CYBER ADVISORY

TLP:CLEAR
28 August 2024

Awareness: Phishing Campaigns Targeting Public Education Sector

Cybercriminals are conducting phishing campaigns that target the Public Education sector, a historical trend that is repeating this year. The following information will help you understand tactics cybercriminals use, steps to prevent falling victim to a phishing email, and steps to take if you think you've received a phishing email.

Tactics

Phishing emails are designed to entice the recipient into clicking on a link or opening a malicious attachment by using a relevant topic in the subject line, or to appear as being sent from someone the recipient is familiar with. Campaigns conducted against the Public Education sector often rely on a subject that is relevant with the start of the school year, such as the following:

- Important! New Student Information
- Fall Semester Scheduling
- New Student Orientation

If a cybercriminal has access to a legitimate email account within the Public Education sector, they will use it to send malicious emails from the compromised account to members of that organization, school district, county offices, or students and parents of students at the school. If you receive an unexpected email from someone that you know or from your office, always confirm with them that they sent the email and attachment. Never seek the confirmation through email, as it could be a cybercriminal providing the response.

What to do if you think you've been phished

If you think that you have received a phishing email, follow your organizations process for reporting phishing emails. Do not forward the suspected phishing email or delete it. If your organization does not have a process, notify your IT department and follow their direction.

If you have clicked a link or opened an attached file in an email that you suspect to be a phishing email, follow your organizations process for computer compromise. Remember to leave your computer on. Turning it off can prevent incident responders from being able to capture vital information related to the compromise.

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

Please send suspected phishing emails to the Cal-CSIC for investigation by performing the following steps:

1. Save the ***original*** Phishing Email as a .msg or .eml
2. Attach that file to the email they send to calcsic.phishing@caloes.ca.gov This will ensure we get the original phishing email with an intact header and body. It's very important for analysis.

The Cal-CSIC provides services to help in the event of a computer and/or network compromise. Contact us at calcsic_watch@caloes.ca.gov or 916-636-2997.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback here.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.