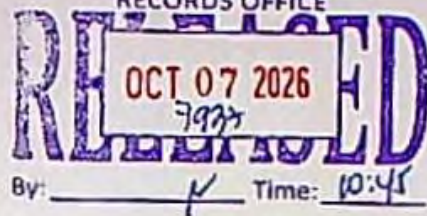




Republic of the Philippines
Department of Education
REGION I
SCHOOLS DIVISION OF DAGUPAN CITY

DepEd SDO Dagupan City
RECORDS OFFICE



Office of the Schools Division
Superintendent

October 7, 2026

OFFICE MEMORANDUM
OSDS-2026-02

**OFFICE NOTICE ON THE WEBSITE SECURITY INCIDENT AND SECURITY
MEASURES UNDERTAKEN FOR THE SDO DAGUPAN CITY OFFICIAL
WEBSITE**

To: Assistant Schools Division Superintendent
Chief Education Supervisors
Public Schools District Supervisors
Non-Teaching Personnel
Others Concerned

1. The ICT Unit hereby informs all concerned personnel of a website security incident involving the official website of the Schools Division Office (SDO) Dagupan City at <https://depeddagupan.com/>.

2. The incident was reported by the Department of Information and Communications Technology (DICT), through the National Computer Emergency Response Team (NCERT), based on information gathered through Open Source Intelligence (OSINT). NCERT identified an unauthorized modification or website defacement involving the SDO Dagupan City website. In particular, an unauthorized webpage displaying the message "hacked by trenggalek6etar" was identified under the affected website.

3. The details communicated by NCERT are as follows:

Asset Name: depeddagupan.com
Affected Asset: depeddagupan.com/cox.html
IP Address: 162.241.225.36
ASN: AS31898
Identified Threat Actor: trenggalek6etar

4. The reported incident indicates a possible compromise of the website and unauthorized modification of its contents. The Information Technology Officer immediately undertook appropriate measures to assess and address the reported security concern.



Republic of the Philippines
Department of Education
REGION I
SCHOOLS DIVISION OF DAGUPAN CITY

**Office of the Schools Division
Superintendent**

5. **Actions Undertaken by the ICT Unit:**

On September 29, 2026, the ICT Unit observed recurring errors when accessing the Division website, including HTTP 404 (Not Found) and HTTP 403 (Forbidden) errors. This prompted the ICT Unit to conduct security system scan for appropriate security assessment and mitigation.

Subsequently, the Information Technology Officer conducted a malware scan and identified infected file paths in the website's file system, as indicated in the scanreport.txt generated through the hosting control panel.

6. **Following the findings, the Information Technology Officer immediately undertook the following measures:**

- a. Conducted an assessment and evaluation of the website's existing security controls, including the status of HTTPS and SSL configuration;
- b. Scanned and cleaned the identified infected file paths to remove potentially malicious or unauthorized files;
- c. Changed the password credentials of backend users to prevent unauthorized access through compromised credentials;
- d. Reviewed and verified the roles and access privileges of all backend users to ensure that only authorized personnel have appropriate access; and
- e. Verified that the login page and backend administrative interface are not publicly accessible and that appropriate access restrictions are in place.

7. **At present, the SDO Dagupan City official website is accessible from both front-end and back-end interfaces. The ICT Unit continues to conduct periodic security scans, monitoring, and assessment of the website to detect and address any recurring errors, malicious files, unauthorized modifications, or other potential security threats.**

The ICT Unit is also reviewing and strengthening the website's security configuration in accordance with the recommendations provided by DICT-NCERT, including regular vulnerability and malware scanning, system and CMS updates, monitoring of system logs, review of user accounts and access privileges, and other appropriate website security hardening measures.

8. **All personnel with access to the Division website or its administrative/backend systems are reminded to observe proper cybersecurity practices, such as:**

To keep account credentials confidential and do not share passwords with other persons;



Republic of the Philippines
Department of Education
REGION I
SCHOOLS DIVISION OF DAGUPAN CITY

Office of the Schools Division
Superintendent

To use strong and unique passwords and change them immediately when compromise is suspected;

To immediately report any suspected unauthorized access or security incident to the ICT Unit;

To access administrative systems only through authorized devices and networks;

To report suspicious login attempts, unauthorized changes, unusual system behavior, or other cybersecurity incidents immediately to the ICT Unit; and

To regularly monitor uploaded issuances on the Division Website, as email push notifications have been decommissioned as part of the security measures implemented by the ICT Unit.

