Dawgen GLOBAL

2026 EDITION



Dawgen Global illustration

CYBERSECURITY SERIES · TECHNOLOGY & CYBER

# Security Awareness & Phishing Defence

## Turn your people into your strongest defence.

Security awareness training, phishing simulations and fraud prevention programmes that change behaviour across your organisation.

**TRAIN. TEST. REINFORCE.**

01 · THE BUSINESS ISSUE

# Most attacks start with a person, not a machine.

Phishing emails, fake invoices, phone scams and messaging app fraud remain among the most common ways attackers get in. A single click or call can lead to ransomware or a fraudulent payment.

### Phishing is convincing

Modern phishing emails copy real suppliers, banks and colleagues, often using information found online.

### Payment fraud is costly

Fake payment instructions and changed bank details cause direct losses that are hard to recover.

### Annual training is not enough

A once-a-year presentation is quickly forgotten. Behaviour changes through regular practice.

### New tricks keep coming

Voice cloning, messaging apps and QR codes are now part of attackers' toolkits.

## BEHAVIOURS WE HELP BUILD

- Spotting and reporting suspicious emails
- Verifying payment and bank detail changes
- Using strong passwords and multi-factor authentication
- Handling customer and personal data safely
- Recognising phone and messaging scams
- Reporting mistakes quickly, without fear

> **The goal is not to catch people out. It is to build a culture where everyone notices, questions and reports.**

02 · OUR SERVICES

# A complete awareness programme.

We combine engaging training, realistic simulations and measurable results, tailored to Caribbean workplaces and the threats they face.

## Awareness training

Short, practical and relevant.

- Live and online sessions
- Role-based modules for finance, HR and IT
- Caribbean examples and scenarios

## Phishing simulations

Safe practice with real-world lures.

- Monthly or quarterly campaigns
- Instant feedback and micro-training
- Reporting rates measured

## Payment fraud prevention

Stopping fake payment requests.

- Finance team training
- Verification procedures
- Fraud scenario exercises

## Executive & board briefings

Leaders who set the example.

- Board cyber briefings
- Executive impersonation risks
- Leadership role in culture

## Policies & measurement

Clear rules and visible progress.

- Acceptable use and security policies
- Awareness metrics dashboard
- Annual culture survey

### WHO WE TRAIN

Staff in every sector, with tailored modules for finance teams, customer service and contact centres, hotel front desks, HR teams, executives and boards.

Training also supports data protection compliance. See our **Data Protection & Privacy Compliance** brochure.

03 · OUR APPROACH

# Baseline, train, test, measure.

Our programmes run on a 12-month calendar. We measure where you start, train and test regularly, and report progress to management and the board.

01 **Baseline**

A first phishing simulation and short survey show where you are today.

02 **Plan**

We agree a 12-month calendar of training, campaigns and communications.

03 **Train**

Short sessions and modules are delivered to staff, with role-based content for higher-risk teams.

04 **Simulate**

Regular phishing campaigns give staff safe practice, with instant feedback for anyone who clicks.

05 **Measure**

Quarterly reports show click rates, reporting rates and improvement by department.

### NO BLAME CULTURE

Results are used to improve training, never to embarrass individuals.

### WHAT WE MEASURE

- Phishing click rates
- Reporting rates
- Training completion
- Repeat behaviour

### LOCAL RELEVANCE

Scenarios use Caribbean banks, utilities, couriers and government services that staff recognise.

04 · PHISHING SIMULATIONS

# Safe practice against real-world tricks.

Phishing simulations send realistic but harmless emails to staff. Those who click receive a short lesson on the spot, and everyone learns to report suspicious messages.

### Realistic lures

Courier notices, invoices, password resets and HR messages.

### Instant learning

A short lesson for anyone who clicks.

### Reporting culture

Staff rewarded for reporting suspicious emails.

## A CAMPAIGN CYCLE

01 **Design**
Lure chosen to match current threats.

02 **Send**
Campaign delivered to agreed groups.

03 **Teach**
Micro-training for those who click.

04 **Report**
Results shared with management.

