





**NEOLORE**  
NETWORKS INC.

# 12 THINGS

## EVERY SMB NEEDS ON THEIR CYBERSECURITY CHECKLIST

Block Most Cyber Threats With This Simple Checklist

 1 833 828-4988

 [neolore.com](https://neolore.com)

## Introduction

### The 12-Piece SMB Cybersecurity Checklist

1. Avoid Local Administrators
2. Enable Multi-Factor Authentication
3. Lock Down Your RDP
4. Limit User Access
5. Restrict What Applications You Run
6. Stay on Top of Vulnerabilities
7. Update Everything
8. Use Secure Passwords
9. Disable Macros
10. Use Your Firewalls
11. Watch Your Domain Access
12. Implement Storage Policies

### Simplify Cybersecurity With NeoLore Networks



# Introduction

[61% of small and medium businesses](#) experience a cyber attack yearly, while large enterprises face [130 security incidents daily](#). These numbers challenge the assumptions that a business can be too large or too small to be targeted.

Regardless of size, every business is a potential target for cybercriminals because launching a cyber attack requires minimal resources. The rise of ransomware-as-a-service (RaaS) and similar service models means that hackers no longer need to be technologically savvy to target your business.

As technology advances, so do cyber threats, and cybersecurity must advance in response. To help you stay ahead, our guide provides 12 essential cybersecurity measures that every business of every size should use (if they aren't already).

**Already Looking For Some Cyber Help?**

[Learn More](#)

## The 12-Piece SMB Cybersecurity Checklist

### 1. Avoid Local Administrators

Granting local administrator rights may seem convenient for tasks such as installing printers, allowing users to manage their system settings and software installations. However, this convenience poses significant risks.

Local administrators have the ability to make changes, both intentional and accidental, that could compromise the security of your system. Moreover, this risk extends beyond a single computer. A user may gain administrative access not just to their own machine, but to every computer on your network.

Therefore, it is advisable to restrict local administrator privileges to mitigate these security risks.

## 2. Enable Multi-Factor Authentication

Multi-factor authentication plays a crucial role in web security by effectively mitigating the risks associated with compromised passwords. By requiring a second verification form, you significantly reduce the likelihood that an unauthorized user can access accounts, even if they have obtained the password.

Many platforms offer this service at no additional cost, so there's really no excuse not to!

## 3. Lock Down Your RDP

Leaving Remote Desktop Protocol (RDP) ports open to the internet poses significant security risks. For businesses, this vulnerability can lead to severe data losses and even ransomware attacks.

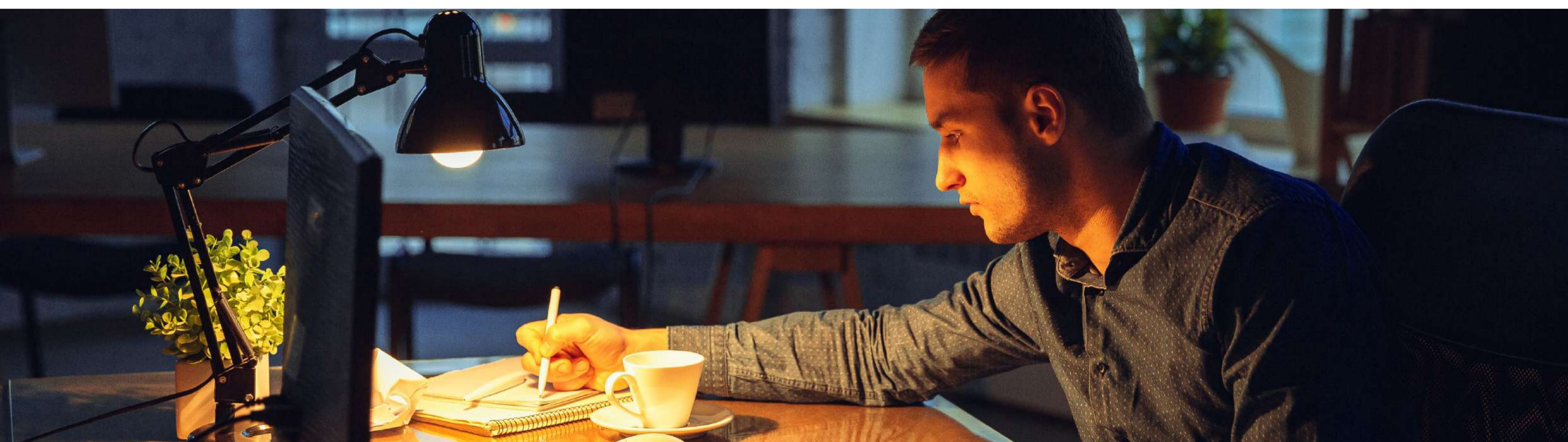
To mitigate these risks, it is critical to restrict all direct internet connections to Remote Desktop and similar services. If Remote Desktop Services (RDS) must be accessible online, ensure this access is via a Remote Desktop Gateway server.

