SGOD-3556

Republic of the Philippines
Department of Education
REGION VI- WESTERN VISAYAS
**SCHOOLS DIVISION OF SAGAY CITY**

DEC 03 2024

**DIVISION MEMORANDUM**
No. 704, s. 2024

**REITERATION OF REGIONAL MEMORANDUM NOS. 1152, S. 2024 REPORTS ON PHISHING SCAMS AND ONLINE BANKING FRAUDS USING DEPED EMAIL**

To: Asst. Schools Division Superintendent
Chiefs of CID and SGOD
Public Schools District Supervisors
Schools Heads of Public Elementary and Secondary Schools
School Information Coordinators

1. This is to reiterate the attached Regional Memorandum Nos. 1152, S 2024 Reports on Phishing Scams and Online Banking Frauds Using DepEd Email which is self-explanatory.

2. The Schools Division Office (SDO) encourages all teaching and non-teaching personnel to promptly report any incidents related to phishing, fraud, or other forms of illegal banking activities that may have compromised personal information. Reports should be sent to the Information Technology Officers (ITOs) at cert@deped.gov.ph for proper documentation and immediate action.

3. Immediate dissemination and compliance of this memorandum is desired.

**MARSETTE D. SABBALUCA, CESO VI**
Schools Division Superintendent

*Enclosure :* *RM 1152, S. 2024*
*Reference :*
*Allotment :*
*No. of Pages:* _____
*To be indicate in the **Perpetual Index** under the following subjects:*
***REPORTS ON FISHING SCAMS***

*FN: /Junmarl Alconga/ Division Information Officer /SGOD*

Republic of the Philippines
Department of Education
REGION VI – WESTERN VISAYAS

NOV 15 2024

**REGIONAL MEMORANDUM**
No. 1162, s. 2024

**REPORTS ON PHISHING SCAMS AND ONLINE BANKING FRAUDS USING THE DEPED EMAIL**

To: Schools Division Superintendents
Regional Functional Division Chiefs/Unit Heads
All Others Concerned

1. Per record, this Office, through the Information and Communications Technology (ICT) Unit, has reported cases of phishing scams and online fraud involving DepEd email accounts which are fraudulent attempts of cybercriminals to trick users by impersonating as customer service representative of Landbank of the Philippines who likewise use DepEd email accounts. This modus operando result in unauthorized access to personal and banking information of DepEd personnel as shown in "***Annex A***" as sample phishing emails that appear to be from LANDBANK, Land Bank of the Philippines, or lbpiaccess@mail.landbank.com.
2. All DepEd teaching and non-teaching personnel are encouraged to report any similar incidents of phishing-related hacking or other forms of online banking fraud that may have compromised personal information to their respective Information Technology Officers (ITOs) or by sending email to cert@deped.gov.ph.

3. Attached are the ICT Cyber Safety Advisory - Information, Education, and Communication (IEC) Campaign Material, and Philippine National Police Anti-Cybercrime Group-Cyber Bulletin NR 362 titled Spotting Rouge Wi-Fi: A Guide to Enhanced Cybersecurity, for further protection, guidance, and awareness of all concerns.

4. Immediate dissemination and compliance with this Memorandum are desired.

**RAMIR B. UYTICO EdD, CESO III**
Regional Director

Encl.: As
Reference: None
To be indicated in the Perpetual Index
under the following subjects:

