Republic of the Philippines
Department of Education
DIGOS CITY DIVISION

DTS
1025071393

Office of the Schools Division Superintendent

DIVISION MEMORANDUM
OSDS-2025- 325

To : School Heads
Division Personnel
ICT coordinators.
Teaching and Non-Teaching Personnel

Subject : REITERATION OF RM ORD-2023-065 AND STRENGTHENING EMAIL AND SOCIAL MEDIA SECURITY

Date : October 27, 2025

Attached is Regional Memorandum ORD-2025-115, re: Reiteration of RM ORD-2023-065 and Prevention of Email Account Compromise.

In light of recent incidents involving the compromise or hacking of government Facebook pages and email accounts, this Office reminds all concerned units—including Regional Offices, Division Offices, and Schools—to ensure the security of their Facebook pages, official websites, and email accounts.

These platforms are among the most commonly used channels for disseminating information to stakeholders. Therefore, it is crucial to secure them to prevent potential breaches or unauthorized access.

Attached are recommendations on how to protect online accounts and pages. In case of a hacking incident, immediately contact your ICT Coordinator or Division Information Technology Officer for technical assistance.

For information and compliance.

MELANIE P. ESTACIO, PhD, CESO VI
Schools Division Superintendent

DepEd Schools Division of Digos City
RECORDS SECTION
RECEIVED
DATE: OCT 27 2025 TIME: 11:20 AM
BY:

Address: Roxas cor. Lopez Jaena Street, Zone II, Digos City (8002)
Telephone Nos.: (082) 553-8375; (082) 553-8396
Email: digos.city@deped.gov.ph
Website: depeddigoscity.org

RECORDS COPY

10251207 67

DTS
1025070795

Republic of the Philippines
Department of Education
DAVAO REGION
Office of the Regional Director

October 14, 2025

REGIONAL MEMORANDUM
ORD-2025-115

REITERATION OF RM ORD-2023-065 AND PREVENTION OF EMAIL ACCOUNT COMPROMISSION

To: Schools Division Superintendents
Functional Division Chiefs

1. This is to reiterate Regional Memorandum ORD-2023-065, dated August 4, 2023, on the **Prevention of Official Facebook Pages, Websites, and Email Compromission**.

2. In light of the recent incidents involving government Facebook pages and email accounts getting compromised or hacked, this Office reminds concerned offices from Regional Office, SDOs and schools to secure their official Facebook pages, official websites and email accounts.

3. Pages, websites, and emails are the most used platforms to disseminate information to stakeholders and thus, they are extremely important to be secured to prevent possible compromission or hacking.

4. Attached are recommendations on how to ensure the protection of online accounts and pages. In case of hacking, contact immediately the ICT Coordinator or Division Information Technology Officer for technical assistance.

5. For information and strict compliance.

ALLAN G. FARNAZO
Director IV

DEPARTMENT OF EDUCATION RO
RECORDS SECTION
RELEASED
BY:
DATE: Time: Oct. 16, 2025

Enclosed as stated.
ORD/ICT2/jcw

Address: F. Torres St., Davao City (8000)
Telephone Nos.: (082) 291-0051
Email Address: region11@deped.gov.ph
Website: www.depedroxi.ph

REMINDERS TO KEEP YOUR ACCOUNT SECURED:

1. **Protect your password**
   - Don't use your Facebook password anywhere else online, and never share it with other people.
   - Your password should be hard to guess, so don't include your name or common words.
   - Your password should be easy for you to remember but difficult for others to guess.
   - Your Facebook password should be different than the passwords you use to log into other accounts, like your email or bank account.
   - Longer passwords are usually more secure.
   - Your password should not be your email, phone number or birthday.
   - Avoid using common words, like "Password".
   - Use a password manager. There are many different applications that can store your passwords securely.
   - Don't share your passwords with anyone, online or in person. If you do, change them as soon as possible.
   - If you see a message letting you know the password you entered isn't strong enough, try mixing together uppercase and lowercase letters. You can also make the password more complex by making it longer with a phrase or series of words that you can easily remember, but no one else knows.

