7 Urgent Security Protections Every Business Should Have In Place Now

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are "low hanging fruit." Don't be their next victim! This report will get you started in protecting everything you've worked so hard to build.

Provided By: YourIT, INC
Author: Chris Moroz
3030 NW Expressway
Suite 200 #371
Oklahoma City, OK 73112
www.YourITok.com
405-367-9090

YOUR I.T.
Simple and secure technology solutions.

Are You A Sitting Duck?

You, the CEO of a small business, are under attack. Right now, extremely dangerous and well-funded cybercrime rings in China, Russia and the Ukraine are using sophisticated software systems to hack into thousands of small businesses like yours to steal credit cards, client information, and swindle money directly out of your bank account. Some are even being funded by their own government to attack American businesses.

Don't think you're in danger because you're "small" and not a big target like a J.P. Morgan or Home Depot? Think again. 82,000 NEW malware threats are being released every single day and HALF of the cyber-attacks occurring are aimed at small businesses; you just don't hear about it because it's kept quiet for fear of attracting bad PR, lawsuits, data-breach fines and out of sheer embarrassment.

In fact, the National Cyber Security Alliance reports that one in five small businesses have been victims of cybercrime in the last year – and that number is growing rapidly as more businesses utilize cloud computing, mobile devices and store more information online. You can't turn on the TV or read a newspaper without learning about the latest online data breach, and government fines and regulatory agencies are growing in number and severity. **Because of all of this, it's critical that you have these 7 security measures in place.**

1. **Train Employees On Security Best Practices.**
   The #1 vulnerability for business networks are the employees using them. It's extremely common for an employee to infect an entire network by opening and clicking a phishing e-mail (that's an e-mail cleverly designed to look like a legitimate e-mail from a web site or vendor you trust). If they don't know how to spot infected e-mails or online scams, they could compromise your entire network.

2. **Create An Acceptable Use Policy (AUP) – And Enforce It!**
   An AUP outlines how employees are permitted to use company-owned PCs, devices, software, Internet access and e-mail. We strongly recommend putting a policy in place that limits the web sites employees can access with work devices and Internet connectivity. Further, you have to enforce your policy with content-filtering software and firewalls that will regulate what web sites your employees access and what they do online during company hours and with company-owned devices, giving certain users more "freedom" than others.

Having this type of policy is particularly important if your employees are using their own personal devices to access company e-mail and data. If that employee is checking unregulated, personal e-mail on their own laptop and infects that laptop, it can be a gateway for a hacker to enter YOUR network. If that employee leaves, are you allowed to erase company data from their phone? If their phone is lost or stolen, are you permitted to remotely wipe the device – which would delete all of that employee's photos, videos, texts, etc. – to ensure YOUR clients' information isn't compromised?

3. **Require STRONG passwords and passcodes to lock mobile devices.**
   A strong computer password can go a long way toward preventing unauthorized access to sensitive business information. This simple step prevents quick and easy physical access to files. Passwords should be at least 8 characters and contain lowercase and uppercase letters, symbols and at least one number. On a cell phone, requiring a passcode to be entered will go a long way toward preventing a stolen device from being compromised. Again, this can be ENFORCED by your network administrator so employees don't get lazy and choose easy-to-guess passwords, putting your organization at risk.

4. **Keep Your Network Up-To-Date.**
   New vulnerabilities are frequently found in common software programs you are using, such as Microsoft Office; therefore it's critical you patch and update your systems frequently. Starting with Windows XP Service Pack 3, Microsoft has downloaded critical updates in the background while a computer is connected to the Internet in an attempt to provide users uninterrupted security patches. Surprisingly, users routinely turn this feature off or ignore the prompts to install the updates, allowing their computers to remain unprotected and vulnerable. If you're under a managed IT plan, this can all be automated for you so you don't have to worry about missing an important update.

5. **Have An Excellent Backup.**
   This can foil the most aggressive (and new) ransomware attacks, where a hacker locks up your files and holds them ransom until you pay a fee. If your files are backed up, you don't have to pay a crook to get them back. A good backup will also protect you against an employee accidentally (or intentionally!) deleting or overwriting files, natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters. Again, your backups should be AUTOMATED and monitored; the worst time to test your backup is when you desperately need it!

