GRANT HUGHES
SPEAKER - AUTHOR - ADVISOR

PEOPLE | PROCESS | TECHNOLOGY
A SAFER TOMORROW

THE CYBER ESSENTIALS PLAYBOOK

10 ESSENTIAL CYBER CONTROLS
EVERY SME SHOULD HAVE



01
IDENTIFY
UNDERSTAND YOUR RISKS

02
IMPLEMENT
PUT THE RIGHT CONTROLS IN PLACE

03
STAY SECURE
BUILD A STRONGER BUSINESS

www.granthughes.co.za | info@granthughes.co.za

PRACTICAL INSIGHTS
REAL IMPACT

Introduction

If you are reading this, you own, run, or are responsible for a Small, Medium and Micro Enterprise (SMME) and have realised that cybersecurity is no longer optional for your organisation.

This guide does not contain radically new information. Instead, it consolidates some of the most basic yet important cybersecurity practices that every business should consider. Implementing these measures can help prevent a significant number of common cyberattacks and fraud.

The recommendations in this guide have been specifically selected because many are either free or very low-cost to implement, making them practical for businesses of any size.

Consider something as simple as passwords. For several years, “123456” has remained one of the most commonly used passwords in the world. There is no financial cost to choosing a stronger password, but there are certainly significant benefits.

Cybersecurity does not always have to be complicated or expensive. Sometimes, getting the basics right can make the biggest difference. I hope this guide is helpful.

ESSENTIAL CONTROL 01

1. Multi-Factor Authentication (MFA)

Cost: Low	Complexity: Low	Fraud Effectiveness: High

What it means: A login step that requires something more than just a password - usually a one-time code sent to your phone or generated by an app - before someone can access your email, banking or business systems.

Why it matters: Passwords get stolen, guessed or leaked in data breaches every day. In South Africa, SIM-swap fraud and phishing make stolen passwords one of the easiest ways criminals get into business email and banking accounts - the first step in most Business Email Compromise (BEC) and account takeover scams.

What your business should do:

- Turn on MFA for email, online banking, accounting software and cloud services (free in Microsoft 365, Google Workspace and most SA banking apps).
- Use an authenticator app (e.g. Google/Microsoft Authenticator) rather than SMS codes where possible, since SIM-swap fraud can intercept SMS one-time codes.
- Make MFA compulsory for everyone with access to email, banking or admin accounts, not only senior staff.

ESSENTIAL CONTROL 02

2. Payment Verification & Dual Authorisation

Cost: Low	Complexity: Low	Fraud Effectiveness: High

What it means: A simple internal rule that no payment, banking-detail change, or supplier account change is ever actioned from an email, unexpected phone call, or WhatsApp message alone - it is always confirmed by phone, using a number you already have on file, before any changes are made or money is transferred.

Why it matters: This is the single most effective defence against Payment Diversion Fraud and fake-invoice scams, where criminals impersonate a supplier, your CEO, or your bank to redirect a legitimate payment into their own account. It is free to implement and directly targets the fraud that costs SMMEs the most money.

What your business should do:

- Require a phone call to a known, previously verified number before paying any new or changed banking details.
- Require two people to approve any payment above an agreed threshold.
- Never change banking details based on an email, unexpected phone call, or WhatsApp message alone, even if it appears to come from your CEO, accountant, or a regular supplier.

ESSENTIAL CONTROL 03

3. Staff Awareness Training

Cost: Low	Complexity: Low	Fraud Effectiveness: High

What it means: Teaching every employee - not only IT or finance staff - how to spot common cyber scams and fraud attempts, and how to report it.

Why it matters: Most successful cybercrime against SMMEs starts with a someone clicking a link, trusting a fake WhatsApp message, or acting on urgency without checking. Teaching staff is your cheapest and most effective defence against WhatsApp/personal-email scams, impersonation fraud and BEC.

What your business should do:

- Run a short 30-minute session using real local scam examples - WhatsApp "boss" scams, fake SARS/bank messages, urgent payment requests.
- Teach a simple "stop, check, verify" habit for any urgent or unusual request involving money or personal information.
- Keep it alive by sharing new scam examples as they appear rather than training once-off every few months.
- For a collection of free and fun content you can use, check Grant’s Cyber Awareness Library

ESSENTIAL CONTROL 04

4. Password Management

Cost: Low	Complexity: Low	Fraud Effectiveness: High

What it means: Making sure every account has its own strong, unique password rather than the same (or a simple) password reused everywhere.

Why it matters: Criminals test stolen passwords from one data breach against many other accounts. A weak or reused password on one forgotten account can hand over access to email or banking.

What your business should do:

- Use a password manager (several good free options exist) so staff do not need to remember dozens of passwords.
- Set a minimum password standard: a unique password for every account, with at least 15 characters.
- Change all default and administrator passwords on routers, POS systems, and software immediately when they are first set up. Ask your IT provider to confirm that this has been done, and securely store the passwords internally in a password manager.
- Never share passwords via WhatsApp or email, especially where the username and password appear in the same message.

ESSENTIAL CONTROL 05

5. Secure Backups and Testing

Cost: Medium	Complexity: Low	Fraud Effectiveness: High

What it means: Keeping regular copies of important business data (invoices, customer records, financial data) somewhere separate from your main systems, so you can recover if something goes wrong.

Why it matters: If ransomware locks your systems, or a laptop is lost, stolen or damaged, a tested backup is the difference between a short interruption and losing the data your business runs on.

