



PROMOTING KNOWLEDGE MANAGEMENT CULTURE

Protecting NARO's Digital Identity:

Combating Impersonation, Online
Fraud and Cyber Threats



Dickson Muyomba

Speaker

Digital Media Officer

ID 894 5721 0694

Passcode 898647



**Wednesday
26 August, 2026**



**11.00 AM to
12.00 PM**



www.naro.go.ug



info@naro.go.ug

Protecting NARO's Digital Identity

Combating Impersonation, Online Fraud, and Emerging Cyber Threats



DICKSON MUYOMBA
DIGITAL MEDIA OFFICER

Impersonation – Spoofing

What is impersonation

practice where an attacker pretends to be a trusted person, brand, or organization to trick a target into sharing private data, transferring money, or granting system access

How it works

- 1. Social Engineering:**
Attackers exploit human trust rather than breaking technical firewalls.
- 2. Communication Channels:**
They send fake emails, make phone calls, or set up fake websites.
- 3. Identity Spoofing:**
They copy real logos, use similar web domains, or mimic a boss's



NARO's Digital Footprint & Assets

Our digital assets

WEBSITE

Official
information

<https://naro.go.ug>

EMAIL

Trusted
instructions

....@naro.go.ug

SOCIAL MEDIA

Public
engagement

@narouganda

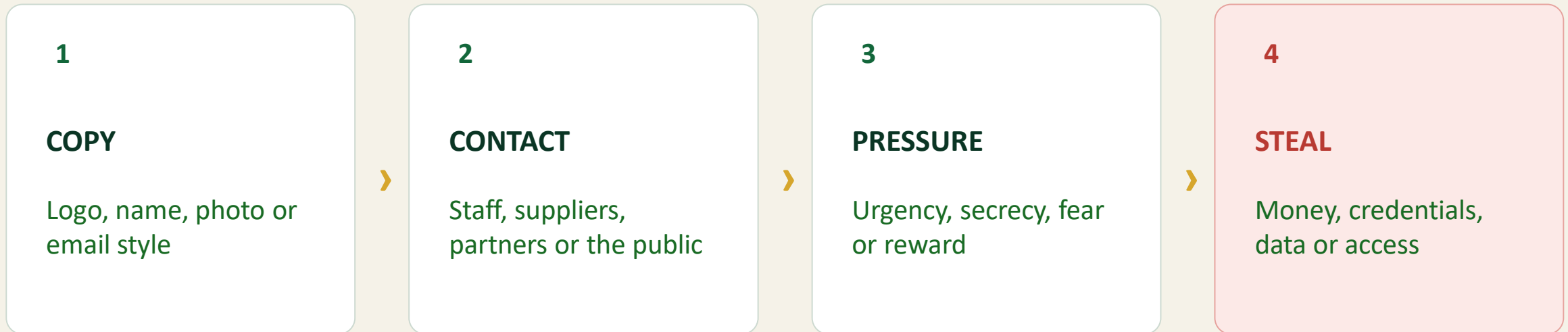
STAFF ACCOUNTS

Everyday
representation

fname.lname@naro.go.ug

When one channel compromised, attackers borrow NARO's credibility.

Turning trust into a weapon



The message may look official. The request is what must be verified.

Common threats staff may encounter

1 Fake executive message

“Buy airtime or send money urgently.”

2 Look-alike email or website

One altered letter can redirect you.

3 Hijacked social account

A real account starts sending unusual requests.

4 Bogus recruitment or tender

NARO’s name is used to collect fees or data.

5 Malicious link or attachment

A document installs malware or steals a login.

6 Supplier-payment diversion

Bank details are “changed” by email.

Spotting Phishing Tactics

Phishing remains the primary entry point for cyberattacks on government institutions

Urgency

Act now. Do not delay.

Secrecy

Do not call anyone.

Unusual value

Money, codes, passwords or data.

Check the details

- ✓ Sender address—not display name
- ✓ Domain spelling and web address
- ✓ Tone, timing and normal procedure
- ✓ Unexpected attachments or login pages

A familiar name is a reason to verify **NOT** a reason to bypass procedure.

How to response: *Pause. Verify. Report.*

1

PAUSE

Do not click, reply, pay or share.

2

VERIFY

Use a known phone number, official website or separate channel.

3

REPORT

Send the evidence quickly to the designated NARO contact.

Verification is not mistrust. It is professional discipline.

Core Safeguards for NARO Staff

01 Use unique passphrases

Never reuse a NARO password on personal or third-party services.

02 Turn on multi-factor authentication

Prefer an authenticator app or security key where available.

03 Approve logins carefully

Reject unexpected prompts and report repeated requests.

04 Keep recovery details current

Use approved organizational contacts and remove former users promptly.

Social media posts can expose more than intended

Before publishing

- ? Is this information approved for release?
- ? Does the image reveal a badge, screen, document or location?
- ? Are partners and people correctly identified?
- ? Is this the official account and device?

If an account is copied

- Capture the profile URL and screenshots
- Do not argue publicly with the impostor
- Report through the platform and NARO
- Warn affected audiences through official channels

Incident Reporting Procedures

- 1 Identify Suspicious Activity:** If you receive an unusual email asking for money or credentials, do not click links or open attachments
- 2 Contact NARO ICT Security Immediately:** Keep the email, URL, username, time, screenshots and payment details.
- 3 Isolate Affected Devices:** Disconnect your computer from Wi-Fi or Ethernet immediately if you suspect malware infection or credential compromise.
- 4 RESET** Change credentials from a clean device when instructed.
- 5 Notify SCO for Impersonation:** If fake social media accounts or fraudulent tender notices appear, inform Directorate of Communications to issue public disclaimers.

Quick check: would you act or verify?

From: “Director General” <dg.naro.office@gmail.com>

Please buy UGX 800,000 in mobile-money vouchers now. I am in a meeting—do not call. Send the codes here.

RED FLAGS

Non-official address

Urgent financial request

Secrecy

Blocks verification

Correct action: PAUSE → VERIFY through a known number → REPORT

Digital identity protection is a shared responsibility

I will...

- ☐ Protect my NARO credentials
- ☐ Verify unusual requests independently
- ☐ Publish only approved information
- ☐ Report suspicious activity immediately

Remember

PAUSE

VERIFY

REPORT

Protect our name.
Protect our people.