National Computer Board

CERT-MU

CERT-MU Security Alert

COVID-19: Signs of Phishing Campaigns

The huge amount of news coverage surrounding the COVID-19 virus has created a new danger - phishing attacks looking to exploit public fears from this pandemic. Cybercriminals are capitalizing on the anxiety associated with COVID-19 by identifying opportunities to initiate phishing attempts and embed malicious links in fake news and articles on the coronavirus. Phishers are sending emails claiming to be from legitimate organizations with information about the coronavirus. For example, the World Health Organization (WHO) recently issued a warning regarding cybercriminals who tried to impersonate the WHO in an attempt to steal money or sensitive information. Therefore, it is a good "cyber hygiene" for companies to regularly educate, train and

test employees on phishing risks, and current events present a prime opportunity to remind employees of the threats and best practices associated with phishing scams.

How to prevent phishing:

1. **Verify the sender by checking their email address and check the link before you click**

   You can inspect a link by hovering your mouse button over the URL to see where it leads. Very often, it is obvious the web address is not legitimate but sometimes phishers can create links that closely resemble the legitimate address.

2. **Be careful when providing personal information**

   Always consider why someone wants your information and if it is appropriate. There is no reason someone would need your username & password to access public information.

3. **Do not rush or feel under pressure**

   Cybercriminals use emergencies such as COVID-19 to get people to make decisions quickly. Always take time to think about a request for your personal information, and whether the request is appropriate.

4. **Watch for spelling and grammatical mistakes**

   If an email includes spelling, punctuation, and grammar errors, it is likely a sign that you have received a phishing email.

5. **If you gave sensitive information, do not panic**

   If you believe you have given data such as your username or passwords to cybercriminals, immediately change your credentials on each site where you have used them.