## 4. Limit User Access

Trusting employees is important, but it is also essential to maintain strict access controls to company data. Many organizations have vast file shares that are accessible to all employees, which increases the risk of data breaches.

No matter how trustworthy your team is, accidents can always happen. In fact, unintentional human error accounts for **94% of incidents**. Therefore, it's best to limit user access only to the files they need to do their work.

Also, by restricting access, any damage is confined to the data the employee is authorized to access.



## 5. Restrict What Applications You Run

It is common for employees to use a limited set of applications to perform their job functions. Despite this, operating systems often allow any application to run, which can leave a business vulnerable to new or unknown types of malicious software.

Without restrictions on what applications can run, systems are exposed to potential vulnerabilities and the misuse of legitimate software. Relying solely on antivirus software is insufficient, as it often fails to block all malicious activities. By restricting the applications that can run on company systems, you ensure that only approved software is used.

## 6. Stay on Top of Vulnerabilities

To effectively manage security risks, it is essential to stay vigilant about potential vulnerabilities across all systems and software used within an organization. Conducting regular security assessments and vulnerability scans allows businesses to identify and address security weaknesses before they can be exploited by attackers.

Implementing a robust vulnerability management program involves not just detection, but also prioritizing risks based on their potential impact on the organization. This strategy ensures that critical vulnerabilities receive immediate attention and resources.

### Read More Insights on How You Can Stay Cyber Secure

- [Email Security For Small Businesses: Tips & Tricks](#)
- [SMB Cybersecurity Guide](#)
- [What is Cyber Vandalism & What Can You Do About It?](#)

## 7. Update Everything

Regularly updating and patching software is crucial in defending against exploiting vulnerabilities. Many cyber attacks exploit known vulnerabilities in software that the developers have already patched. Unfortunately, if these updates are not applied in a timely manner, the security gaps remain open.

Establishing a routine for monitoring and applying software updates ensures systems are protected against known threats. This proactive approach is vital for maintaining the integrity and security of your organization's information systems.

## 8. Use Secure Passwords

Many businesses express concerns about the length of password complexity requirements when signing up for security services. However, there is a reason why passwords must be that complex. The harder a password is to guess, the safer you will be.

To maintain password security, follow this checklist (and ensure your staff is doing the same):

- Ensure passwords incorporate a mix of symbols and characters.
- Use different passwords for different accounts.
- Consider using a password manager to manage and generate strong passwords.
- Change passwords immediately if a security breach is detected.

## 9. Disable Macros

Macros were once hailed for their ability to automate tasks in documents and spreadsheets, which significantly enhanced productivity. However, this functionality soon caught the attention of attackers who exploited macros to automate malicious processes.

If macros are not necessary for your operations, it is advisable to disable them to prevent potential security risks. Disabling macros can be done through network settings or manually on individual computers.

## 10. Use Your Firewalls

For cyber attacks to be successful, they often need to spread across a network. One common method for this propagation involves using push installers. Perimeter firewalls are great, but relying solely on perimeter firewalls to prevent spread is insufficient.

Implementing firewalls on individual machines adds an additional layer of defense, helping to block unauthorized attempts to install or run malicious software across the network.

## 11. Watch Your Domain Access

It is crucial to ensure that users do not operate with domain administrator privileges unless absolutely necessary. Regularly review and audit your domain admin groups to remove users who do not require these elevated privileges, leaving only a select few who truly need administrative access.

Additionally, renaming default administrator accounts is a smart security measure. This step adds an extra layer of difficulty for potential attackers trying to gain unauthorized access, as it obfuscates the usernames they often target.

## 12. Implement Storage Policies

Implement policy-driven controls that restrict access at the user and application levels. These measures include configuring settings that limit application access to specific file shares. For instance, ensuring that only designated applications can interact with their respective data prevents unauthorized applications.

Additionally, it's important to prevent users from saving potentially harmful file types to your servers. This can be managed by establishing a clear policy that specifies allowed file types and blocks all others.

Backup policies are also a must. However, they should be set to allow only backup software access to backup drives. That will minimize the risk of these drives being targeted by ransomware or other attacks.

