ACADEMIC UPDATE ON CYBERSECURITY AND DATA PRIVACY POLICIES FOR DEPED EMPLOYEE AND LEARNER EMAIL ACCOUNTS

by:
Richard M. Alboro
Information Technology Officer I

The Department of Education has made significant moves supposed to offer cybersecurity and data privacy protection for its stakeholders mainly employees and students through specially designed email systems. The fast pacing towards the adoption of digital technologies in education instantly created a need for adequate cybersecurity policies and controls. These policies form a nucleus for mitigating vulnerabilities and protecting sensitive information, thereby creating a safe and secure digital environment. These provide requirements for the protection of personal and sensitive data under the Data Privacy Act of 2012 (RA 10173). Employee and learner email accounts hold strict confidentiality and integrity protocols with regards to unauthorized access, disclosure, or misuse.

Information acquired and directed by DepEd is pursuant to informed consent; practices relating to collection and use of information are transparent. Only authorized users-students, teachers, or staff-receive DepEd email accounts, specifically for personal and academic purposes to preclude data compromise. All DepEd accounts shall be enabled with 2FA, or another layer of security when it would require a secondary step for verification for an account to pass. Passwords are complex and are regularly changed; policies are also enforced by recommending to use secure password management tools. Peoples' access is governed based on job needs. Accesses to these accounts that resulted in unauthorized attempts are monitored.

Despite all these protocols, incidents already surfaced showing that cyber threats really possess stalwart characteristics. Cases were observed where phishing e-mails have been targeting DepEd accounts where primary objectives were credentials acquisition or malware installation. Very few unique cases were noted where the unauthorized access attempts by intruders have had to be addressed right away. In some cases, misconfigurations of email settings inadvertently resulted in the unintentional exposure of data prompting the reassessment of email controls and configurations.

DepEd has developed proactive approaches in countering these incidents through Incident Response Plan or IRP, awareness, and training, security audits, vulnerability assessments, and in collaboration with Cybersecurity Organizations and Agencies. An organized IRP clearly identifies which actions will be taken on breaches such as isolating, investigating, and recovering to minimize damage. Cyber training of all DepEd personnel and students would improve sensitivity about suspicious activities and phishing. System audits usually look for and correct vulnerabilities in the email system as identified by best practices and emerging threats. Support of DepEd with cybersecurity agencies strengthens defenses, shared threat intelligence, and engages rapidly against emerging threats.

Commitment to data privacy and cybersecurity of its email platforms further protected the sensitive information of the employees and learners through DepEd. Continuous refinement of policies, strengthening of counter strategies, and data privacy are vital if DepEd is to be able to better face the potential threats that may face such a learning platform.

References:

Data Privacy Notice | Department of Education. (n.d.). https://www.deped.gov.ph/about-deped/data-privacy-notice/

December 3, 2012 DO 85, s. 2012 – Policy on the Establishment Of DepEd Email Service | Department of Education. (2012, December 3). https://www.deped.gov.ph/2012/12/03/do-85-s-2012-policy-on-the-establishment-of-deped-email-service/