TECHNIVANA

Nimble. Scalable. Secure.

Scan to get a free (yes free, no hassle) consultation!

info@technivana.com

(541) 570-4072

technivana.com

Often the teams at SMBs are making mistakes they don't even realize. Below are some of the biggest reasons small businesses fall victim to cyberattacks. Read on to see if any of this sounds familiar around your company!

1. Underestimating the Threat

One of the biggest cybersecurity mistakes of SMBs is underestimating the threat landscape. Many business owners assume that their company is too small to be a target. But this is a dangerous misconception. Cybercriminals often see small businesses as easy targets. They believe the company lacks the resources or expertise to defend against attacks. It's essential to understand that no business is too small for cybercriminals to target. Being proactive in cybersecurity is crucial.

2. Neglecting Employee Training

When was the last time you trained your employees on cybersecurity? Small businesses often neglect cybersecurity training for their employees. Owners assume that they will naturally be cautious online.

But the human factor is a significant source of security vulnerabilities. Employees may inadvertently click on malicious links or download infected files. Staff cybersecurity training helps them:

- *Recognize phishing attempts*
- *Understand the importance of strong passwords*
- *Be aware of social engineering tactics used by cybercriminals*

3. Not using Passwordless Logins or Using Weak Passwords

Weak passwords are a common security vulnerability in small companies. Many employees use easily guessable passwords. They also reuse the same password for several accounts. This can leave your company's sensitive information exposed to hackers.

People reuse passwords 64% of the time.

Encourage the use of strong, unique passwords, or passwordless logins. Consider implementing multi-factor authentication (MFA) wherever possible. This adds an extra layer of security.

4. Ignoring Software Updates

Failing to keep software and operating systems up to date is another mistake. Cybercriminals often exploit known vulnerabilities in outdated software to gain access to systems. Small businesses should regularly update their software to patch known security flaws. This includes operating systems, web browsers, and antivirus programs.

5. Lacking a Data Backup Plan

Small companies may not have formal data backup and recovery plans. They might mistakenly assume that data loss won't happen to them. But data loss can occur due to various reasons. This includes cyberattacks, hardware failures, or human errors.

6. No Formal Security Policies

Small businesses often operate without clear policies and procedures. With no clear and enforceable security policies, employees may not know critical information. Such as how to handle sensitive data. Or how to use company devices securely or respond to security incidents.

Small businesses should establish formal security policies and procedures. As well as communicate them to all employees. These policies should cover things like:

·Password management
·Data handling
·Incident reporting
·Remote work security
·And other security topics

7. Ignoring Mobile Security

As more employees use mobile devices for work, mobile security is increasingly important. Small companies often overlook this aspect of cybersecurity.

Put in place mobile device management (MDM) solutions. These enforce security policies on company- and employee-owned devices used for work-related activities.

8. Failing to Regularly Watch Networks

SMBs may not have IT staff to watch their networks for suspicious activities. This can result in delayed detection of security breaches.

Install network monitoring tools. Or consider outsourcing network monitoring services. This can help your business promptly identify and respond to potential threats.

9. No Incident Response Plan

In the face of a cybersecurity incident, SMBs without an incident response plan may panic. They can also respond ineffectively.

Develop a comprehensive incident response plan. One that outlines the steps to take when a security incident occurs. This should include communication plans, isolation procedures, and a clear chain of command.

10. Thinking They Don't Need Managed IT Services

Cyber threats are continually evolving. New attack techniques emerge regularly. Small businesses often have a hard time keeping up. Yet, they believe they are "too small" to pay for managed IT services.

Managed services come in all package sizes. This includes those designed for SMB budgets. A managed service provider (MSP) can keep your business safe from cyberattacks. As well as save you money at the same time by optimizing your IT.

Learn More About Managed IT Services

Don't risk losing your business because of a cyberattack. Managed IT services can be more affordable for your small business than you think.

Give us a call today to schedule a chat! (541) 570-4072

Proud Member: Albany Area Chamber of Commerce

*** Information used with permission from The Technology Press. ***