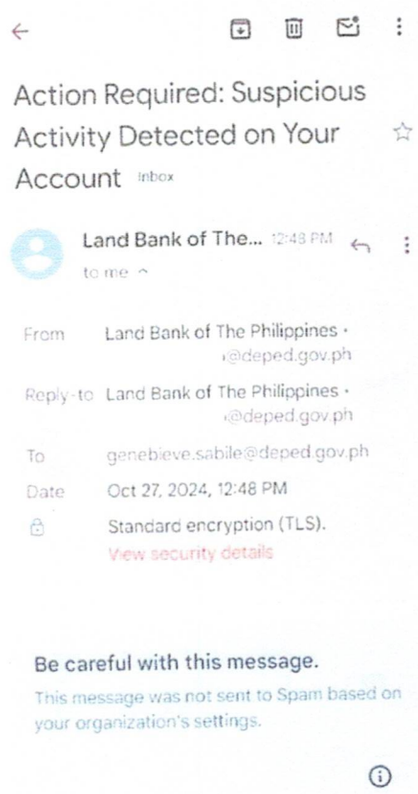
INFORMATION TECHNOLOGY
REPORTS

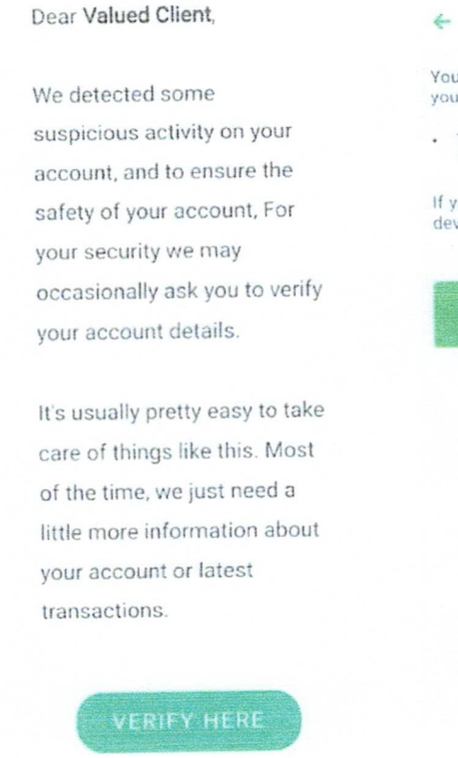


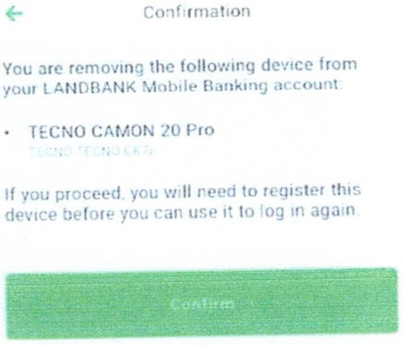
DepED MATATAG
BAGONG PILIPINAS
TUV NORD ISO 9001
Certificate No. PHP QMS 24 93 0184

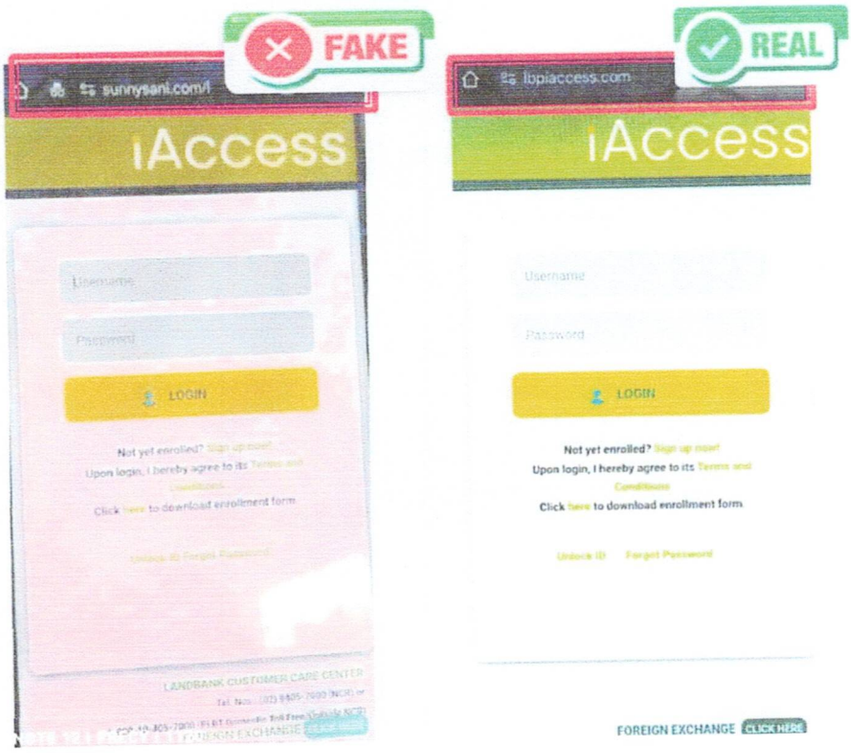
## Annex A


All inboxes
lbpiaccess@mail.landbank.
[ IMPORTANT ] Please Update Your...
Dear Valued Client,Greetings from L...
lbpiaccess@mail.landbank.
[ IMPORTANT ] Please Update Your...
Dear Valued Client,Greetings from L...