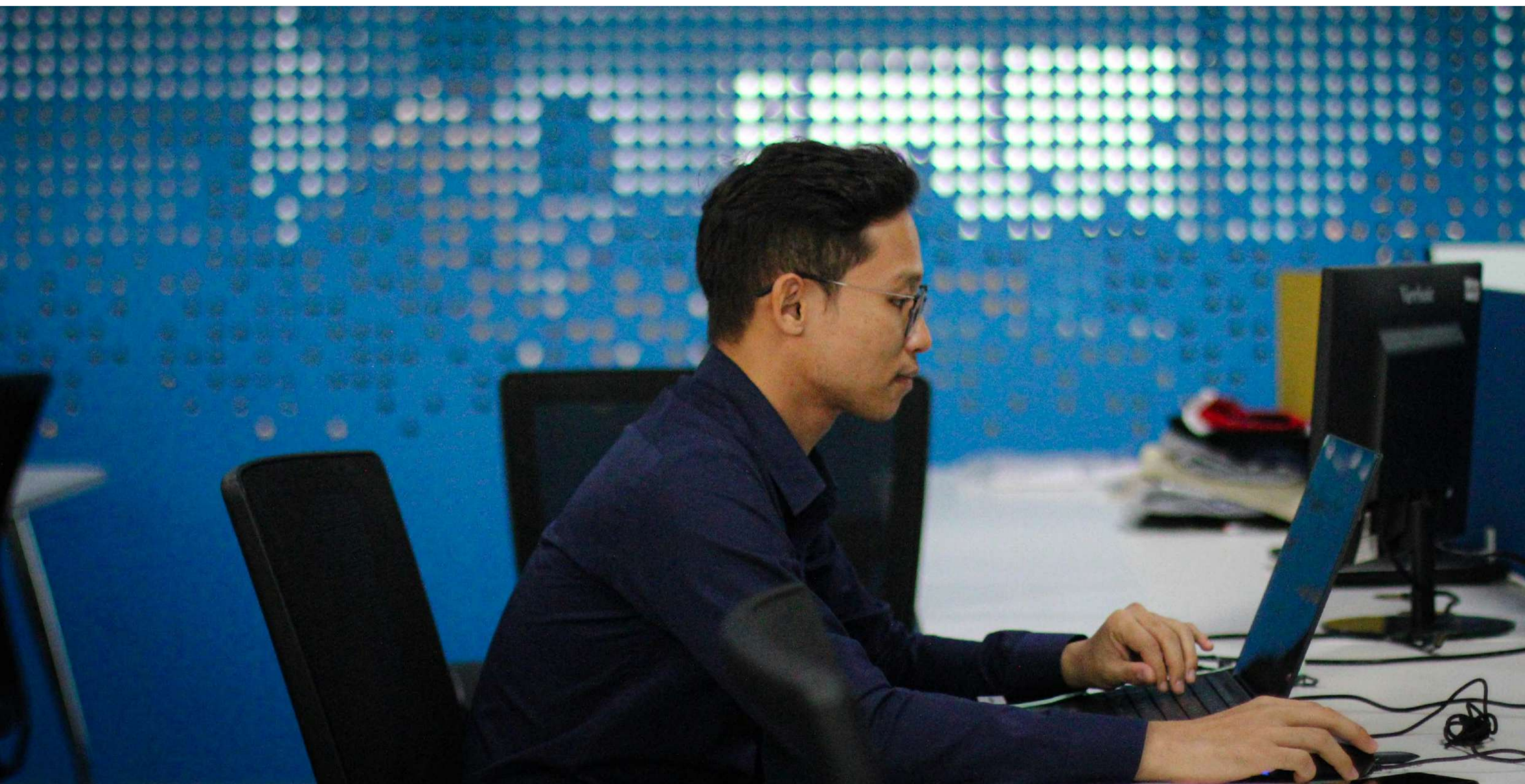


## Simplify Cybersecurity With NeoLore Networks


Adding these 12 checklist items to your cybersecurity strategy will do wonders for your SMB. However, many of these items require some effort to implement, and some require consistent maintenance to stay effective.

If you don't have the time for that, consider working with NeoLore Networks. We're an established, Ottawa-based cybersecurity firm that can do all the cybersecurity heavy lifting so you don't have to.


[Reach out to us](#) today to get started!



Connect With Us

 2781 Lancaster Road, Suite 302 Ottawa, Ontario K1B 1A7 Canada

 [neolore.com](https://neolore.com)

 1 833 828-4988