



Republic of the Philippines
Department of Education
CARAGA REGION



OCT 11 2025

REGIONAL MEMORANDUM

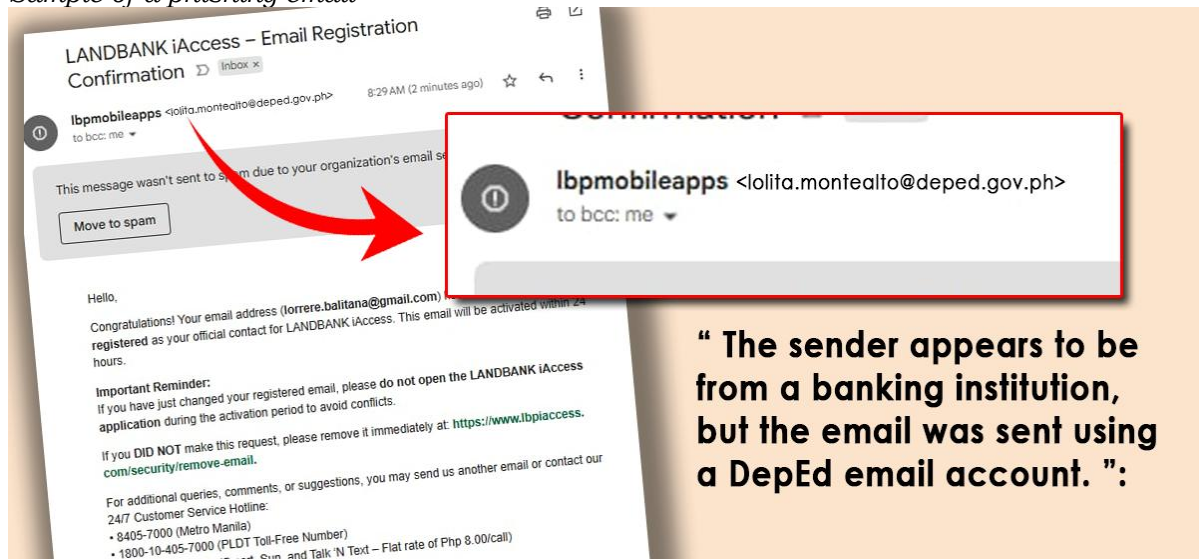
No. 1072, s. 2025

To: Schools Division Superintendent
RO Functional Division Chiefs
All DepEd Caraga Personnel
All Others Concerned

GUIDELINES ON REPORTING COMPROMISED DEPED EMAILS AND
IMPLEMENTING SECURITY MEASURES

1. In light of the increasing cyberattacks targeting DepEd personnel and government sites, this memorandum provides guidelines for reporting compromised email accounts and implementing appropriate security measures.
2. Recent incidents reveal that some emails appearing to be from legitimate banking institutions have been sent using DepEd email accounts, as shown in the sample below, asking employees to click links, provide personal information, or download files. These are fraudulent phishing emails and must be treated accordingly.

Sample of a phishing email



3. DepEd personnel who receive suspicious or unfamiliar messages must verify the sender and content before taking any action. If an email from a supposed legitimate source (e.g., a bank) originates from a DepEd email address, it must be immediately reported to the Information Technology Officer (ITO) or School ICT Coordinator for verification and appropriate action.
4. To prevent account compromise and strengthen email security, all personnel are reminded to observe the following practices:
 - Never share DepEd email credentials.



Address: J.P. Rosales Avenue, Butuan City
Trunkline No: (085) 225-1151
Telefax No: (085) 342-5959
Email: caraga@depd.gov.ph
Website: caraga.dep.d.gov.ph



Doc. Ref. Code	RO-ASD-F107	Rev	00
Effectivity	02.01.23	Page	1 of 2



- Regularly update passwords and use strong, unique passphrases.
- Enable 2-Step Verification (2SV), Two-Factor Authentication (2FA), or Multi Factor Authentication (MFA), especially for Google and Microsoft accounts.
- Regularly review account activity and immediately report any unauthorized access to your IT personnel.
- Avoid opening suspicious emails, attachments, or links, and do not download files from unverified senders.
- Always verify the sender's email address before responding.
- Log out after using shared or public computers and use incognito or private browsing mode when connected to public Wi-Fi networks to protect your identity.
- Use DepEd email strictly for official transactions and refrain from personal or non-work-related activities.

5. Personnel found intentionally engaging with or spreading phishing or malicious links may face administrative sanctions in accordance with existing DepEd policies.

6. Immediate dissemination of this memorandum is highly encouraged.


MARIA INES C. ASUNCION
 Director IV
 Regional Director

Encl.: None

Reference: None

To be indicated in the Perpetual Index
under the following subjects:

COMPUTER EDUCATION

CYBER SECURITY

ORD/mma
10/07/2025