9. Immediate and widest dissemination of the contents of this memorandum is desired.


MARCIANO U. SORIANO JR. PhD, CESO VI
Assistant Schools Division Superintendent
Officer-In-Charge
Office of the Schools Division Superintendent



Reynante Infante <reynante.infante@depd.gov.ph>

[TLP:Amber + Strict]: NCERT Ticket#14878 - Department of Education - Dagupan City - Website Defacement

6 messages

National Computer Emergency Response Team <ncert@dict.gov.ph>
To: reynante.infante@depd.gov.ph
Cc: monitoring <monitoring@ncert.gov.ph>

Tue, Oct 6, 2026 at 11:08 AM

TLP: AMBER + STRICT

Recipients may only share TLP: AMBER + STRICT information with members of their own organization who need to know the information to protect themselves or prevent further harm

Greetings!

We are the Philippine National Computer Emergency Response Team under the Cybersecurity Bureau of the Department of Information and Communications Technology Office (DICT), which is mandated to provide proactive government countermeasures to address and anticipate all domestic and transnational incidents affecting the Philippine cyberspace and any cybersecurity threats to the country.

Through the application of Open Source Intelligence (OSINT), NCERT, has identified a website defacement incident that may significantly impact the integrity of Critical Information Infrastructure (CII). In this event, a threat actor illicitly modified the official website of the Department of Education - Dagupan City by introducing unauthorized content. Upon checking the official website, NCERT observed an unauthorized webpage displaying the message "hacked by tronggalek6etar." The presence of this unauthorized content is indicative of a possible compromise and website defacement, and may indicate activity associated with a threat actor.

Event Details

Asset Name: hxxps://depddagupan[.]com/
Affected Asset: hxxps://depddagupan[.]com/cox.html
IP Address: 162.241.225.36
ASN: AS31898
Threat Actor: tronggalek6etar

Please see the attached screenshot showing the defaced website for your reference.

Additionally, NCERT recommends the following:

- Immediately remove the defaced website from public access or redirect to a maintenance page.
- Conduct a thorough assessment of the current state of data security within the infrastructure and a comprehensive evaluation of the website.
- Verify and remove any changes made by the threat actor if any modifications or added entries exist.
- Disable remote administrative access until proper authentication is ensured.
- Secure and preserve server logs, web application logs, and firewall/IDS/IPS logs for forensic review.
- Check the user lists for any suspicious or unauthorized user(s) that may have been added. If there are added unknown user(s), immediately delete the account(s).
- Confirm if the login page, the directory and its contents should not be publicly accessible. If so, check the configuration of your server and set restrictions to prevent public access.
- Ensure all resources only contain user(s) that is/are authorized to access, including their roles.
- Ensure that the installed Content Management System (CMS) and other technologies used are regularly updated in its latest versions and enhance the overall security configuration of identified critical systems such as enabling HTTPS/TLS encryption on websites.

For security hardening:

- Enable Web Application Firewall as this will automatically screen web requests and will help in filtering cyber-attacks on web servers.

- Use a dedicated file upload folder. Instead of allowing users to upload files to any location on your site, create a dedicated folder for file uploads. This will help to prevent users from uploading malicious files to important areas of your site.
- Website directories not intended for public consumption should disable the use of HTTP.
- Ensure that the installed Content Management System (CMS) and other technologies used are regularly updated in its latest versions and enhance the overall security configuration of identified critical systems such as enabling HTTPS/TLS encryption on websites
- Install a security plugin: For this can help to block malicious file uploads and alert you if any suspicious activity is detected on your site.
- Enable Web Application Firewall as this will automatically screen web requests and will help in filtering cyber-attacks on web servers.
- Regularly scan your website for vulnerabilities and malware using reliable security tools and ensure that the system is configured securely, and all sites are running the latest security patches to address known vulnerabilities in the software.
- Regularly monitor system logs for any suspicious activity, such as failed login attempts or unauthorized access attempts. This can help detect potential security threats before they become a major issue.

We have assigned the incident as Ticket#14878 and this will be kept open until the necessary actions have been conducted. Furthermore, NCERT will also be providing a signed Incident Notification Report regarding this incident for proper documentation and reference.

Please be informed that your internal security team can re-assess and re-confirm the detected threat/vulnerability to verify and to tag the incident as a false positive or true positive for further investigation.

We look forward to your immediate response and cooperation. Please expect to hear from us again for a follow-up regarding this matter. Should you require further assistance, do not hesitate to contact us at ncert@dict.gov.ph or 920-0101 local 1708 and 2501.

Please acknowledge receipt of this message. If you are not the right personnel to handle this issue, please forward this to the appropriate office in your organization.

Regards,

—

Annabelle E. Pillado, RCrim
Incident Response Section
Cybersecurity Bureau, Department of Information & Communications Technology
Address: 49 Don A. Roces, Diliman, Quezon City

Disclaimer: The information contained in this communication is intended solely for the use of the individual or entity to whom it is addressed and other parties authorized to receive it. It may contain confidential or legally privileged communication. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this information is strictly prohibited and may be unlawful. If you have received this communication in error, please notify us immediately by responding to this e-mail and then immediately delete it from your system. Opinions contained in this e-mail or any of its attachments do not necessarily reflect the opinions of the Department of Information and Communications Technology (DICT).



