10 WAYS HACKERS BREACH YOUR DEFENSES

A FREE REPORT

CSU COMPUTER SERVICES UNLIMITED

CSU COMPUTER SERVICES UNLIMITED

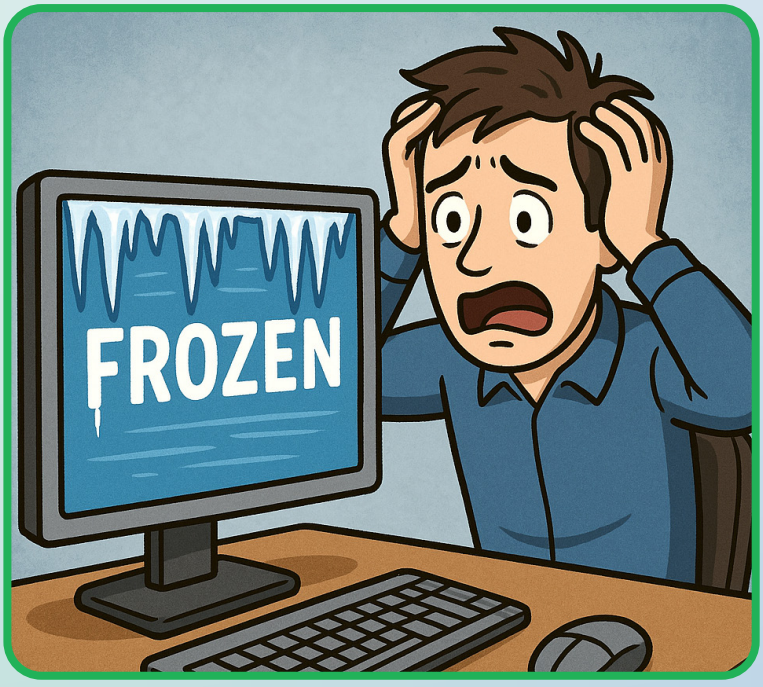
Imagine this: You start your workday like any other—coffee in hand, emails open—when suddenly your system locks up.

A message appears: "Your files have been encrypted. Pay $20,000 in Bitcoin to regain access."

You call your IT team. A phishing email slipped through. One employee clicked. Your firewall wasn't up to date. Backups? Failed weeks ago.

Your business is now frozen. Client data, financial records, everything—held hostage.

This isn't rare... 1 in 5 small businesses were hit by cybercrime last year. 82,000 new threats emerge every day. Half of all attacks target businesses like yours.



You rarely hear about these attacks. Victims stay silent—afraid of the fallout: bad PR, lawsuits, fines, and sheer embarrassment. But the threat is real. Every day, headlines announce another breach, another business brought to its knees. Fines and regulations are increasing. Cybercrime isn't just an IT issue—it's a business survival issue.

Cyber crime is at an all time high, even with new and stronger defenses. Hackers have set their sights on small and medium businesses who are "low hanging fruit." Don't be their next victim.

This guide reveals common ways hackers get through your security and how you can protect yourself and your business.

Securing These 10 Weak Points May Be What Saves Your Business

SMBs Like Yours Are the #1 Target

It's critical to protect yourself from these 10 common tactics hackers use to break into businesses like yours:

1. Untrained Employees Who Fall for Scams

Your team is your first line of defense—and your biggest vulnerability. One click on a phishing email can bring your entire business to its knees. If your staff can't spot a fake login page or malicious link, it's not a matter of if you'll be hit, but when.

2. Unsafe Use of Personal and Work Devices

Employees using work laptops for personal browsing—or accessing company data on personal phones—opens serious risk. Without an Acceptable Use Policy and mobile device management in place, your sensitive data could be exposed, lost, or stolen without your knowledge.

3. Weak or Reused Passwords

"Password123" isn't protecting anything. Hackers can crack weak passwords in seconds. Strong, complex passwords—enforced through proper IT policy—are your best defense. Add multi-factor authentication (MFA) and you shut down one of the easiest entry points.

4. Outdated or Unpatched Software

If your systems aren't kept up to date, you're running with known vulnerabilities—ones hackers already know how to exploit. Regular, automated patching should be part of every business's IT maintenance routine.

5. No Reliable Backup in Place

Ransomware attacks encrypt your data and hold it hostage. But if you have a secure, automated, off-site backup system, you can simply restore everything—no ransom, no panic. Backups also protect against hardware failure, accidental deletion, and natural disasters.

