

Cybersecurity essentials for revenue officers

Course outline · issued 14 September 2026

Technology areas	Cybersecurity
Level	Foundation
Short course	2 days
One-month track	4 weeks · 8 training days · 48 contact hours
Two-month track	8 weeks · 16 training days · 96 contact hours
Delivery	In person, Virtual, Hybrid
Class size	15 to 40 participants
Certification	Certificate of completion
Entry requirements	None. Intended for all staff who use agency systems.

Who it is for

All staff who handle taxpayer records or use agency systems.

REVENUE USE CASE

Tabletop exercise on a spear-phishing attempt targeting a tax office.

By the end, participants can

- Recognise phishing, social engineering and account takeover attempts
- Handle sensitive records and removable media correctly
- Report and escalate incidents promptly

Short course modules (2 days)

1. Threat landscape for revenue agencies
2. Identity, passwords and MFA
3. Safe handling of taxpayer data
4. Incident recognition and reporting
5. Tabletop exercise

One-month track — weeks 1 to 4

4 weeks · 8 training days · 48 contact hours

Week 1 — The threat landscape for revenue agencies

- Who targets tax administrations and why
- Phishing, business email compromise and fraud
- Real incident patterns in public institutions
- Your own role in the attack surface

Practical: Pull apart a set of real-world phishing samples.

Week 2 — Identity, passwords and access

- Password practice that people actually follow
- Multi-factor authentication and its bypasses
- Shared accounts and why they fail an audit
- Access reviews and leavers

Practical: Audit your own account hygiene and fix what you find.

Week 3 — Handling taxpayer data safely

- Classification: what is sensitive and what is not
- Email, removable media and printing
- Working away from the office
- Disposal and retention

Practical: Walk a real document through its full handling lifecycle.

Week 4 — Recognising and reporting incidents

- What an incident looks like from a desk
- Reporting fast and without blame
- Preserving evidence rather than tidying up
- Tabletop: a spear-phishing attempt on a tax office

Practical: Run the tabletop exercise and write the incident report.

Checkpoint: the one-month track is assessed [here](#).

Two-month track — continues through weeks 5 to 8

8 weeks · 16 training days · 96 contact hours

Week 5 — Device and application security

- Updates, patching and why delay costs
- Endpoint protection and what it misses
- Browser, extension and mobile app risk
- Approved software and shadow IT

Practical: Harden a workstation against a supplied checklist.

Week 6 — Social engineering in depth

- Pretexting, vishing and physical tailgating
- Fraud patterns around payments and refunds
- Verifying an unusual request properly
- Pressure, urgency and authority as attack tools

Practical: Run a simulated social-engineering call and debrief it.

Week 7 — Security in agency processes

- Segregation of duties in revenue processes
- Third parties, vendors and contractor access
- Business continuity and backup awareness
- Where policy and practice diverge in your unit

Practical: Map the security gaps in one real workflow in your office.

Week 8 — Capstone improvement plan

- Prioritising the gaps you found
- Making change stick in a busy office
- Briefing colleagues effectively
- Agreeing the plan with your unit head

Practical: Present the unit security improvement plan.

Capstone assessment and post-course evaluation.

Capstone

A unit-level security improvement plan: the risks that apply to this office, the behaviours to change and the escalation route, agreed with the unit head.

About this outline

Indicative extended tracks. The one-month track runs weeks 1 to 4; the two-month track continues through week 8 with deeper labs, certification preparation and a capstone. Weeks, contact hours and cohort sizes are finalised with each client.

Prepared by	Dividend Consulting Nigeria Limited
RC number	463831
Contact	0806 022 0612 · imudiagra@gmail.com
