7 Urgent Security Protections Every Business Should Have In Place Now!

CNS
Your Partner in Technology

(916) 366-6566 | callcns.com

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."

As the CEO of a small business, you are increasingly vulnerable to cyberattacks. Well-funded and highly organized cybercrime groups, often operating out of nations like China and Russia, are deploying advanced software to target thousands of businesses just like yours. These attacks aim to steal sensitive information, including credit card data, customer details, and even siphon funds directly from your bank accounts. Alarmingly, some of these groups receive backing from their governments, specifically to target U.S. businesses.

Think your small business is safe because you're not a Fortune 500 company like J.P. Morgan or Home Depot? Think again. Every day, 560,000 new malware threats are unleashed, and nearly half of all cyberattacks target small businesses. These incidents often go unreported, not due to their insignificance, but because of the fear of negative publicity, potential lawsuits, costly data breach fines, and the embarrassment that comes with being a victim.

Recent data from the National Cyber Security Alliance reveals that 20% of small businesses have fallen victim to cybercrime in the past year—a figure that is rapidly increasing as more companies adopt cloud computing, mobile technologies, and store critical information online. The news is replete with reports of the latest data breaches, and regulatory bodies are responding with more stringent fines and compliance requirements.

Because Of All Of This, It's Critical That You Have These 7 Security Measures In Place.

1 Train Employees on Phishing Emails.

The greatest vulnerability in business networks is often the employees who use them. It's alarmingly common for an entire network to be compromised when an employee inadvertently clicks on a phishing email. These emails are increasingly sophisticated, designed to mimic legitimate communications from trusted websites or vendors. If your team isn't trained to identify these threats, they could unknowingly put your entire organization at risk.

Implementing a comprehensive phishing training solution is far more effective than merely forwarding detected phishing emails as a warning. Security Awareness Training and Phishing Simulation programs significantly reduce the likelihood of employees falling victim to phishing attempts. As employees become more aware of the risks, they are less likely to click on dangerous links, divulge sensitive information, or engage in actions that could compromise your organization's security.

Training Videos: Access a library of concise, targeted videos that educate employees on how to identify actual phishing scams. These can be integrated into onboarding for new hires and used in annual training sessions to ensure ongoing vigilance.

Phishing Simulation: Engage in proactive cybersecurity education through simulated phishing attacks. This hands-on approach trains employees to recognize and respond to threats in real-world scenarios, thereby strengthening your overall security posture.

2 Limit Access with Compliant Devices

Unmanaged PCs represent a significant vulnerability to both company and customer data. Devices that operate with local user profiles and without centralized management leave critical endpoints exposed to security risks. To safeguard access to company data, it is essential to establish Corporate Profiles on every device. This also enables you to restrict the use of personal computers that may otherwise leave sensitive information unprotected on unmanaged devices.

Device Management: Microsoft Azure Entra ID enhances device management by enabling features such as device registration, enforcement of conditional access policies based on device compliance, and the application of security policies across all devices. This ensures that workstations and other endpoints are properly secured and managed.

Centralized Identity Management: With Microsoft Azure Entra ID, administrators benefit from a centralized identity management system, allowing for streamlined control over user identities, permissions, and access policies. This centralized approach simplifies user provisioning, de-provisioning, and the overall identity lifecycle management, ensuring consistent security across the organization.

Reporting and Auditing: Microsoft Azure Entra ID offers robust reporting and auditing capabilities. Administrators can monitor user activities, sign-ins, and access events, aiding in compliance, security monitoring, and troubleshooting. These insights are crucial for maintaining a secure and compliant IT environment.

Disk Encryption: Encrypting data at rest, such as on virtual machines or disks, is vital for protecting sensitive information. Disk encryption ensures that even in the event of unauthorized access, the data remains unreadable without the appropriate encryption keys. This layer of security is essential for safeguarding your organization's most critical assets.

3 Implement Data Loss Prevention (DLP)

Sending sensitive data via email without encryption is a significant security risk. Data Loss Prevention (DLP) is a comprehensive set of tools and features designed to help organizations prevent the accidental or intentional exposure of sensitive information.

Protect Sensitive Data: Microsoft 365 DLP safeguards your organization by identifying and preventing unauthorized sharing or exposure of confidential data, such as financial records, customer information, intellectual property, and more. This proactive approach ensures that sensitive information remains secure.