Screenshot 2026-10-06 091026.png
53K



Screenshot 2026-10-06 091026.png

Open with ▾



depeddagupan.com/cox.html

hacked by trenggalek6etar

- JATIM4U -

Jangene_Cakep - Panataran - 0x1999 - 0xIDiot - Unlucky - Mr.Optimuz_Root

National Computer Emergency Response Team <ncert@dict.gov.ph>
To: reynante.infante@deped.gov.ph

Tue, Oct 6, 2026 at 11:11 AM

Additionally, please find attached the Incident Response Playbook, which provides recommended actions and guidance to help mitigate the website defacement incident.



Disclaimer: The information contained in this communication is intended solely for the use of the individual or entity to whom it is addressed and other parties authorized to receive it. It may contain confidential or legally privileged communication. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this information is strictly prohibited and may be unlawful. If you have received this communication in error, please notify us immediately by responding to this e-mail and then immediately delete it from your system. Opinions contained in this e-mail or any of its attachments do not necessarily reflect the opinions of the Department of Information and Communications Technology (DICT).

[Quoted text hidden]



Incident Response Playbook - COMPROMISED SYSTEM Web Application (CMS) via Web Defacement - Deped Dagupan City.docx
4936K

Reynante Infante <reynante.infante@deped.gov.ph>
To: National Computer Emergency Response Team <ncert@dict.gov.ph>

Tue, Oct 6, 2026 at 12:42 PM

Acknowledged receipt of this email.

Thank you.

Reynante B. Infante
Information Technology Officer I
Department of Education - Dagupan City

Community Manager
Google Educators Group - Dagupan City



You may also follow me at:

facebook
+google
@reynanteinfante

[Quoted text hidden]

Reynante Infante <reynante.infante@deped.gov.ph>
To: National Computer Emergency Response Team <ncert@dict.gov.ph>

Tue, Oct 6, 2026 at 12:45 PM

Thank you for reaching out to us for the said web incident.

Last September 29, 2026, we noticed a recurring error in our website, whenever we access the said site, error 404 or error 403 appears. This prompted us to check-in with the hosting site for appropriate security measures. The hosting site conducted a malware scan and found out that there are some infected file path, "The infected file path will be listed in file manager >> scanreport.txt file".

The ICT unit immediately conducted the following steps:

1. Conducted assessment and evaluation of the current data security in place for the website, such as enabling HTTPS and updating of SSL;
2. Scanned and cleaned the infected file path;
3. Change password credentials for back-end users;
4. Checked the roles of every back-end user;
5. Ensured that the log-in page is not publicly accessible

At present, the division website is accessible both from front and back ends. We are still conducting periodical scans for possible errors.

Thank you very much.

Reynante B. Infante
Information Technology Officer I
Department of Education - Dagupan City

Community Manager
Google Educators Group - Dagupan City



You may also follow me at:
facebook
+google
@reynanteinfante

[Quoted text hidden]

Reynante Infante <reynante.infante@deped.gov.ph>
To: National Computer Emergency Response Team <ncert@dict.gov.ph>

Tue, Oct 6, 2026 at 1:24 PM

also, the depeddagupan.com/cox.html is now deleted from the file manager and we have installed plugins such as ALOS, Malcare and Wordfence for added security.

Thank you.

Reynante B. Infante
Information Technology Officer I
Department of Education - Dagupan City

Community Manager
Google Educators Group - Dagupan City



You may also follow me at:
facebook
+google
@reynanteinfante

[Quoted text hidden]

National Computer Emergency Response Team <ncert@dict.gov.ph>
To: Reynante Infante <reynante.infante@deped.gov.ph>

Tue, Oct 6, 2026 at 1:47 PM

This is to acknowledge the receipt of the actions taken and express gratitude for your prompt response and continuous cooperation with NCERT in addressing this matter

Please be informed that the information given by your team will be documented. And with this information, we will now be closing the assigned ticket number **NCERT#14978** and will tag this incident as "Resolve and Remediated" for this incident.

We would like to ask for your feedback by filling up this form: <https://forms.gle/zyqpM3jCvNewADs5> to help us serve you better.

Should you require further assistance, do not hesitate to contact us at ncert@dict.gov.ph or 920-0101 local 1708 and 2378.

Thank you so much and God Bless!

Regards,
Annabelle E. Pillado, RCrim
Incident Response Section
Cybersecurity Bureau, Department of Information & Communications Technology
Address: 49 Don A. Roces, Diliman, Quezon City