2. **Never share your login information**
   - Scammers may create fake websites that look like Facebook and ask you to log in with your email and password.
   - Always check the website's URL before you enter your login information. When in doubt, type www.facebook.com into your browser to get to Facebook.
   - Don't forward emails from Meta to other people, since they may have sensitive information about your account.

3. **How to identify suspicous emails or messages**
   If you can recognize suspicous messages or emails, then you may be able to avoid phishing scams.

4. **Emails about your account always come from:**
   - fb.com
   - facebook.com
   - facebookmail.com

5. **Never click suspicious links, even if they appear to come from a friend or a company you know:**
   If you get a suspicious email or message claiming to be from Facebook, then don't click any links or attachments.
   - This includes links on Facebook (example: on posts) or in emails.

- Keep in mind that Facebook/Meta will never ask you for your password in an email.

6. **Don't respond to these emails and don't answer messages that:**
   - Ask for your Password
   - Ask for your Social security number
   - Ask for your Credit card information
   - Demand money
   - Offer gifts
   - Threaten to delete or ban your Facebook account

7. **Log out of Facebook when you use a computer you share with other people**
   If you forget, you can log out remotely by doing the following steps:
   - Go to your Security and login settings.
   - Go to the section **Where you're logged in**. You may have to click **See more** to see all of the sessions where you're logged in.
   - Find the session you want to end. Click ⋮ and then click **Log out**.

   Clicking **Log out** will immediately log you out of Facebook on that device.

8. **Don't accept friend requests from people you don't know**
   - Scammers may create fake accounts to befriend people.
   - Becoming friends with scammers might allow them to spam your timeline, tag you in posts and send you malicious messages.

9. **Watch out for malicious software**
   - Malicious software can cause damage to a computer, server or computer network.
   - Learn the signs of an infected computer or device and how to remove malicious software.
     - **On Facebook**
       - Your account is posting spam or sending unwanted messages.
       - Strange or suspicious log in locations are appearing in your account history.
       - You see messages or posts in your activity log you don't remember sending.
     - **On your computer or mobile device**
       - Your applications run slower or tasks take longer than usual to complete.
       - You notice new applications you don't remember installing.
       - You notice strange pop ups or other ads without opening a web browser.

- **On your web browser**
  - You notice strange pop ups or other ads you don't remember seeing before.
  - Your search engine or home page has changed and you don't remember changing it.

- Keep your web browser up to date and remove suspicious applications or browser add-ons.
- Use our extra security options

10. Additional Recommendations for Securing Your Email Accounts
Since your email is often the **gateway to all your accounts**, protecting it is critical:

a. Enable Two-Factor Authentication (2FA)
- Turn on 2FA to require a code from your phone or authenticator app in addition to your password.
- Use **authenticator apps** (like Google Authenticator or Authy) instead of SMS when possible.

b. Regularly Review Account Activity
- Check recent login activity for unfamiliar devices or IP addresses.
- Sign out of devices you no longer use.

c. Set Up Recovery Options Securely
- Make sure your **recovery phone number and email** are up to date.
- Avoid using another account that you rarely access as your recovery email.

d. Be Cautious with Public Wi-Fi
- Avoid accessing your email on **public or shared Wi-Fi networks**.
- If necessary, use a **VPN** for added protection.

e. Keep Your Software Updated
- Update your email app, browser, and device regularly to protect against new security threats.

f. Don't Store Passwords in Your Inbox
- Delete emails that contain login credentials or password reset links.
- Don't forward sensitive information to your own email for "safe-keeping."

g. Beware of Phishing and Spoofing Emails
- Always check the **sender's domain** carefully.
- Watch for slight spelling changes or additional characters (e.g., @gma11.com or @out1ook.com).
- Hover over links to preview where they lead before clicking.

h. Log Out on Shared or Public Devices
- Always sign out when using a computer at work, school, or an internet café.

