Your Small Business IT Survival Guide

As businesses increasingly rely more on technology to operate daily, and while cyberthreats are simultaneously becoming more common, it's hard to keep your networks secure. A breach can result in loss of money, time, resources and reputation. We've put together 11 key factors you need to keep in mind to keep your business secure. Think of it as your IT survival guide:

IT Basics Every Business Needs to Operate and Grow Effectively

1

Office 365 backup options
If you have an intrusion, make sure you have backup options which will allow you to recover your Office 365 data. Microsoft recommends that you regularly backup your Microsoft 365 data using third-party apps and services. This includes e-mail, SharePoint, and OneDrive data.

2

Back up critical workstations
At a minimum, make sure your critical workstations are regularly backed up. This refers to workstations that play a critical role in your business, such as QuickBooks. Not backing up these stations places the business at tremendous risk in the event of a breach.

3

2FA on everything
Make sure all your applications have two-factor authentication (2FA). If you do not have 2FA set up on all your external web-based applications, speak with your vendors today to put it in place.

4

Remove all local admin rights from computers
Do not allow any employees to use admin usernames for their typical login. If you need to give admin computer rights to certain employees, hand them out as a secondary login. For example, if something needs to be installed, an employee needs to log out and log in again with their admin username, or input the additional credentials into a elevated privilege prompt. Regular computer usage should require a non-admin account.

TECH SQUARED
REDUCE STRESS + ADD VALUE

5

Secure any accounts immediately when a user or employee leaves

If an employee or user leaves, secure the account immediately. You may find it tempting to reuse the account for a future user because you have already set everything up for the user, but resist. Reusing accounts can create a big potential vulnerability, particularly with people reusing passwords from other accounts.

6

Test your backups monthly

Routinely, restore test data to make sure the backups work as expected. Do not just set them up and forget them. You don't want to find out when you need the backup that something has not been captured as expected.

7

Security training for users

Provide each user with regular training on keeping their accounts safe. This directive also needs to come from the top down. In other words, make sure that all the higher-ups in the organization go through the training as well, as this creates a culture of cybersecurity rather than sending the message that this training is unimportant.

8

Maintain updates and patches for all software

When vulnerabilities are found and fixed in software, updates and patches are issued. Make sure that each update is installed and reboot systems at least once a week so the operating system can properly update itself. This includes firmware updates for network switches and firewalls.

9

Do not allow personal devices, laptops, cell phones, etc to connect to the corporate network

If you want to provide guests, which includes employee's personal devices, with wireless access, you can do so, just make sure the system is configured correctly. You do not want outside devices to get access to your corporate network.

TECH SQUARED

REDUCE STRESS + ADD VALUE

10

Chose a corporate password manager
A corporate-sponsored password manager standardizes the process. It avoids people storing sensitive passwords in a variety of different locations and again prompts a culture of security, as password managers make it easier for people to actually use secure codes.

11

Filter content using OpenDNS, firewall services or endpoint protection
You do not want to risk people accessing infected sites on your network. Filter all web content through systems such as OpenDNS or firewalls to keep dangerous content out. These systems have a dynamic mechanism for uncovering and blocking the material that can threaten your business.

Keep Your Business Protected with Tech Squared

For businesses to keep their systems and their data protected, they must think carefully about a variety of different aspects of cybersecurity. A secure business does not come from a single step, but instead from thinking about network security from all possible angles.

There are many parts to running a business that business owners need to deal with, but IT should not be one of them. Leave your IT system and security to the experts, so you can dedicate your energy to your business.

BOOK A CONSULTATION

with us today to learn how we will keep your system secure.

TECH SQUARED
REDUCE STRESS + ADD VALUE