6. **Upgrade Your Email Service.**
   Email is still one of the most vulnerable pathways into a business. Phishing Attacks. SPAM. Disorganized Inboxes. Infected attachments. And the list goes on, and on… Many businesses still rely on the email service provided for free from their ISP, believing that email service is email service regardless of who's delivering it. But the fact is that upgrading to a true business email service from companies such as Microsoft (Office 365) and Google (Google Apps) not only give far greater protection, but also significant increases in email storage capacities and better synchronization across multiple devices, just to name a few benefits.

7. **Don't Scrimp On A Good Firewall.**
   Residential consumer routers from companies such as Linksys, D-Link, Netgear, and Belkin have made big leaps in features and now routinely include basic firewalls, separate guest networks, and some level of content filtering. But even with all these improvements they're still geared towards consumers and lack the necessary features and reliability to keep business safe and secure. A firewall acts as the frontline defense against hackers blocking everything you haven't specifically allowed to enter (or leave) your computer network. But all firewalls need monitoring and maintenance, just like all devices on your network. This too should be done by your IT person or company as part of their regular, routine maintenance.

YOUR I.T.
Simple and secure technology solutions.

Want Help In Implementing These 7 Essentials?

If you are concerned about employees and the dangers of cybercriminals gaining access to your network, then call us about how we can implement a managed security plan for your business.

As an existing customer **NOT** currently taking advantage of one of our managed and monitored services, we're offering to conduct a free **Security And Backup Audit** of your company's overall network health to review and validate as many as **5** different data-loss and security loopholes. We'll also look for common places where security and backup get overlooked, such as mobile devices, laptops, tablets and home PCs. At the end of this free audit, you'll know:

- Is your network really and truly secured against the most devious cybercriminals? And if not, what do you need to do (at a minimum) to protect yourself now?
- Is your data backup TRULY backing up ALL the important files and data you would never want to lose? We'll also reveal exactly how long it would take to restore your files (most people are shocked to learn it will take much longer than they anticipated).
- Are your employees freely using the Internet to access gambling sites and porn, to look for other jobs and waste time shopping, or to check personal e-mail and social media sites? You know some of this is going on right now, but do you know to what extent?
- Are you accidentally violating any PCI, HIPAA or other data-privacy laws? New laws are being put in place frequently and it's easy to violate one without even being aware; however, you'd still have to suffer the bad PR and fines.
- Is your firewall and antivirus configured properly and up-to-date?
- Are your employees storing confidential and important information on unprotected cloud apps like Dropbox that are OUTSIDE of your backup?

I know it's natural to want to think, "We've got it covered." **Yet I can practically guarantee my team will find one or more ways your business is at serious risk for hacker attacks, data loss and extended downtime – I just see it all too often in the numerous businesses we've audited over the years.**

You Are Under No Obligation To Do Or Buy Anything

I also want to be very clear that there are no expectations on our part for you to do or buy anything when you take us up on our **Free Security And Backup Audit**. As a matter of fact, I will give you my personal guarantee that you won't have to deal with a pushy, arrogant salesperson because I don't appreciate heavy sales pressure any more than you do.

You've spent a lifetime working hard to get where you are. You earned every penny and every client. Why risk losing it all? Get the facts and be certain your business, your reputation and your data are protected. Call us at 405-367-9090 or you can e-mail me personally at chris@youritok.com

Dedicated to serving you,

Chris Moroz
Web: www.YourITok.com
E-mail: chris@youritok.com
Office: 405-367-9090
Direct: 405-698-3944

YOUR I.T.
Simple and secure technology solutions.

Here's What A Few Of Our Clients Have Said:

"You've freed us from the worry of computer security so we can focus on our business"

We are so thankful for your immediate availability when we have questions or problems. Because Your|I.T. focuses on small business, we can trust Chris to stay up- to- date with the security challenges that we face. **We are confident that we are safer now more than ever before**. We don't feel the pressure to learn the ins and outs of our computers, hardware, and security, because we know Your|I.T. is managing it.

-Kathy Burns, Insight Books

"Support and Advice on the Latest Tech"

YourIT employs top notch techs and provides top level service. Without their help, my business would have a more difficult time keeping up with the shifting technology landscape. **They are trustworthy, affordable, and, most importantly, extremely competent**. Don't hesitate to use YourIT.

- *Brandon Lehman, Directors Inc.*

"Trusted Partner Who's There When Needed"

We have been very pleased and impressed with YourIT. In this day and age it is important for me to have a resource to go to for assistance with my computers. **YourIT keeps our systems running perfectly**.

-Mark Muse Allstate Insurance