11. Scam emails impersonating Landbank or other banks (what to watch for and what to do) Emails pretending to be from Landbank (or any bank) are common. Treat them with extreme caution — banks will **never** ask for your full password, OTP, or PIN by email.

Common tricks used in bank impersonation emails

- Slightly altered sender addresses (e.g., landbank-notice@landbank-secure.com or support@landbänk.com).
- Urgent subject lines that pressure you to act immediately (e.g., "ACCOUNT SUSPENDED — VERIFY NOW", "UNAUTHORIZED TRANSACTION — ACTION REQUIRED").
- Fake links that look like the bank's site but lead to phishing pages.
- Requests to confirm online banking credentials, one-time passwords (OTPs), card numbers, or to authorize fund transfers.
- Attachments that contain malware (e.g., fake transaction receipts, forms).
- Promises of refunds, loan approvals, or "account upgrades" asking you to click a link.

Example suspicious subject lines (do not click or reply):

- "Landbank Notice: Immediate Account Verification Required"
- "Unusual activity detected on your Landbank account — confirm now"
- "Landbank Refund — Click here to claim"
- "Final Notice: Account will be closed if you do not verify"

How to verify if an email is real

1. **Don't click any link** in the email.
2. Hover over the link to preview the URL — check carefully for misspellings or unusual domains.
3. Open a new browser window and go to the bank's official website (type the URL yourself) or use the bank's official app.
4. Call the bank using the **official phone number** listed on the bank's website or on your bank card (do not use any phone number inside the suspicious email).
5. If the email claims to be from Landbank, use the contact information published on Landbank's official website to confirm.

Immediate actions if you clicked a suspicious link or entered details

- Change your email password and the password for your bank/finance accounts immediately.
- If you entered an OTP, password, or card details — contact your bank **right away** and inform them of possible compromise.
- Check recent transactions for unauthorized activity and report any suspicious charges.
- Scan your device with a reputable antivirus app and remove any detected malware.

How to report and block

- Mark the email as **phishing** or **spam** in your email provider so it's blocked and investigated.

- Forward the suspicious message to your bank's official fraud or phishing reporting channel (find the bank's official reporting email or hotline on their website). **Do not** forward it to addresses you find in the suspicious email itself.
- Consider reporting the scam to local cybercrime or consumer protection authorities if you lost money or sensitive information.

Preventive measures specific to bank-related scams

- Never provide your **OTP, full passwords, or PIN** to anyone. Banks will not ask for this via email.
- When setting up bank notifications, enable **transaction alerts** to your phone so you are notified immediately of withdrawals or transfers.
- Use strong, unique passwords for online banking and enable 2FA where available.
- Keep your primary email account extra secure since password resets often go through email.

Please visit the following links for more recommendations on how you can ensure the protection of your accounts, pages and websites.

1. Keeping your Facebook account and pages secure:
   https://www.facebook.com/help/235353253505947

2. Keeping your websites secure:
   https://www.cisa.gov/news-events/news/website-security

For further assistance, SDOs and RO can report to their respective IT officers.

Republic of the Philippines

Department of Education

DAVAO REGION

Office of the Regional Director

REGIONAL MEMORANDUM
ORD-2023-065

To : Assistant Regional Director
Schools Division Superintendents
Chiefs of Functional Divisions

Subject : ADVISORY ON THE PREVENTION OF OFFICIAL FACEBOOK PAGES AND WEBSITES COMPROMISSION

Date : August 4, 2023

In light of the recent incidents involving Government Facebook pages getting compromised or hacked, this Office would like to remind all concerned offices from regional office, schools division offices and schools to secure their official Facebook pages and official websites.

Facebook pages and websites are the most used platforms to disseminate information to stakeholders and thus, it is extremely important to secure the said platforms to prevent possible compromission or hacking.

Attached are recommendations on how to ensure the protection of online accounts and web pages. In case of hacking, please contact immediately the ICT Coordinator or Division Information Technology Officer for technical assistance.

For information and strict compliance.

