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!

WINDSTAR
Technologies Inc.

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 and Russia 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. 560,000 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 a victim 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 news article 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 is 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.

To Request Your FREE Security And Backup Analysis, please visit www.windstartech.com/sittingduck or call our office at 540-317-1200.

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 the 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.

To Request Your FREE Security And Backup Analysis, please visit www.windstartech.com/sittingduck or call our office at 540-317-1200.

4 Keep Your Network Up-To-Date

New vulnerabilities are frequently found in common software programs you are using, such as Microsoft 365; 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 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.

To Request Your FREE Security And Backup Analysis, please visit www.windstartech.com/sittingduck or call our office at 540-317-1200.

Want Help 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 Analysis** of your company's overall network health to review and validate as many as 10 different data-loss and security loopholes, including small-print weasel clauses used by all third-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 Analysis, you'll have these questions answered:

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?

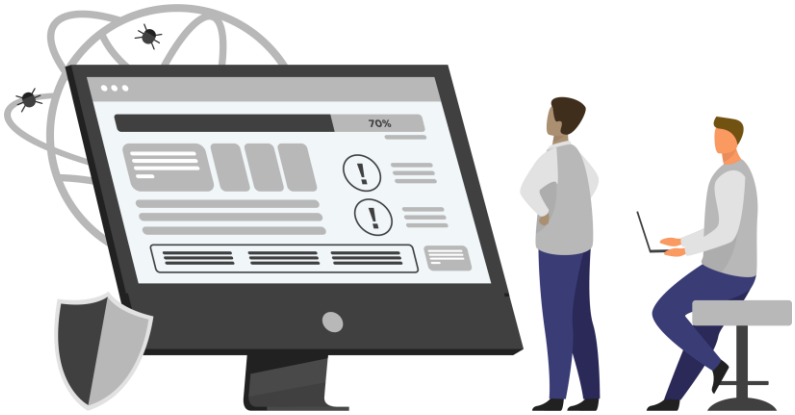
To Request Your FREE Security And Backup Analysis, please visit www.windstartech.com/sittingduck or call our office at 540-317-1200.

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 many businesses we've Analysised 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 third 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 Analysis**. 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 540-317-1200 or you can e-mail me personally at David.Groot@WindStarTech.com.

Together, We Make 'IT' Secure,

David Groot, President
Web: www.windstartech.com
E-mail: David.Groot@WindStarTech.com
Phone: 540-317-1200

To Request Your FREE Security And Backup Analysis, please visit www.windstartech.com/sittingduck or call our office at 540-317-1200.

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

Operations On Schedule

Early morning or late evening, Windstar's fast responsive service is personalized to our needs. Unlike our last provider who put us on a waiting list, Windstar Technologies constantly puts customer service first. Our biggest benefit to having Windstar enhanced security plan is having a partner who helps us navigate and achieve HITECH/HIPAA compliance. We never have a worry about our technology and security with the Windstar team working on our side.

– Yolanda Kay, Executive Director, Culpeper Surgery Center

Increased Productivity

Windstar continues to be an invaluable guide to the ASWB organization. Moving our SQL Server to Azure has created a centralized management system with better access and improving backups. This allows us access to SQL from multiple locations allowing ASWB to be more productive. Windstar has been critical in helping manage the Azure environment especially with updates, upgrades, security, and disaster recovery.

–Dan Sheehan, IT Director, Association of Social Work Boards

Lower Costs, Increase Knowledge, and Stay Connected

Communication and high-quality customer service sets Windstar Technologies apart from other IT firms I have worked with in the past. Switching to Microsoft 365 Cloud and Voice helps the Culpeper Chamber of Commerce work remotely and allows us to integrate digital and virtual aspects into our Networking Programs all while Lowering Costs. The Culpeper Chamber uses Microsoft Teams for Town Halls, Meetings, and even Surveys to bring our Membership together during this Pandemic. Working with Windstar means we stay abreast of updates and new platforms we can use to communicate with our community better.

–Jeff Say, President, Culpeper Chamber of Commerce

On Cloud 9

Our Organization struggled with outdated software (Windows 7), file sharing with remote staff, file storage and connectivity issues. Windstar Technologies helped our business integrate the latest technologies in our daily operations by migrating to Microsoft 365. The Windstar Team provided prompt response to our concerns with ongoing communication throughout the project. Moving to Microsoft 365 has allowed remote staff to decrease connection issues for file sharing, standardized our software for all staff members, increased security measures, and resolved file storage issues. We recommend Windstar Technologies to other businesses.

– Lisa Fettig, Executive Vice President, Emergency Management Services Internal, Inc.

To Request Your FREE Security And Backup Analysis, please visit www.windstartech.com/sittingduck or call our office at 540-317-1200.

To Request Your FREE Security And Backup Analysis:

1. **online to www.windstartech.com/sittingduck/**
2. **Call us direct at 540-317-1200.**
3. **E-mail your appointment request to David Groot at David.Groot@WindStarTech.com**

WINDSTAR
Technologies Inc.