads to the new host.

The best way to protect yourself from viruses is with a reliable antivirus program that is kept updated. Additionally, you should be wary of any executable files you receive because viruses often come packaged in this form. For example, if you're sent a video file, be aware that if the name includes an "exe" extension like .mov.exe, you're almost certainly dealing with a virus.

Spyware – just like a spy, a hacker uses spyware to track your internet activities and steal your information without you being aware of it. What kind of information is likely to be stolen by Spyware? Credit card numbers and passwords are two common targets.

And if stealing your information isn't bad enough, Spyware is also known to cause PC slowdown, especially when there is more than one program running on your system – which is usually the case with a system that's infected.

Worms – similar to viruses, worms also replicate themselves and spread when they infect a computer. The difference, however, between a worm and a virus is that a worm doesn't require the help of a human or host program to spread. Instead, they self-replicate and spread across networks without the guidance of a hacker or a file/program to latch onto.

In addition to a reliable antivirus software, to prevent worms from infecting your system you should ensure your firewall is activated and working properly.

Trojan – like the trojan horse from ancient greek mythology, this type of malware is disguised as a safe program designed to fool users, so that they unwittingly install it on their own system, and later are sabotaged by it. Generally, the hacker uses a trojan to steal both financial and personal information. It can do this by creating a "backdoor" to your computer that allows the hacker to remotely control it.

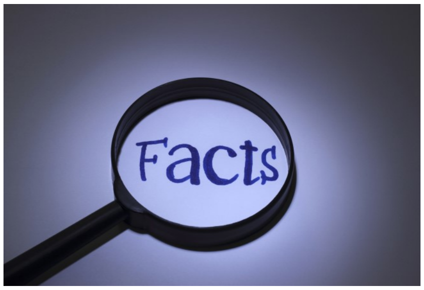
Similar to the other malware mentioned above, antivirus software is a dependable way to protect yourself against trojans. For further safety, it's wise to not open up suspicious attachments, and also ensure that your staff members aren't downloading any programs or applications illegally at the office – as this is a favorite place hackers like to hide trojans.

Curious to learn about other common malware that can cause trouble for business owners? Want to upgrade your existing network security system? Give us a call today at 701-364-2718, we're sure we can help.

This Entry was posted in General Articles A, Security—News and General| Tagged 2015 Jul22_Security_A, Antivirus, Firewall, Malware, QS_3, Ransomware, Software, Spyware, Trojan, Virus Worm— http://www.techadvisory.org/2015/07/4-different-types-of-malware-explained/

The Lighter Side:

IT Fun Facts



Technology has forever changed our lives and our world more than you know. Here are some numbers to put that fact into perspective:

1. About 4 billion people worldwide own a mobile phone, but only 3.5 billion people own a toothbrush.

2. Computers and other electronics account for 220,000 tons of annual trash in the U.S. alone.

3. About 300 hours of video are uploaded to YouTube every minute.

4. Around 100 billion e-mails traverse the Internet every day, and about 95% of those messages go straight to spam folders.

5. The annual amount of electricity it takes for Google to handle a billion search queries every day is around 15 billion kWh, which is more than most countries consume.

6. About 500 new mobile games appear on the Apple App Store each day.

7. The "father of information theory," Claude Shannon, invented the digital circuit at age 21 while he was in college.

8. Regular computer users blink only half as often as non-users.

9. Over 1 million children can say their parents met on Match.com