

# THE DIGITAL **PLAYBOOK** for Sri Lankan SMEs

---

Eight practical guides to take your business digital. Step by step, in plain language.  
No technical background needed.

Available in **English** - Sinhala - Tamil

---

# Staying **Safe** Online

You do not need to be a tech expert to protect your business online. You need to know the three things that cause 90% of all cybersecurity incidents and how to prevent them. This module is the fastest return on 45 minutes you will ever get.

~45 minutes - Do this with your whole team

**Why this matters:** A scam email that tricks your employee into sending LKR 50,000 to a fake supplier. A password breach that locks you out of your own accounts. These happen to Sri Lankan businesses every day. Most are completely preventable with basic habits.

## STEP - BY - STEP GUIDE

### 01 Use a password manager for all business accounts

Using the same password for your email, banking app, and social media means one breach unlocks everything. A password manager, Google Password Manager (built into Chrome, free) or Bitwarden (free), creates and remembers unique strong passwords for every account. You only need to remember one master password. A strong password is at least 12 characters with numbers and symbols.

Google Password Manager (free) - Bitwarden (free)

MODULE 07 STEP 01 - USE A PASSWORD MANAGER

<p style="background-color: #ffe0e0; padding: 5px; margin-bottom: 10px;"><b>The problem - one password, everywhere</b></p> <div style="background-color: #ffe0e0; padding: 5px; margin-bottom: 5px;"> <p><b>Gmail</b> Password: yourshop123 <span style="float: right; color: red;">EXPOSED</span></p> </div> <div style="background-color: #ffe0e0; padding: 5px; margin-bottom: 5px;"> <p><b>Facebook</b> Password: yourshop123 <span style="float: right; color: red;">EXPOSED</span></p> </div> <div style="background-color: #ffe0e0; padding: 5px; margin-bottom: 5px;"> <p><b>Bank App</b> Password: yourshop123 <span style="float: right; color: red;">EXPOSED</span></p> </div> <div style="background-color: #ffe0e0; padding: 5px; margin-bottom: 5px;"> <p><b>Instagram</b> Password: yourshop123 <span style="float: right; color: red;">EXPOSED</span></p> </div> <div style="background-color: #ffe0e0; padding: 5px; margin-bottom: 5px;"> <p><b>Daraz</b> Password: yourshop123 <span style="float: right; color: red;">EXPOSED</span></p> </div> <div style="background-color: #ff4d4d; color: white; padding: 5px; text-align: center; margin-top: 10px;"> <p>One breach - everything lost</p> </div>	<p style="background-color: #e0ffe0; padding: 5px; margin-bottom: 10px;"><b>The solution - Google Password Manager</b></p> <div style="background-color: #e0ffe0; padding: 5px; margin-bottom: 5px;"> <p><b>Gmail</b> ***** <span style="float: right; color: green;">Strong</span></p> </div> <div style="background-color: #e0ffe0; padding: 5px; margin-bottom: 5px;"> <p><b>Facebook</b> ***** <span style="float: right; color: green;">Strong</span></p> </div> <div style="background-color: #e0ffe0; padding: 5px; margin-bottom: 5px;"> <p><b>Bank App</b> ***** <span style="float: right; color: green;">Strong</span></p> </div> <div style="background-color: #e0ffe0; padding: 5px; margin-bottom: 5px;"> <p><b>Instagram</b> ***** <span style="float: right; color: green;">Strong</span></p> </div> <div style="background-color: #e0ffe0; padding: 5px; margin-bottom: 5px;"> <p><b>Daraz</b> ***** <span style="float: right; color: green;">Strong</span></p> </div> <div style="background-color: #2e8b57; color: white; padding: 5px; text-align: center; margin-top: 10px;"> <p>Unique password for every account</p> </div>
---	---

You only need to remember one master password. The manager handles everything else.

*Before: one password used everywhere leaving all accounts exposed. After: unique strong password for each account*

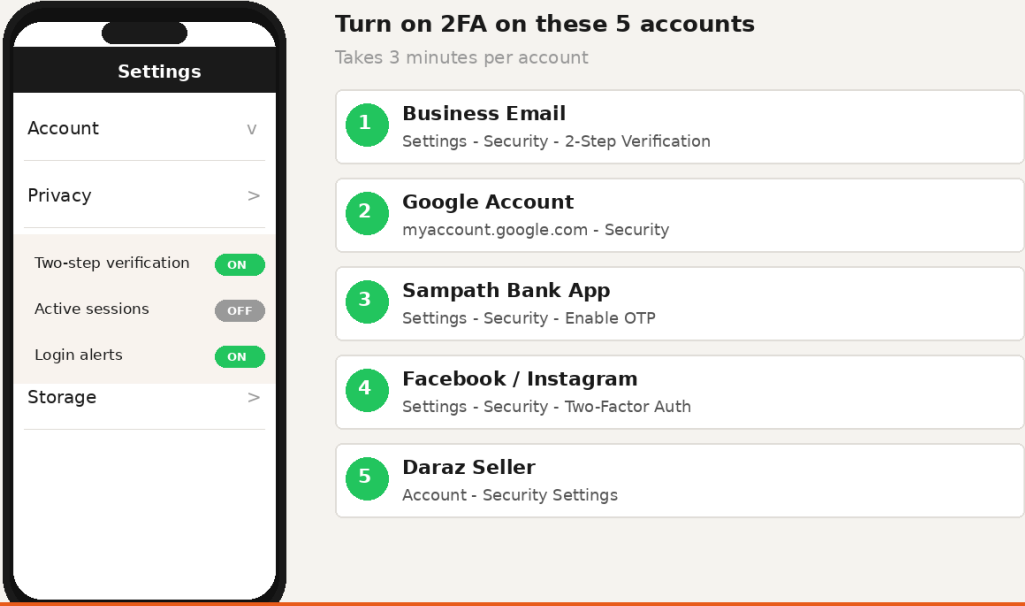
### 02 Turn on two-step verification on every critical account

Two-step verification means that even if someone steals your password, they still cannot log in without your phone. Turn it on for: your business email, Google account, banking app, and social media. On most services: Settings, Security, Two-step verification. Takes 3 minutes per account and stops most account takeovers completely.

