

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: Intelligent IT Designs
Author: Paul Villanueva
27 Stephenson Blvd., New Rochelle, NY 10801
www.IntelligentITDesigns.com

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. We can easily set up permissions and rules 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 that 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?

Further, if the data in your organization is highly sensitive, such as patient records, credit card information, financial information and the like, you may not be legally permitted to allow employees to access it on devices that are not secured; but that doesn’t mean an employee might not innocently “take work home.” If it’s a company-owned device, you need to detail what an employee can or cannot do with that device, including “rooting” or “jailbreaking” the device to circumvent security mechanisms you put in place.

3. **Require STRONG passwords and passcodes to lock mobile devices.** 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. 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 to work!

6. **Don't allow employees to download unauthorized software or files.** One of the fastest ways cybercriminals access networks is by duping unsuspecting users to willfully download malicious software by embedding it within downloadable files, games or other “innocent”-looking apps. This can largely be prevented with a good firewall and employee training and monitoring.
7. **Don't Scrimp On A Good Firewall.** 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.

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.

At no cost or obligation, we'll send one of our security consultants and a senior, certified technician to your office to conduct a free **Security And Backup Audit** of your company's overall network health to review and validate different data-loss and security loopholes, including small-print weasel clauses used by all 3rd-party cloud vendors, giving them zero responsibility or liability for backing up and securing your data. 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 many of the businesses we've audited over the years.**

Even if you have a trusted IT person or company who put your current network in place, it never hurts to get a 3rd party to validate nothing was overlooked. I have no one to protect and no reason to conceal or gloss over anything we find. If you want the straight truth, I'll report it to you.

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.

Whether or not we're a right fit for you remains to be seen. If we are, we'll welcome the opportunity. But if not, we're still more than happy to give this free service to you.

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 877-914-3577 or you can e-mail me personally.

Dedicated to serving you,

Paul Villanueva

Web: www.IntelligentITDesigns.com

E-mail: Paul@IntelligentIT.net

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



Intelligent I.T. Designs Keeps Our Company's Data Safe, Secure and Running Smoothly!

We were having a critical issue with our server and VoIP phones. We called Intelligent IT Designs and within the hour they were at our office troubleshooting, fixing and helping our company to quickly get up and running again. Once the emergency issue with our server and phones was resolved, Intelligent IT evaluated the hardware and software being used in our company. They made some great suggestions that will help our keep company's technology and data safe, secure and running smoothly. Paul's IT knowledge and experience is exactly what our company was looking for and needed.

Jeannie Colangelo, Finance Manager/IT Coordinator

The School Choice Group

Intelligent I.T. Designs Resolves Issues Before They Impact Us!



We rely on our computer system to operate our business. If our computers aren't up, we can't operate, and if they are down for a significant period of time, we incur significant reputational exposures. In our situation it was a no brainer. We need to be on top of and in front of everything that impacts our computer systems and Internet connections. Unfortunately, we don't have in-house computer expertise. We rely on Intelligent IT Designs. Their continuous monitoring of our system and identification of problems, often before we know about them, are what we depend on. They resolve issues before they impact us, and the few times there have been problems that have affected our computers, Intelligent IT Designs has been right on it, getting us up and running quickly.

Stephen Markowitz, President and CEO

Ruby & Jack's Doggy Shack



Paul And His Team Are Like A Part Of Our Staff, We Can Sleep At Night While They Monitor Our I.T. System!

Prior to enlisting the services of Paul V. and his IT team, we were with a company that in retrospect was reacting to whatever problems arose, rather than anticipating. This led to a reactive, band-aid approach to IT solutions, rather than a systemic, proactive approach. And in reality, rather than a steady reliable cost of doing business, the pricing structure was scattershot, unpredictable and at times even alarming. When it comes to pricing, my attitude about it is, what salary would I pay an in-house IT support person? And when I look at it that way I'm satisfied because the reality is that 24/7 Paul and his team are available to us, working for us and supporting us. So really, they are like a part of our staff. Paul V. and his team are low-key, high-caliber IT professionals. If and when there is a problem, they always provide reassuring, competent assistance. If you like to sleep at night, take this concern off your mind and hand it over to Paul and his team who will monitor your IT system on a regulated schedule. Because of their genuine thoughtfulness, trustworthiness and sincere interest in getting things right and making things run right, I can relax and leave the driving to them, so I can run my business.

Nicole Pasternak, Office Operations
GNF Marketing

I Have Confidence In Your Company. You Provided Superior Support During The Restoration Of The Fire Salvaging Our Servers and PCs!



ARDSLEY COUNTRY CLUB

As you know, your services have been invaluable to me, especially this past year since the fire. We have relied on your services since 2013 and you were with us the day after the fire salvaging the server and computers so we could keep our administrative operations running without interruption. Since then your guidance has been very helpful and your technicians have provided superior support for all of the changes we have had over the past year to continue our operations during the restoration. I have confidence in your company. Jobs are quickly completed and done correctly the first time. I appreciate that you have accommodated many of my cost cutting solutions, purchasing my own computers and repurposing older computers and reusing older equipment in less critical situations. However, as you know our network is critical for our operations and you have helped me develop a fast, reliable and secure network that my company relies on without worry. Your monthly maintenance keeping each workstation, the servers, and the firewall and our software up to date and monitoring back-ups is efficient and I feel I am doing all I can to mitigate the threat of a data breach or other failure.

Spencer A. Koja, Controller
The Ardsley Country Club

Paul Villanueva is an efficient, experienced and knowledgeable IT professional. He is a pleasure to work with and actually answers his phone or responds within the hour to messages. He set up our new office network, firewall, server and VoIP as well as suggesting future upgrades and additions to make our infrastructure even more powerful and conducive to our workflow. Intelligent IT Designs will be an asset to any company needing IT consultation, setup and maintenance.

Kim Holbrook, Director of Post Production
Kaleidoscope Productions

We hired Intelligent IT Designs to design, buy and set up our office computer system for 10 users. They did an excellent job. They helped us identify what our needs were, designed an efficient system that could easily grow with our offices, purchased all hardware for us at excellent prices and installed and set up our whole system. They were very easy to work with, customized our system to work seamlessly in the office or while travelling and provided support to “fine tune” and answer our many questions. I would strongly recommend them.

Eric Scheffler, Principal
Glacier Global Partners

Paul Villanueva is a real pro. We had a real dilemma with our web site software and hosting. Paul proved to be knowledgeable, he knew how to attack the problem and he delivered positive results on time. I would recommend Paul without hesitation.

Chuck Barredo, Sales Manager
East Coast Abstract

Paul shows up on time, does what he promises and fixes all of our problems. He is available with short notice and we are very happy with his service. We recommend him without qualification.

Chase Welles, Partner
SCG Retail

My firm has been using Paul and his company for 3 years. Both he and his associates are personable, knowledgeable, timely, and persistent. Whenever we have an issue with our computers, we never have the additional stress caused by an IT person who doesn't answer a call or come to the office in a timely manner to fix the problem. This is an important quality for my firm, and Paul has been great since we first hired him

Robin A. Bikkal, Owner
Bikkal & Associates, PC