



Republic of the Philippines
Department of Education
REGION IV- A CALABARZON
CITY SCHOOLS DIVISION OF THE CITY OF TAYABAS

12 October 2026

DIVISION MEMORANDUM
No. 669 s. 2026

FAKE MESSAGES FROM BANKS AND GOVERNMENT OFFICE SCAMMERS

To: Assistant Schools Division Superintendent
Chief Education Supervisors
Heads, Public Elementary and Secondary Schools
Heads, Unit/Section
All Others Concerned

1. Phishing attacks impersonating banks and government agencies directly compromise DepEd operations, financial management, and data privacy rights under **Republic Act No. 10173 (Data Privacy Act of 2012)**. Scammers manipulate official authority to create urgency, bypassing basic vigilance.
2. The ICT Unit is sharing simple visual guides to help personnel use their official DepEd emails safely and professionally. These guides show personnel how to protect their accounts from scammers, follow data privacy rules, and practice good digital manners when sending messages.
3. Should there be any questions or clarification, do not hesitate to contact the ICT Unit through this communication platform: ict.tayabas@deped.gov.ph, (042) **785-9615 local 108**.
4. For immediate dissemination and compliance of all interested.


CELEDONIO B. BALDERAS JR.
Schools Division Superintendent

Encl.: As stated
Reference: DepEd Order No. 227, 2012
To be indicated in the Perpetual Index
under the following subjects:

DEPED EMAIL

OSDS-ICT- fake messages from banks and government office scammers
ICT800N5-000480/October 12, 2026

Subject: △ URGENT CYBERSECURITY ADVISORY: Fake Account Migration & Banking Phishing Scams

Attention: All DepEd Personnel

SDO DepEd Tayabas (ICT Unit) has identified active phishing campaigns targeting DepEd email accounts through fake administrative notices and fraudulent banking alerts.

The Threats

Threat 1: Internal Account Migration Scam

- **The Hook:** Deceptive emails titled "**Migration and Upgrading Accounts**" falsely claim that users must migrate their accounts, to maintain access to **Google Workspace for Education Plus**.
- **The Trap:** Recipients are directed to click a fraudulent link (portal.gmail.com) to enter their DepEd login credentials.

Threat 2: Fake Bank Security Emails

- **The Hook:** Attackers send spoofed emails pretending to be major financial institutions (e.g., Landbank, BDO, BPI). These emails allege urgent issues such as "Account Suspended," "Unusual Login Detected," or "Mandatory Security Upgrade."
- **The Trap:** The email prompts you to click a link to a fake online banking portal designed to capture your account numbers, passwords, OTPs, and personal identification information.

Critical Safeguards

DO NOT CLICK ANY LINKS OR PROVIDE YOUR CREDENTIALS. These are malicious attempts to compromise your personal information and DepEd accounts. DepEd and legitimate financial institutions will **never** ask for your password, PIN, or OTP via email or external web links.

Required Action Items

1. **Identify:** Carefully inspect email senders, embedded links, and wording to recognize phishing attempts.
2. **Report:** Do not simply delete phishing emails. Use the "**Report Phishing**" option directly within your email client interface.
3. **Notify ICT:** Capture a screenshot of the fraudulent email and forward it to **cert@deped.gov.ph**, CCing **ict.tayabas@deped.gov.ph**.
4. **Verify:** Official ICT maintenance notices and administrative updates are communicated strictly through official DepEd Memorandum channels—never via external links, unverified email domains, or generic third-party messages.

Stay vigilant and help maintain the security of our digital workspace.

DepEd Tayabas City ICT Unit

URGENT CYBERSECURITY ADVISORY: FAKE ACCOUNT MIGRATION & BANKING PHISHING SCAMS

Attention: All DepEd Personnel

Stay vigilant and help keep our digital workspace safe.

THREAT 1: INTERNAL ACCOUNT MIGRATION SCAM

Subject: Migration and Upgrading Accounts
Fake deadline: Feb 28, 2026
Target: Google Workspace for Education Plus

EVIL LINK: Fake Link (portal.gmail.com)

THREAT 2: FAKE BANK SECURITY EMAILS

Landbank Suspended
BDO
BPI Account Suspended
Account Suspended
Unusual Login Detected
Mandatory Security Upgrade

FRAUDULENT LINK: FAKE BANKING PORTAL

CRITICAL SAFEGUARDS

DO NOT CLICK LINKS OR PROVIDE YOUR CREDENTIALS!

These are malicious attempts to compromise your accounts and Legit institutions **NEVER** ask for passwords or PINs via email links.

Legit institutions **NEVER** ask for passwords or PINs via email links.

REQUIRED ACTION ITEMS

IDENTIFY: Inspect email senders, links, and wording.

REPORT: Use the "Report Phishing" option in your email client.

NOTIFY ICT: Send screenshot to cert@deped.gov.ph and CC ict.tayabas@deped.gov.ph.

VERIFY: Official notices come through DepEd Memorandum channels, NOT external links.

COMMUNICATION CHANNELS

Official DepEd Memorandums

No external links

Verified domains

[-gov.ph](https://deped.gov.ph)

DepEd Tayabas City ICT Unit