Policy Enforcement: With Microsoft 365 DLP, organizations can define and enforce specific policies on how sensitive information should be managed. This includes preventing the sharing of certain data outside the organization and enforcing encryption on emails containing sensitive content, thereby reducing the risk of data breaches.

Regulatory Compliance: Microsoft 365 DLP helps organizations adhere to industry regulations and data protection laws by providing tools to control the flow of sensitive information. This is particularly critical for industries subject to stringent regulatory requirements, such as healthcare (HIPAA), finance (PCI DSS), and others.

4 Ensure Security Patches Are Up-to-Date

New vulnerabilities are continuously discovered in widely used software applications, such as Microsoft 365. It is crucial to regularly patch and update your systems to protect against these emerging threats. Under a managed IT plan, this process can be automated, ensuring that all critical updates are applied promptly, without the risk of missing any important security patches.

Mitigate Exploitation Risks: Cybercriminals actively scan for unpatched systems as they provide easy entry points for attacks. By keeping your software up-to-date, you significantly reduce the risk of exploitation from known vulnerabilities, safeguarding your business from potential breaches.

Enhance System Performance and Stability: Security patches often include updates that improve the overall performance and stability of your software. Regularly applying these patches ensures that your systems run efficiently, minimizing downtime and enhancing productivity.

Maintain Compliance: Many industry regulations and standards require organizations to keep their software up-to-date as part of their cybersecurity protocols. Ensuring that your patches are current helps your business remain compliant with these regulations, avoiding potential fines and legal issues.

5 Implement a Robust Backup Strategy

Having a reliable backup solution is essential in protecting your business against even the most sophisticated ransomware attacks, where hackers encrypt your files and demand a ransom for their release. With a comprehensive backup in place, you can restore your data without paying cybercriminals. Additionally, a strong backup strategy protects your business from accidental file deletions, overwrites, natural disasters, fires, water damage, hardware failures, and other data-loss scenarios. To ensure your backups are effective:

Automate and Monitor Backups: Your backups should be automated and continuously monitored to guarantee that they are always up-to-date and functional. The worst time to discover a backup failure is when you urgently need to recover your data.

Multi-Platform Safeguards: It's critical to secure data across multiple platforms, including on-premises servers, Microsoft 365, and cloud environments like Microsoft Azure. This multi-layered approach ensures that your data is protected, regardless of where it is stored or accessed.

Regular Testing: Regularly test your backups to confirm they can be restored quickly and completely. Routine testing helps identify potential issues before they become critical, giving you peace of mind that your data is secure.

6 Avoid Granting Local Admin Rights to Employees

Cybercriminals often gain access to networks by deceiving users into downloading malicious software, which is commonly disguised within seemingly innocuous files, games, or applications. To mitigate this risk, it is essential to remove local admin rights from employees. By restricting these privileges, you significantly reduce the potential for unauthorized software installation and enhance your overall network security.

Reduce Risk of Malicious Software Installation: Without admin rights, employees cannot install unauthorized software, which helps prevent the introduction of malicious programs and reduces the risk of potential security breaches.

Limit Damage from Accidental Actions: Restricting admin rights helps minimize the impact of accidental or unintentional actions that could compromise network security, such as unauthorized changes to system settings or configurations.

Improve Compliance with Security Policies: Removing local admin rights ensures that users adhere to established security policies and standards, facilitating better control over software installations and system modifications, and aiding in compliance with industry regulations.

7 Don’t let your Firewall Security Subscription Expire

A firewall plays a crucial role in securing computer networks by monitoring and controlling incoming and outgoing network traffic. One needs to be installed at the corporate office to protect the data on the external storage device with customer data, copy machines and any check scanners. These devices have a security subscription that needs to be maintained every year or monthly. Without such a security subscription the following protection is not active.

Intrusion Detection and Prevention: Firewalls can include intrusion detection and prevention systems (IDPS) to identify and respond to potential security threats. They can detect suspicious patterns or behaviors and take preventive actions to stop potential attacks.

Logging and Auditing: Firewalls log information about network traffic, access attempts, and security events. These logs are valuable for security audits, troubleshooting, and forensic analysis in the event of a security incident.

Content Filtering: Firewalls can be configured to filter content based on specific criteria, such as keywords, URLs, or file types. This helps in blocking access to inappropriate or malicious content, enhancing overall security.