Action Required: Suspicious Activity Detected on Your Account
Inbox
Land Bank of The... 12:48 PM
to me
From Land Bank of The Philippines
Reply-to Land Bank of The Philippines
To geneblieve.sabile@deped.gov.ph
Date Oct 27, 2024, 12:48 PM
Standard encryption (TLS).
View security details
Be careful with this message.
This message was not sent to Spam based on your organization's settings.


Dear Valued Client,
We detected some suspicious activity on your account, and to ensure the safety of your account, For your security we may occasionally ask you to verify your account details.
It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account or latest transactions.
VERIFY HERE


Confirmation
You are removing the following device from your LANDBANK Mobile Banking account:
TECNO CAMON 20 Pro
If you proceed, you will need to register this device before you can use it to log in again.
Confirm

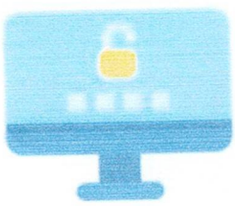

FAKE
sunnysani.com/l
iAccess
Username
Password
LOGIN
Not yet enrolled? Sign up now!
Upon login, I hereby agree to its Terms and Conditions
Click here to download enrollment form
Unlock ID Forgot Password
LANDBANK CUSTOMER CARE CENTER
FOREIGN EXCHANGE CLICK HERE
REAL
lbpiaccess.com
iAccess
Username
Password
LOGIN
Not yet enrolled? Sign up now!
Upon login, I hereby agree to its Terms and Conditions
Click here to download enrollment form
Unlock ID Forgot Password
FOREIGN EXCHANGE CLICK HERE

DepED MATATAG BAGONG PILIPINAS

ICTS

# ICT CYBER SAFETY ADVISORY

## Information and Communications Technology Service



## KEEP YOURSELF SECURED.

Please be wary of phishing and ransomware attempts which involve emails and push notifications masquerading as legitimate notifications. When clicked, these emails may collect your credentials and data that could be utilized for unlawful actions.

### IMPLEMENT STRONG PASSWORDS

Minimum of 10 characters, including uppercase, lowercase, numbers, and special characters.

### ENABLE MULTI-FACTOR AUTHENTICATION

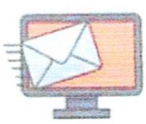
Add extra layers of security to your email and other important accounts.

### NEVER SHARE EMAIL CREDENTIALS

Keep your passwords strictly confidential. Do not share them with anyone.

### AVOID USING DEPED EMAIL IN UNSECURED LOCATIONS

Refrain from accessing your DepEd email while using public Wi-Fi networks (cafes, malls, etc.)

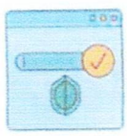


### WORK EMAIL FOR WORK ONLY

Avoid using your DepEd email address for personal online activities like online shopping, personal social media accounts, and others.

### VERIFY SENDER'S LINK

- Carefully examine the sender's email address for any irregularities.
- Hover your mouse over links to see their full address before clicking.
- Call the sender to verify your email communication.



### BE CAUTIOUS AND CONSCIOUS

Don't automatically trust emails or messages that seem strange, even if they appear to come from familiar sources.

### UTILIZE THE REPORT BUTTON

If you suspect a phishing or spam email, use your mail platform's built-in "Report Phishing" or "Report Spam" features.

For any suspicious email activity, **report immediately** to your Division IT Officer or Regional IT Officer. You may also reach out to your IT Officer to help you secure your account.

**LET'S WORK TOGETHER TO KEEP OUR DATA SECURE.**