Google Authenticator (free) - Built into most banking apps

*Tip: When you set up 2FA, write down the backup codes on paper and store them safely, not on your phone. If your phone is lost, these are your way back in.*

MODULE 07 STEP 02 - TURN ON TWO-STEP VERIFICATION



**Turn on 2FA on these 5 accounts**  
Takes 3 minutes per account

- 1 Business Email**  
Settings - Security - 2-Step Verification
- 2 Google Account**  
myaccount.google.com - Security
- 3 Sampath Bank App**  
Settings - Security - Enable OTP
- 4 Facebook / Instagram**  
Settings - Security - Two-Factor Auth
- 5 Daraz Seller**  
Account - Security Settings

Write backup codes on paper when you set up 2FA. If your phone is lost, these restore access.

*Phone settings showing two-step verification turned on and five accounts to protect*

### 03 Teach your team to spot a scam message

Phishing is when a criminal sends a message pretending to be your bank or a government body to trick you into clicking a link or sharing a password. Warning signs: extreme urgency such as Your account will be closed in 24 hours, a link that does not match the real website, or requests for your OTP by call or message. Your bank will NEVER ask for your OTP. If in doubt, hang up and call the bank directly using the number on their official website.

Rule: never share your OTP with anyone

*Tip: Share this with every person who has access to your email, banking, or social media. Most breaches start with one employee clicking a link they should not have.*

#### MODULE 07 STEP 03 - HOW TO SPOT A SCAM MESSAGE

### Real vs fake - can you spot the difference?

Criminals copy official messages exactly. Look for these warning signs.

#### SCAM - do not click

From: no-reply@sampath-bank-secure.com  
Subject: **URGENT: Verify your account NOW**

Dear Customer,  
Your account has been SUSPENDED due to suspicious activity. You must verify your details within 24 HOURS or your account will be permanently closed.

[Click here to verify NOW](#)

- xFake domain - not sampath.lk
- xExtreme urgency to pressure you
- xThreat of account closure
- xSuspicious link destination

#### REAL - safe to open

From: no-reply@sampath.lk  
Subject: **Your transaction alert**

Dear Nimal,  
A payment of LKR 4,300 was made from your account ending 4521.  
If this was not you, call us on 0800 114 114 immediately.

- ✓ Correct domain - sampath.lk
- ✓ No urgency or threats
- ✓ Gives phone number to call
- ✓ No suspicious link to click

Your bank will NEVER ask for your OTP by call or message. If unsure, hang up and call the bank directly.

*Side by side comparison of a scam email and a real bank email with warning signs labelled*

## 04 Back up your data every week

A backup is a copy of your important files stored somewhere other than your main computer. Google Drive (free up to 15GB) or a USB drive kept at a separate location are both valid options. SITS provides automated daily cloud backups with a 30-day restore window under their Command package.

Google Drive (free, 15GB) - **SITS Secure Cloud Backup**

*Tip: Set a recurring reminder every Sunday: Back up business files. Takes 5 minutes and has saved entire businesses.*

MODULE 07 STEP 04 - BACK UP YOUR DATA EVERY WEEK

### The 3-2-1 backup rule

3 copies, 2 different locations, 1 offsite

**Original + 2 backups**  
Never rely on a single copy of important data

**Computer + cloud**  
If one location fails, the other still has your data

**Cloud or USB elsewhere**  
Fire, theft or flood cannot destroy all three copies

**Back up these files every Sunday**

<b>Customer records</b>	Names, contacts, order history	Google Drive
<b>Invoices and receipts</b>	6 months minimum for loan applications	Google Drive
<b>Product photos</b>	All original images	Google Drive
<b>Accounting data</b>	Wave or Zoho export files	Google Drive
<b>Staff records</b>	EPF, contracts, payroll history	Google Drive

Set a recurring reminder every Sunday: Back up business files. Takes 5 minutes, saves everything.

*The 3-2-1 backup rule: 3 copies, 2 locations, 1 offsite - and a list of files to back up weekly*

### AFTER THIS MODULE

- ✓ Unique strong passwords on every business account
- ✓ Two-step verification protecting your critical accounts
- ✓ You and your team able to identify a scam message
- ✓ Weekly data backups running automatically or by habit

### COMMON MISTAKES

- ✗ Sharing your password with staff. Create separate accounts for each person
- ✗ Clicking links in WhatsApp messages that claim to be from your bank
- ✗ Backing up only to your phone. It can be lost or stolen too
- ✗ Ignoring software update notifications. They fix known security holes

### GLOBAL INSIGHT - SINGAPORE CYBERSG PROGRAMME

Singapore found that SMEs who completed a structured cybersecurity programme reduced their incident rate by **67% within 12 months**. The biggest factor was not the technology. It was staff awareness training. Human error caused 89% of incidents. This module directly addresses that.