### TYPICAL RESULTS OVER 12 MONTHS

- Fewer staff clicking
- More staff reporting
- Faster reporting times
- Better finance verification

### INSURER EVIDENCE

Simulation results support cyber insurance applications and renewals.

05 · PAYMENT FRAUD PREVENTION

# Protect the payments that keep you running.

Business email compromise and fake payment requests target finance teams across the region. A few simple controls, practised regularly, stop most of these frauds.

### Controls

Procedures that stop fraud.

- Call-back verification on new bank details
- Two-person approval for large payments
- Supplier master data controls
- Urgent-request escalation rules

### Training

Finance teams who spot the signs.

- Recognising fake invoices
- Executive impersonation scenarios
- Messaging app and voice scams
- Fraud exercise with the finance team

## IF IT HAPPENS

**Act fast**

Call your bank immediately to try to stop the payment.

**Preserve**

Keep the emails and records.

**Investigate**

Our forensic team can find how it happened.

> **A two-minute phone call to verify a change of bank details is the cheapest fraud control there is.**

06 · WHO SHOULD CONSIDER THIS SERVICE

# For every organisation with people and payments to protect.

**Finance teams** handling supplier payments

**Contact centres and front desks** talking to customers every day

**HR teams** handling personal data

**Executives** targeted by impersonation

**Growing businesses** building a security culture

**Regulated entities** needing training evidence

07 · ILLUSTRATION

## A distributor cuts its phishing click rate

**Situation.** A distributor's first phishing simulation showed many staff clicking a fake courier notice, and only a few reporting it. The finance team had recently stopped a fraudulent payment by chance.

**Our work.** We ran a 12-month programme of short training sessions, monthly simulations, finance-specific fraud exercises and quarterly reports to management.

**Outcome.** Click rates fell sharply and reporting rates rose within the year, and the finance team now verifies every bank detail change by phone.

Anonymised composite illustration based on regional experience.

### WHAT YOU RECEIVE

- Baseline simulation and survey
- 12-month programme calendar
- Training sessions and modules
- Monthly phishing simulations
- Payment fraud procedures
- Quarterly progress reports

08 · ENGAGEMENT OPTIONS

# Choose the support you need.

### Awareness programme

Training and simulations over 12 months.

### Phishing simulations

Regular campaigns with reporting.

### Finance fraud workshop

Training and procedures for finance teams.

### Board briefing

Cyber awareness for directors and executives.

Fees are tailored to each organisation and agreed in the engagement letter once scope and deliverables are confirmed.

## WHY DAWGEN GLOBAL

- **Caribbean insight.** Over 24 years serving Caribbean business.
- **One desk, 35 territories.** Centrally managed from our Caribbean headquarters.
- **Certified specialists.** Offensive, defensive and forensic skills in one team.
- **Joined-up advice.** Cyber, audit, risk, legal and data protection together.

## 09 · START HERE

- Request a security awareness proposal
- Book a baseline phishing simulation
- Ask about a finance team fraud workshop

## CONTACT


**Email**
info@dawgen.global

**Web**
https://www.dawgen.global/

**Territory desks**
Write to your territory desk at *territory*@dawgen.com (for example guyana@dawgen.com). Jamaica: info@dawgen.global

**Headquarters**
Dawgen Towers, 47-49 Trinidad Terrace, Kingston 5, Jamaica


AUDIT & ASSURANCE · TAX ADVISORY · TECHNOLOGY & CYBER · FINANCE & BPO · GROWTH & RECOVERY · HR & LEGAL


This brochure provides general information only and is not professional advice. Services are provided only under a signed engagement letter. The illustration is an anonymised composite and does not describe any single client.

Dawgen Global is an independent, integrated multidisciplinary professional services firm and is not a member of any international network. As a multidisciplinary firm, Dawgen Global offers some regulated services; in each case the head of the regulated division holds the appropriate professional practice licence in the respective jurisdiction. Some regulatory services are performed by affiliated firms, and clients are advised of this when a request is made.

BIG FIRM CAPABILITIES. CARIBBEAN UNDERSTANDING. · © 2026 Dawgen Global.