5 Cybersecurity Mistakes That Could Cost Your Business (And How to Fix Them)

Running a business in South Africa today means juggling a hundred different priorities. Between managing staff, keeping customers happy, and watching your bottom line, cybersecurity often falls to the bottom of the to-do list.

But here's the reality: cybercrime is growing fast, and small to medium businesses are the prime targets. Why? Because cybercriminals know you're busy, and they're counting on you to make simple mistakes.

The good news? Most cyber attacks can be prevented with a few straightforward fixes. Let's walk through the five most common mistakes we see at Elijah IT, and more importantly, how you can avoid them.

1. Using Weak or Repeated Passwords

We get it. Remembering dozens of complex passwords is a headache. That's why so many people use "Password123" or recycle the same password across multiple accounts.

Why it's dangerous: Hackers use automated tools that can crack simple passwords in seconds. If they get into one account, they'll try that same password everywhere else.

The fix: Use a password manager like Bitwarden or LastPass. These tools generate strong, unique passwords for every account and remember them for you. You only need to remember one master password. Plus, enable multi-factor authentication (MFA) wherever possible – it's like adding a deadbolt to your digital door.

2. Skipping Software Updates

Those pop-up notifications telling you to update your software? They're not just annoying reminders – they're critical security patches.

Why it's dangerous: Cybercriminals actively search for known vulnerabilities in outdated software. When companies release updates, they're often fixing security holes that hackers already know about.

The fix: Enable automatic updates on all your devices and software. Yes, updates can be inconvenient, but they're far less disruptive than dealing with a ransomware attack that locks you out of your entire system.

3. Clicking Links Without Thinking

Phishing emails are getting more sophisticated. They look like they're from your bank, SARS, or even your own IT department. One careless click can give hackers access to your entire network.

Why it's dangerous: Phishing is the number one way cybercriminals gain access to business systems. They're betting on people being busy and distracted.

The fix: Train yourself and your team to pause before clicking. Does the email seem urgent or threatening? Is it asking for sensitive information? Check the sender's email address carefully – scammers often use addresses that look almost right, like "support@m1crosoft.com" instead of "microsoft.com". When in doubt, contact the company directly using a phone number or website you find yourself, not one provided in the email.

4. Not Backing Up Your Data

"It won't happen to me" is what everyone thinks – until it does. Hard drives fail, ransomware strikes, and accidents happen. Without backups, your business data could disappear in an instant.

Why it's dangerous: Ransomware attacks have skyrocketed. Criminals encrypt your files and demand payment to unlock them. Without backups, you're stuck between paying criminals or losing everything.

The fix: Follow the 3-2-1 backup rule. Keep three copies of your data, on two different types of storage, with one copy stored offsite (like in the cloud). Test your backups regularly to make sure they actually work. At Elijah IT, we set up automated cloud backups for our clients so they never have to think about it.

5. Giving Everyone Full Access

Not every employee needs access to every file and system. When everyone has administrator rights, a single compromised account can expose everything.

Why it's dangerous: If a hacker gains access to an account with full permissions, they can steal data, install malware, or delete critical files. Internal threats – whether intentional or accidental – are also a real concern.

The fix: Implement the principle of least privilege. Give employees access only to the systems and data they need to do their jobs. Use role-based access controls, and review permissions regularly. When someone changes roles or leaves the company, update or revoke their access immediately.

The Bottom Line

Cybersecurity doesn't have to be complicated or expensive. Most breaches happen because of simple, preventable mistakes. By addressing these five areas, you're already ahead of most businesses.

Remember, cybercriminals are looking for easy targets. Make your business a hard target.

Need help securing your business? At Elijah IT, we specialize in cybersecurity solutions for South African businesses. From vulnerability assessments to 24/7 monitoring, we've got you covered. Get in touch with us at support@elijahit.co.za or call our Durban office at +27 87 265 7561.

Don't wait until it's too late. Your business deserves better protection.