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 offer to conduct a **FREE Security Audit** to assess your company's overall network health, identifying and addressing potential data-loss risks and security vulnerabilities. Additionally, we'll examine common areas where security measures may be overlooked.

- 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 their personal devices to access your companies sensitive data?
- Is your firewall and PC protection configured properly and up-to-date?
- Are your employees able to send emails with sensitive data?

IT and Security Management

- When doing business with CNS instead of addressing problems piecemeal and requesting additional funds for proper resolution, we prioritize doing it correctly from the outset. Rather than charging thousands of dollars to configure our customers' systems as they should be, CNS invests upfront time to migrate data, reconfigure PCs, secure systems, protect data, and transition to the cloud. We aim to ensure that we develop our relationship with customers by bringing them up to standards and then maintaining such a level of security.
- **Enhanced Security and Compliance:** CNS implements industry-standard security policies, ensuring a robust infrastructure that protects sensitive data and maintains compliance with industry regulations. MSPs like CNS stay abreast of the latest security threats, proactively adapting measures to evolving risks, a task challenging for in-house teams to match.
- **Focus on Core Business Functions:** By outsourcing the implementation and maintenance of security policies to CNS, your organization can focus on its core business functions without the distraction of managing complex IT security matters. This enables your internal teams to direct their energy and resources towards strategic initiatives and activities that directly contribute to the company's growth and success.
- **On-Demand Technical Support:** CNS provides on-demand assistance, promptly addressing technical issues to minimize downtime and optimize productivity. Employees can easily reach out to CNS for help with IT concerns, fostering overall satisfaction and ensuring a streamlined workflow in the organization.

You Are Under No Obligation To Do Or Buy Anything

It's natural to feel confident that your current IT setup is secure. However, based on my 25 years of experience, I can almost guarantee that my team will uncover one or more vulnerabilities that put your business at significant risk of hacker attacks, data loss, or prolonged downtime. We see these issues far too often.

Even if you have a trusted IT person or company managing your network, it's always beneficial to have a third-party review to ensure nothing has been overlooked. As an independent consultant, I have no vested interest in protecting anyone or glossing over potential issues. If you want an honest, unbiased assessment of your network's security, I'm here to provide you with the straight truth.

I want to assure you that there are no obligations or expectations when you take advantage of our Free Security Audit. I personally guarantee that you won't encounter any pushy or aggressive sales tactics—like you, I appreciate a straightforward, pressure-free experience.

Whether we're the right fit for your needs is something we can determine together. If we are, we'd be honored to work with you. If not, we're still pleased to offer this valuable service to help protect your business.

You've worked hard to build your business, earning every client and every dollar. Why risk losing it all? Get the facts and ensure your business, reputation, and data are fully protected.

Dedicated to serving you,

Thank you,

John Guarienti
Vice President

What Our Clients Are Saying...

Good IT companies won't confuse you with techno-mumbo-jumbo, and they certainly shouldn't make you feel stupid for asking questions. All great consultants have the "heart of a teacher" and will take time to answer your questions and explain everything in simple terms. As you interact with them in the evaluation process, watch for this.

Our technicians are trained to take time to answer your questions and explain everything in simple terms. Just look at what our clients had to say:

Douglas Woods

★★★★★

"We have been using CNS for our IT needs for about 6 months. They are friendly, knowledgeable, responsive, innovative and consistently proactive in making sure that if one individual has an issue that no one else at the branch experiences that problem. CNS works well servicing large and small organizations."

Douglas Woods - Branch Production Manager - American Pacific Mortgage

Cooper Hosley

★★★★★

"More than five years ago, Grow West handed over our IT infrastructure to CNS. They've been a crucial business partner ever since, consistently delivering dependable service and stellar support. Through challenges like wildfires, winter storms, and the pandemic, our team maintained full access to our systems, even with our offices closed. With CNS, we can focus on our core functions, secure in the knowledge that our IT infrastructure and support are in excellent hands."

Heather Headley

★★★★★

"I work for APMC mortgage as a LO/Loan. Since CNS-Service/Capital Network Solutions, Inc. has become our in-house help desk, it's been AWESOME. They're corrected tech items that just couldn't be handled before. I've spoken with 4 different people and every single one has been knowledgeable, courteous, works and gets things done at warp speed and have always completed correctly. They're really nice too. I can't recommend this company highly enough. Heather Headley, NMLS #247345"