ALLAN G. FARNAZO
Director IV

Enclosed: As stated.

ORD/ICT2/pch

DEPARTMENT OF EDUCATION R...
RECORDS SECTION
RELEASED
BY:
Date: Aug. 04, 2023

By the Authority of the Regional Director:

8/4/2023
MARILYN B. MADRAZO, EdD.
Chief, PRO
Officer-in-Charge

REMINDERS TO KEEP YOUR ACCOUNT SECURED:

1. **Protect your password**
   - Don't use your Facebook password anywhere else online, and never share it with other people.
   - Your password should be hard to guess, so don't include your name or common words.
   - Your password should be easy for you to remember but difficult for others to guess.
   - Your Facebook password should be different than the passwords you use to log into other accounts, like your email or bank account.
   - Longer passwords are usually more secure.
   - Your password should not be your email, phone number or birthday.
   - Avoid using common words, like "Password".
   - Use a password manager. There are many different applications that can store your passwords securely.
   - Don't share your passwords with anyone, online or in person. If you do, change them as soon as possible.
   - If you see a message letting you know the password you entered isn't strong enough, try mixing together uppercase and lowercase letters. You can also make the password more complex by making it longer with a phrase or series of words that you can easily remember, but no one else knows.

2. **Never share your login information**
   - Scammers may create fake websites that look like Facebook and ask you to log in with your email and password.
   - Always check the website's URL before you enter your login information. When in doubt, type www.facebook.com into your browser to get to Facebook.
   - Don't forward emails from Meta to other people, since they may have sensitive information about your account.

3. **How to identify suspicous emails or messages**
   If you can recognize suspicous messages or emails, then you may be able to avoid phishing scams.

4. **Emails about your account always come from:**
   - fb.com
   - facebook.com
   - facebookmail.com

5. **Never click suspicious links, even if they appear to come from a friend or a company you know:**
   If you get a suspicious email or message claiming to be from Facebook, then don't any links or attachments.
   This includes links on Facebook (example: on posts) or in emails.

- Keep in mind that Facebook/Meta will never ask you for your password in an email.

6. **Don't respond to these emails and don't answer messages that:**
   - Ask for your Password
   - Ask for your Social security number
   - Ask for your Credit card information
   - Demand money
   - Offer gifts
   - Threaten to delete or ban your Facebook account

7. **Log out of Facebook when you use a computer you share with other people**
   If you forget, you can log out remotely by doing the following steps:

   a) Go to your Security and login settings.
   b) Go to the section **Where you're logged in**. You may have to click **See more** to see all of the sessions where you're logged in.
   c) Find the session you want to end. Click ⋮ and then click **Log out**.

   Clicking **Log out** will immediately log you out of Facebook on that device.

8. **Don't accept friend requests from people you don't know**
   - Scammers may create fake accounts to befriend people.
   - Becoming friends with scammers might allow them to spam your timeline, tag you in posts and send you malicious messages.

9. **Watch out for malicious software**
   - Malicious software can cause damage to a computer, server or computer network.
   - Learn the signs of an infected computer or device and how to remove malicious software.
     - **On Facebook**
       - Your account is posting spam or sending unwanted messages.
       - Strange or suspicious log in locations are appearing in your account history.
       - You see messages or posts in your activity log you don't remember sending.
     - **On your computer or mobile device**
       - Your applications run slower or tasks take longer than usual to complete.
       - You notice new applications you don't remember installing.
       - You notice strange pop ups or other ads without opening a web browser.

- **On your web browser**
  - You notice strange pop ups or other ads you don't remember seeing before.
  - Your search engine or home page has changed and you don't remember changing it.
- Keep your web browser up to date and remove suspicious applications or browser add-ons.
- Use our extra security options

Please visit the following links for more recommendations on how you can ensure the protection of your accounts, pages and websites.

1. Keeping your Facebook account and pages secure:
   https://www.facebook.com/help/235353253505947/?helpref=hc_fnav
2. Keeping your websites secure:
   https://www.cisa.gov/news-events/news/website-security