# IT BEST PRACTICES
## You Should Be Following Now

## 1 Stay informed.

All too often we rely on the software and technology that was built to secure us, but your biggest threat by far is your staff. People can be easily tricked into helping bad actors get past your technology defenses,

**Make sure your IT is doing regular trainings!**

## 2 Password best practices.

Every employee is required to log in to multiple accounts every day, from email to payroll, file sharing, data collection, and everything in between. Each log in requires a password, and it's only natural to want to take shortcuts such as using the same password across all platforms, choosing easily remembered passwords or jotting them all down on a "hidden" piece of paper.

Reusing passwords is like handing a master key to a cybercriminal. It doesn't matter how strong your defenses are, a hacker can use the master key and walk right in. If you think using your kids' names or your own birthdate are safe, think of what you share on social media platforms such as Facebook and Twitter.

**Use a password manager and make your passwords as unique and complex as possible without using significant names or dates. Be aware of where you are storing those passwords and how you are sharing them. If you do have to share a password, use encryption!**

## 3 Keep your software updated.

There is a window of opportunity between when your software company finds, patches and creates an update for a vulnerability and when each of your employees install those patches. You need to be sure you make that window of opportunity (known as a Zero-Day Exploit) as short as possible. Encourage your employees to install these updates as soon as they receive them. Your entire network security can be compromised by just one outdated security patch.

**Having an IT partner that is proactive and has a process to manage these updates across your business is vitally important.**

## 4 Know how to spot sophisticated phishing emails.

While we still see the occasional obvious phishing email, they have gotten tremendously more advanced in how to hide their identity and intentions.

**Train your staff to use the 10 best practices for email security by hanging a reminder in offices and breakrooms throughout your organization.**

## 5 Multifactor Authentication and Dual Approval.

Using Multifactor Authentication tools can lock down your personal information and make it significantly harder for bad actors to compromise your accounts and information. You can also use human to human dual approval when possible. Encourage employees to give a quick phone call for verification of any usual requests, such as changing the routing of payment that is coming from a vendor or client.

**Using a different medium to authenticate or confirm unusual requests can stop a malicious attack dead in its tracks.**

## 6 Calls to action.

Be on alert for emails, websites, social platforms that call you to take an action. Some examples might include a link in an email, a pop up that requests your login information, a shortened link on a social media post. Most often a cyberattack requires a human to interact with it to help it launch.

**One of the best practices you can implement is to go directly to the source. If you see a link to an article on LinkedIn that interests you, do not click on the "suggested" link. Go instead to the official website that is hosting the information you want and search for the content there.**

## 7 Have a layered security platform.

Having anti-virus and malware protection is good. Having a firewall is good. Having web filtering is good. Having email filtering is good. But each one is not enough on its own. Each is subject to exploits, hacks and vulnerabilities.

**You want to have multiple overlapping forms of cyber security that can authenticate the identity of the correct user. This is one of the most important tips for preparing an effective cybersecurity strategy. Partner with an MSP to manage your cybersecurity platform, update it, monitor and evaluate it continuously, and strategic and proactive changes.**

## 8 Have a backup.

Many times, the strategy of a bad actor is to install something called ransomware. Ransomware is currently one of the biggest threats to SMB's. This malware encrypts your data and holds the unencrypting key hostage for ransom, leaving you with only two courses of action: paying the criminal and hoping they give you your data back without selling or exposing it, or relying on your backups to restore your encrypted or deleted files.

**Backups are the best option dealing with ransomware, malicious threats and other malware, natural disasters such as fire or storm damage, and failing equipment.**

## 9 Have a disaster recovery plan.

Having a backup is good, but what if you couldn't get all of your data back for a month? Weeks? Days? What will that data loss cost your business in downtime, inefficiency, and loss of reputation with your clients and customers? A disaster recovery plan puts your backup in a position to minimize the time it takes to recover your data and put you "back in business."

**Your IT partner should work with you to build a comprehensive Disaster Recovery Plan. This plan will help you determine how quickly you need to get back to becoming fully operational, how much redundancy you need in your backup plan, and how to deal with different types of events including fire, flood, lost files, damaged hardware, and malware.**

## 10 Partnerships.

Your employees may feel that IT just complicates their jobs. You need an IT company that understands this and creates a compromise between overly restrictive IT requirements and employee satisfaction while never backing down from rigorous security.

**The ultimate IT best practice is to partner with a reliable Managed Services Provider who will provide you with the best, most cost-effective solutions available to meet your small to medium-sized business' requirements.**