



Republic of the Philippines
Department of Education
Region XI
SCHOOLS DIVISION OFFICE OF DAVAO ORIENTAL

Office of the Schools Division Superintendent
No. 095, s. 2025

OCT 23 2025

MEMORANDUM

To : **SGOD and CID Chief
Public Schools District Supervisor
Public School Heads
Teachers
All Others Concerned**

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

Date : 20, October 2025

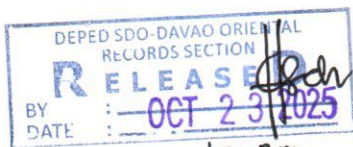
1. This is to reiterate **Regional Memorandum ORD-2023-065**, dated August 4, 2023, on the **Prevention of Official Facebook Pages, Websites, and Email Compromission.**

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.

For information and compliance



1:45 P.M

DR. JOSEPHINE L. FADUL
Schools Division Superintendent



Address: Government Center, Dahican, Mati City
Contact No.: (087) 388-3372
Email Address: davao.oriental@deped.gov.ph
Official Website: <https://depeddavor.com/>

"Where the Sunrise Beckons the Sweetest Smile"



Republic of the Philippines
Department of Education
Region XI
SCHOOLS DIVISION OFFICE OF DAVAO ORIENTAL

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 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 change them as soon as possible.
- If you see a message letting you know the password you entered isn't strong enough, try mixing 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 suspicious emails or messages

If you can recognize suspicious 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



Address: Government Center, Dahican, Mati City
Contact No.: (087) 388-3372
Email Address: davao.oriental@deped.gov.ph
Official Website: <https://depeddavor.com/>

"Where the Sunrise Beckons the Sweetest Smile"



Republic of the Philippines
Department of Education
Region XI
SCHOOLS DIVISION OFFICE OF DAVAO ORIENTAL

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 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 account history.
- You see messages or posts in your activity log you 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.



Republic of the Philippines
Department of Education
Region XI
SCHOOLS DIVISION OFFICE OF DAVAO ORIENTAL

- 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-keep"

g. Beware of Phishing and Spoofing Emails

- Always check the sender's domain carefully.
- Watch for slight spelling changes or additional characters (e.g., @gmail.com or @outlook.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.



Republic of the Philippines
Department of Education
Region XI
SCHOOLS DIVISION OFFICE OF DAVAO ORIENTAL

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@landbanksecure.com or support@landbank.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.



Republic of the Philippines
Department of Education
Region XI
SCHOOLS DIVISION OFFICE OF DAVAO ORIENTAL

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 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 website secure:
<https://www.cisa.gov/news-events/news/website-security>

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



Address: Government Center, Dahican, Mati City
Contact No.: (087) 388-3372
Email Address: davao.oriental@deped.gov.ph
Official Website: <https://depeddavor.com/>

"Where the Sunrise Beckons the Sweetest Smile"