BOOST YOUR DIGITAL DEFENSES:
5 ESSENTIAL SECURITY TIPS FOR SMALL BUSINESSES FROM NUVERA

Nuvera Business

You're busy with the work your company is designed to do. So, creating and maintaining a cybersecurity plan to protect your business may seem like an overwhelming task. But cybercriminals are busy too.

It's critical to stay on top of the latest threats that might put your revenue, customer data, reputation, and more at risk and learn what you can do to protect them.

The financial risk is real, according to the Small Business Administration, cyberattacks cost small businesses over $2 billion per year.

Start getting prepared today with some essential industry tips.

5 ESSENTIAL SECURITY TIPS FOR SMALL BUSINESSES

1. Secure your network

A secure network starts with a consistent connection from your internet provider. Nuvera delivers that with our 1,400-mile fiber network and three data centers. With the right speed internet plan in place, it's also important to confirm that you're using security measures like firewalls, multi-factor authentication, and virtual private networks (VPNs).

Let's explore how these can help.

- Think of a firewall as a barrier that stops unauthorized access. It can identify and eliminate threats to your network. Install firewalls for both on-site and remote workers as a safeguard.
- VPNs and endpoint security solutions can enhance security, especially for remote workers. A VPN hides your IP address, keeping your data private even when using public or shared Wi-Fi.
- Multi-factor authentication adds another layer of security. It typically involves a login that requires a password and at least one other piece of information, such as a phone number.
- Apply similar security measures to cloud computing platforms, apps, and Wi-Fi networks. For example, you can encrypt and password protect Wi-Fi networks and ensure the router hides the network name.

If you share data with vendors, it's important to ask them about their network security policies.

You can take these steps yourself or turn to the experts at Nuvera, who offer managed services for firewalls, Wi-Fi, and more.

2. Educate and train employees

There's a lot to know about the risks of cyberattacks and the continually evolving landscape of threats. This may help explain why the World Economic Forum's 2022 Global Risks Report found human error causes 95 percent of security breaches.

Train your employees to identify and respond to

potential threats to lower your risk.

- Teach employees how cybercriminals might target them. Make them aware of phishing and spoofing – scams disguised as legitimate emails used to steal passwords or account information.
- Create policies requiring workers to choose unique and complex passwords and change them regularly. Consider a password manager that can suggest secure passwords.
- Set clear procedures for handling data and safe internet browsing. Help employees understand the risks of pirated content and using business computers for personal purposes. Consider additional guidelines to support your remote workers.
- Explain the importance of regular software updates, but also consider limiting authority to install software.

3. Keep devices clean, up to date, and backed up

Cybercriminals may exploit security holes in outdated software to deliver viruses and malware.

- Update devices with the latest security software, web browser, and operating systems. Consider running antivirus software after each update.
- Regularly back up data and information to the cloud to protect against ransomware, hardware failures, or accidental deletions. Regularly test to ensure the backup systems are working, or work with a partner who can test for you.
- Create user accounts for each employee to help control access to computers and devices.
- Create a mobile device action plan with guidance on passwords, security apps, and steps for reporting lost or stolen equipment. Remember phones and laptops may not be protected by traditional antivirus tools.

- Consider a more sophisticated endpoint security solution to secure every device that connects to your network and is equipped with security detection capabilities.

4. Regularly monitor and revise your cybersecurity plan

Cybersecurity threats are constantly evolving. You can find reporting systems that automatically monitor data and trigger alerts. But when a problem arises, you may need someone to help diagnose and fix the cause.

You might find it valuable to work with a company that can help you monitor reports and customize a plan for your future. Our experts at Nuvera can help you review performance issues like processor and memory utilization and hard drive usage. And they can help you pinpoint any issue from failing hardware, undetected malware, or outdated equipment. They can also assist you in deciding whether you need antivirus software, remote monitoring, and 24/7 security analyst support.

5. Be prepared for disaster

Even after you've taken all the steps you can to protect your data, it's important to be prepared for the unexpected.

A disaster recovery plan can keep your business up and running.

- Consider solutions that use a cloud service so you don't need to worry about a physical backup location that could also be affected by a disaster.
- When evaluating a disaster recovery plan, consider if the work begins with a risk assessment and business analysis. Also, ask questions about ease of implementation and the speed of recovery.
- At Nuvera, our cloud-based disaster recovery solution doesn't require significant up-front capital investment or an extensive timetable for setup. We continually test the plan and update it as needed.

Remember that cybersecurity is an ongoing process. Defending your digital assets requires a protection plan that is customizable, flexible, and cost-effective. If you need help tailoring a plan for your business, click here to schedule a free consultation or call 844.610.5300.