CENIC COVID-19 Update: Phishing Warning

CENIC Colleagues, the Systems team posted a Slack Service Desk announcement on Sunday, 3/8, regarding the Cyber Infrastructure Security Administration (CISA) warning about COVID-19 cyber scams. You can review this announcement on Slack at #servicedesk channel post from 3/8, or directly from the CISA announcement page at Defending Against COVID-19 Cyber Scams. This CISA announcement, as well as many other reputable sources, provides useful guidance on how to identify fake emails and avoid exposing your personal data due to phishing activities.

Phishing is a fraudulent attempt to electronically acquire sensitive information such as usernames, passwords, and IDs by masquerading as a trustworthy individual or entity. Some phishing attempts are very sophisticated, and the email may seem to come from someone you know.

Do NOT open attachments or links within emails from any untrusted sources and always be suspicious of any email asking for personal or user account information. The CENIC Help Desk staff will never ask you for such information via email.

Here are a few examples of what some COVID-19 phishing emails may look like, as shared by Symantec on their Coronavirus Phishing Emails warning page:

Fake CDC alert:
Fake health advice email:

Singapore Specialist : Corona Virus Safety Measures

DT

Tuesday, 28 January 2020 at 03:51

Show Details

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus. This little measure can save you.

Use the link below to download

Safety Measures.pdf

Symptoms: Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

Regards
Dr [name]
Specialist wuhan-virus-advisory

Fake workplace policy email:

All,

Due to the coronavirus outbreak, [[company_name]] is actively taking safety precautions by instituting a Communicable Disease Management Policy. This policy is part of our organizational preparedness and we require all employees to read and acknowledge the policy before [[current_date_1]].

If you have any questions or concerns regarding the policy, please contact [[company_name]]

Human Resources

Regards,
Human Resources
If you have questions or concerns about a possible phishing email, please contact the CENIC Help Desk by emailing help@cenic.org with the subject: Possible Phishing Email - Verification Assistance Needed. Additional guidance can be found on our CENIC Email Spam & Phishing Guide.

Philip Romero
Sr. Enterprise Security Architect, CENIC
promero@cenic.org
Phone: (714) 220-3430
Mobile: (562) 445-2529