6. Unauthorized or Risky Software

Free games, browser plugins, or unapproved "productivity tools" can hide spyware, malware, or worse. Without proper controls and employee training, a well-meaning download can lead to a full-scale breach.

7. Weak or Unmanaged Firewalls

Firewalls are your digital gatekeepers—but they're not a "set it and forget it" solution. They must be configured correctly, regularly updated, and continuously monitored to stay effective.

8. Public WiFi Use Without Protection

That free WiFi at the coffee shop or airport? It might be a trap. Hackers often set up fake networks to capture your login credentials or access your devices. VPNs and mobile security protocols are a must for any business with remote or traveling staff.

9. Deceptively Real Phishing Attacks

"Your Amazon package is delayed." "Payroll issue—click here." These emails look legitimate—but they're traps. Phishing remains one of the most successful hacker strategies. Ongoing employee awareness and email filtering tools are your best protection.

10. Social Engineering—When Hackers Pretend to Be You

Sometimes, hackers don't need code—they just need confidence. By impersonating executives, vendors, or even IT staff, they trick employees into handing over access, passwords, or sensitive information. Awareness and strict verification procedures stop this trickery in its tracks.

CSU Can Implement A Managed Security Plan For Your Business

For organizations concerned about employee behavior or the increasing threats posed by cybercriminals, Computer Services Unlimited offers a free Security and Backup Audit. CSU will dispatch a certified technician and security consultant to assess the overall health of the company's network and identify data-loss vulnerabilities and security loopholes. This includes exposing fine-print clauses used by many third-party cloud vendors that eliminate their responsibility for securing or backing up customer data. The audit also evaluates commonly overlooked areas such as mobile devices, laptops, tablets, and home PCs that may not be adequately protected. At the end of this free audit, you'll know:

- **Are cybercriminals one step away from breaching your network?**
  We'll test your defenses to see if they can withstand today's sneaky and sophisticated attacks.
- **Is your backup system really backing up everything important—and can you recover fast if disaster strikes?**
  We'll show you exactly how long a full restore would take (and it's often longer than most business owners expect).
- **Are employees unknowingly putting your business at risk?**
  We'll reveal if internet usage habits—like streaming, shopping, social media, or even job hunting—are putting productivity or security in jeopardy.
- **Are you violating any data privacy regulations (like PCI or HIPAA) without realizing it?**
  The rules are constantly changing, and a simple misstep could cost you thousands in fines and PR damage.
- **Is your antivirus, firewall, and cloud storage actually doing its job?**
  We'll identify weak points, like outdated software, misconfigurations, or overlooked personal devices that aren't protected.
- **Are employees using cloud apps like Dropbox or Google Drive that fall completely outside your backup system?**
  These "shadow IT" risks are easy to miss—and hackers know it.

I know it's natural to want to think, "We've got it covered." Yet, CSU uncovers critical security gaps—even in organizations with internal IT staff or existing service providers. A third-party assessment can provide unbiased insight and ensure nothing critical has been overlooked. We deliver an honest, transparent evaluation with no agenda other than helping businesses protect their data and operations.

You Are Under No Obligation To Do Or Buy Anything

I also want to be very clear that there are no expectations on our part for you to do or buy anything when you take us up on our Security And Backup Audit. As a matter of fact, I will give you my personal guarantee that you won't have to deal with a pushy, arrogant salesperson because I don't appreciate heavy sales pressure any more than you do.

Whether or not we're a right fit for you remains to be seen. If we are, we'll welcome the opportunity. But if not, we're still more than happy to give this free service to you.

You've spent a lifetime working hard to get where you are. You earned every penny and every client. Why risk losing it all? Get the facts and be certain your business, your reputation and your data are protected.

Request Your Security And Backup Audit Today!

Taking the first step is simple. Reach out to Computer Services Unlimited by:

Phone: 703-968-2600

Email: info@csuinc.com

Website: Fill out the form to schedule a meeting here, https://www.csuinc.com/cybersecurity

Our office will call you to schedule a convenient time for us to meet for 20-30 minutes. Remember, there is no obligation for you to buy or do anything – this is simply a discovery meeting to see if your organization is safe from the hacker loopholes!

Let's Connect!
Follow us on social media:

Facebook
Computer Services Unlimited Inc.

LinkedIn
Computer Services Unlimited Inc.

Instagram
computer_services_unlimited

CSU COMPUTER SERVICES UNLIMITED

14240-G Sullyfield Circle
Chantilly, VA 20151

Phone: 703-968-2600

Websites: csuinc.com,
vetitservices.com, csugov.com