GRANT HUGHES
SPEAKER - AUTHOR - ADVISOR

PEOPLE | PROCESS | TECHNOLOGY
A SAFER TOMORROW

THE RISKY BUSINESS PLAYBOOK

A PRACTICAL GUIDE TO FINDING AND FIXING THE BUSINESS PROCESSES CYBERCRIMINALS EXPLOIT

01
IDENTIFY
FIND THE REAL RISKS

02
UNDERSTAND
SEE HOW THEY'RE EXPLOITED

03
FIX
TAKE PRACTICAL ACTION

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

PRACTICAL INSIGHTS
REAL IMPACT

INTRODUCTION

A PRACTICAL GUIDE TO FINDING AND FIXING THE BUSINESS PROCESSES CYBERCRIMINALS EXPLOIT

Small businesses are attractive targets for fraud and cybercrime — not because their defences are weak, but because their processes are predictable. Criminals don't need to break into your systems if they can simply ask someone to hand over money, data, or access. These scams work by impersonating someone you trust (a supplier, an executive, a colleague, an IT technician) and creating a sense of urgency that discourages the person receiving the request from stopping to check.

This guide walks through common risky processes found in small businesses. For each one, you'll see a realistic example, an explanation of why it's risky and how criminals exploit it, and a straightforward, improved version of the process you can put in place instead.

THE ONE PRINCIPLE THAT FIXES MOST OF THESE

Almost every process below becomes safer with the same fix: add an independent verification step through a separate, pre-established channel. Never confirm a request using only the contact details supplied within the request itself — a phone number in the email, a link in the message, or the sender's name on the account. Look the contact up yourself, from a source you already trust, and check.

RISKY PROCESSES

Practical process changes that reduce fraud and cyber risk.

01 Updating vendor bank details based on a received email

RISKY PROCESS	IMPROVED PROCESS
A supplier's accounts team emails to say their bank has changed and asks that future invoices be paid to a new account.	Require the vendor to submit the request formally. Call a known, independently-sourced number for the vendor (never a number provided in the email) to verify verbally, obtain a bank confirmation letter, and independently verify that letter before updating records.

WHY IT'S RISKY, AND HOW IT'S EXPLOITED Attackers compromise or spoof a supplier's email account and send a convincing, letterhead-matched notice of a bank change. Because the request is verified using only the email itself, staff update the record and payments are silently redirected to the criminal's account — often not discovered until the real supplier chases an unpaid invoice.

02 Approving urgent payments based on an email from the CEO or an executive

RISKY PROCESS	IMPROVED PROCESS
An employee receives an email or WhatsApp that appears to be from the CEO, marked urgent and confidential, asking for an immediate payment to be made to a supplier.	Require verbal confirmation, or approval through an established workflow, for any payment request — regardless of who it appears to be from. Never rely solely on email or WhatsApp messages to authorise an urgent payment.

WHY IT'S RISKY, AND HOW IT'S EXPLOITED This is a classic Business Email Compromise (BEC) scam. Attackers impersonate a senior executive and lean on urgency and secrecy — 'don't call me, I'm in a meeting' — specifically to stop the employee from following the normal checks that would catch the fraud.

03 Changing employee payroll banking details from an email request

RISKY PROCESS	IMPROVED PROCESS
Payroll receives an email, often from an employee's personal email address, asking that their bank details be updated before the next pay run.	Require the employee to submit the request through HR's official channel, verify their identity, obtain supporting documentation, and confirm the change verbally before updating payroll.

WHY IT'S RISKY, AND HOW IT'S EXPLOITED Attackers who compromise (or spoof) an employee's personal email impersonate that employee to redirect their own salary. Because the only 'proof' is the email, the criminal simply collects the next payroll payment.

04 Purchasing gift cards or vouchers following an executive's email request

RISKY PROCESS	IMPROVED PROCESS
An employee receives an urgent email or WhatsApp message, apparently from a senior leader, asking them to buy gift cards for a client or staff reward and to send the card codes right away.	Confirm the request through a known phone number or an approved collaboration platform — not by replying to the email. Require a second person's approval before any gift cards are purchased.

WHY IT'S RISKY, AND HOW IT'S EXPLOITED This is a well-known scam because once the codes are sent, the funds are effectively untraceable and unrecoverable.

05 Making large payments with no transaction limits or approvals

RISKY PROCESS	IMPROVED PROCESS
Any staff member with payment access can process a payment of any size, with no extra sign-off required regardless of amount.	Implement payment thresholds that require multiple approvals as the transaction value increases, and use dual authorisation for all high-value payments.

WHY IT'S RISKY, AND HOW IT'S EXPLOITED Without a ceiling on what one person can approve alone, a single mistake, a single dishonest employee, or a single compromised account can result in an unlimited financial loss.

06 Resetting an employee's password based on an email request

RISKY PROCESS	IMPROVED PROCESS
IT receives an email, apparently from a locked-out employee, urgently asking for their password to be reset.	Verify the employee's identity through an approved authentication process, or a call to a known number, before resetting any credentials.

WHY IT'S RISKY, AND HOW IT'S EXPLOITED An attacker who has compromised or spoofed the employee's account can use this to hijack it, and gain access to the organisation.

07 Leaving system access active after an employee or contractor leaves

RISKY PROCESS	IMPROVED PROCESS
An employee or contractor departs, but no one formally removes their system access — it's left in place, relying on someone 'remembering' to deal with it.	Tie access removal directly to HR's offboarding checklist with a fixed deadline (e.g. same day), and review access periodically (e.g. quarterly) to catch anything missed.

WHY IT'S RISKY, AND HOW IT'S EXPLOITED A departed employee's still-active account is both an insider risk and an easy target for external attackers, who specifically look for dormant, unmonitored accounts to compromise because no one is watching them.

08 Allowing a single employee to create vendors and approve payments

RISKY PROCESS	IMPROVED PROCESS
One person in accounts is able to both set up a new vendor record and approve payments to that vendor.	Segregate duties so that different individuals create vendors, approve vendors, approve payments, and release payments.

WHY IT'S RISKY, AND HOW IT'S EXPLOITED Without segregation of duties, a single compromised or dishonest employee can create a fake vendor and pay it themselves, with no second person in a position to notice.

09 Actioning work requests sent to personal email accounts

RISKY PROCESS	IMPROVED PROCESS
A 'client' or 'manager' sends a work request to an employee's personal email address instead of their work email.	Require that all work requests be sent to a work email address. Any work request received on a personal account should be flagged immediately, not actioned.

WHY IT'S RISKY, AND HOW IT'S EXPLOITED This bypasses your company's email security filtering and monitoring entirely, and personal email offers no reliable way to verify who's really sending the message — making it a favourite route for impersonation.

GRANT HUGHES
SPEAKER - AUTHOR - ADVISOR

PEOPLE | PROCESS | TECHNOLOGY
A SAFER TOMORROW

THANK YOU

FOR READING THE RISKY BUSINESS PLAYBOOK

My hope is that this guide has given you practical, actionable steps to identify, manage and reduce risks in your business.

Every business faces risk, but with the right awareness, strategies and discipline, you can make better decisions, build a stronger, more resilient business, and create a safer tomorrow.

Here's to a stronger 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.