



Republic of the Philippines  
**Department of Education**  
REGION XI  
SCHOOLS DIVISION OF DAVAO DEL NORTE

**Office of the Schools Division Superintendent**

DIVISION MEMORANDUM  
No. 0315, s. 2023

To: Chief Education Program Supervisor, School Governance and Operation Division  
Chief Education Program Supervisor, Curriculum Implementation Division  
Public Schools District Supervisors  
School Principals/Heads  
All others concerned

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

Date: August 8, 2023

Attached herewith is the Regional Memorandum ORD-2023-065 dated August 4, 2023, from the Office of the Regional Director of DepEd Region XI, on the **Advisory on the Prevention of Official Facebook Pages and Websites Compromission**.

This is to remind all concerned offices from the division office and schools to secure their official Facebook pages and official websites.

Enclosed 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.

  
**REYNALDO B. MELLORIDA, CESO V**  
Schools Division Superintendent



OSDS/pea





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 *A. - 3*

Enclosed: As stated.

ORD/ICT2/pch

DEPARTMENT OF EDUCATION REGIONAL OFFICE  
 RECORDS SECTION  
**RELEASED**

By: *[Signature]*  
 Date: *Aug 04, 2023*

By the Authority of the Regional Director:

*[Signature]* 8/4/2023  
**MARILYN B. MADRAZO, EdD.**  
 Chief, PPRO  
 Officer-in-Charge





Republic of the Philippines  
**Department of Education**  
DAVAO REGION

Office of the Regional Director

**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](http://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](http://fb.com)
- [facebook.com](http://facebook.com)
- [facebookmail.com](mailto: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.



Republic of the Philippines  
**Department of Education**  
DAVAO REGION


**Office of the Regional Director**

- 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.
  - o **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.
  - o **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.





Republic of the Philippines  
**Department of Education**  
DAVAO REGION

---

**Office of the Regional Director**

- **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](https://www.facebook.com/help/235353253505947/?helpref=hc_fnav)
2. Keeping your websites secure:  
<https://www.cisa.gov/news-events/news/website-security>