What your business should do:

- Follow the simple "3-2-1" rule: 3 copies of data, on 2 different storage types, with 1 copy offsite or offline (for example a cloud backup option).
- Use an affordable cloud backup service, or the backup features already included in Microsoft 365 or Google Workspace.
- Most importantly, test that you can restore from backup at least twice a year - an untested backup is not a reliable backup.

ESSENTIAL CONTROL 06

6. Software & Device Updates

Cost: Low	Complexity: Low	Fraud Effectiveness: High

What it means: Keeping computers, phones and software (operating systems, browsers, accounting/POS software) up to date.

Why it matters: Most malicious software exploit known weaknesses the software provider has already fixed - the victim simply had not installed the update. This is one of the cheapest, easiest controls available.

What your business should do:

- Turn on automatic updates for all computers, phones and business software. In larger organisations, a more structured and controlled approach is recommended.
- Keep a list of the devices and software your business relies on so nothing is missed.
- Replace or retire devices too old to receive security updates.

ESSENTIAL CONTROL 07

7. Email & Endpoint Protection

Cost: Low-Medium	Complexity: Medium	Fraud Effectiveness: High

What it means: Software and email settings that automatically detect and block malicious software (malware), suspicious attachments, and spoofed emails before they reach your staff.

Why it matters: Email remains the most common way malware and phishing links reach a business, and criminals frequently spoof a company's own domain to impersonate staff. This control closes that gap automatically, rather than relying on staff catching every attempt.

What your business should do:

- Turn on the built-in spam/phishing filtering in Microsoft 365 or Google Workspace.
- Install reputable anti-malware on all computers - several South African banks offer free antimalware licences to their clients, so check with your bank before purchasing any.
- Ask your IT provider or email host to set up SPF, DKIM and DMARC - free technical settings that stop criminals spoofing your business's email domain.

ESSENTIAL CONTROL 08

8. Least-Privilege Access Control

Cost: Low	Complexity: Medium	Fraud Effectiveness: Medium

What it means: Giving each staff member access only to the systems, files and data they actually need for their job, not full access by default.

Why it matters: This limits how much damage a compromised account or a dishonest employee can do, reducing the risk from insider threats and unnecessary exposure of sensitive customer or financial data.

What your business should do:

- Give staff standard user accounts, not admin or privileged accounts, unless their role specifically requires it.
- Disable an employee's access immediately on their last working day.
- Review who has access to banking, accounting and customer data every few months, and remove access that is no longer needed.

ESSENTIAL CONTROL 09

9. Basic Incident Response Plan

Cost: Low	Complexity: Medium	Fraud Effectiveness: Medium

What it means: A simple, one-page written plan for what to do if something goes wrong - who to call, what to do first, and how to keep the business running.

Why it matters: Without a plan, businesses lose critical time during an actual incident, deciding what to do while the damage and cost grows. A basic plan turns panic into a checklist.

What your business should do:

- Write a one-page plan: who to call and what to switch off or disconnect first.
- Keep a printed copy - if ransomware locks your systems you may not be able to access a digital version.
- Know your bank's fraud hotline in advance and report suspicious payments immediately - acting within hours can sometimes stop a fraudulent transfer.

ESSENTIAL CONTROL 10

10. Third-Party & Supplier Risk Checks

Cost: Low	Complexity: Medium	Fraud Effectiveness: Medium

What it means: Basic checks on your suppliers, IT providers and software vendors who have access to your systems or data, since your security is only as strong as theirs.

Why it matters: Criminals increasingly attack SMMEs indirectly, through a trusted supplier, bookkeeper or IT provider with weaker security. This is a growing source of supply-chain attacks and payment diversion fraud.

What your business should do:

- Keep a simple list of vendors who have access to your data, systems or banking details.
- Ask key suppliers - especially your IT provider, accountant and payment processor – to confirm that they have basic security controls in place.
- Apply the same "verify by phone" rule to any supplier who asks you to change their banking details.

GRANT HUGHES
SPEAKER - AUTHOR - ADVISOR

PEOPLE | PROCESS | TECHNOLOGY
A SAFER TOMORROW

THANK YOU

FOR READING THE CYBER ESSENTIALS PLAYBOOK

My hope is that this guide has given you practical, actionable steps to make your business safer, stronger and more resilient.

Cybersecurity does not have to be complicated or expensive. Getting the basics right can make a significant difference.

Here's to a safer tomorrow.

Grant Hughes

GRANT HUGHES
SPEAKER | AUTHOR | ADVISOR



CYBERSECURITY ADVISORY | CONSULTING | TRAINING | SPEAKING

ABOUT GRANT HUGHES



Grant Hughes is a certified and experienced cyber professional who has worked across small and large, local and global organisations.

To learn more about Grant, visit www.granthughes.co.za or connect with him on LinkedIn.

www.granthughes.co.za
linkedin.com/in/grant-hughes-52196569

AFFORDABLE SECURITY FOR THE SA MARKET

Dark Risk is a South African developed third-party risk management platform, built for local businesses, with a focus on affordability, practicality and real risk visibility.

DarkRisk
Know Your Exposure.

To learn more about Dark Risk, email grant@darkrisk.io

LET'S STAY IN TOUCH

078 280 4699 | info@granthughes.co.za | www.granthughes.co.za

PRACTICAL INSIGHTS. REAL IMPACT.