CERT Tonga

Ministry of Meteorology, Energy Information, Disaster Management, Environment, Communications and Climate Change

TLP: White[1]

COVID-19/Coronavirus Themed Scams and Cyber Attacks

Dear Constituents,

The coronavirus (COVID-19) crisis is being used as bait in email attacks on targets around the globe. As the number of those afflicted continue to surge, campaigns that use the disease as a lure likewise increase. This has been observed by many entities, researchers and cyber security organisations who have seen a significant spike in the detection of the use of the subject in attacks.

The practice of leveraging worldwide events by basing malicious emails on current important topics has become common among cyber criminals. Such a strategy is able to trick more victims into clicking malicious links or opening malicious files, ultimately increasing the effectiveness of a cyber attack campaign. They aim to take advantage of fears over coronavirus as a means of conducting phishing attacks and spreading malware, along with stealing login credentials and credit card details.

The below examples are not and most likely will not be the only methods of using the crisis by cyber criminals and threat actors. The message is *to be cautious when coming across emails and information related to the Coronavirus or COVID-19*.

How it Works

Emails

Cyber criminals send emails claiming to be from legitimate organizations with information about the coronavirus.

Some email messages might ask you to open an attachment to see the latest statistics. If you click on the attachment or embedded link, you're likely to download malicious software onto your device.

The malicious software could allow cyber criminals to take control of your computer, log your keystrokes, or access your personal information and financial data, which could lead to identity theft. There is also some reports of the victim's data being wiped clean.

In other attacks, they encourage the user to click on a link to a supposedly genuine website. On the ripped-off copy of the site, however, the crooks had added the devious extra step of popping up an email password box on the main page.

We have also received reports here in Tonga of attempted Business Email Compromise where the criminals pretending to be a legitimate business transactions partner are using the coronavirus pandemic as a reason to urgently demand the victim to send payments to a different account in a different country.

1 CERT Tonga adopts the Traffic Light Protocol

Websites

There are also reports of websites purporting to show updated coronavirus cases on a global map found a clever ploy to hide a credential and payment card skimmer behind the website.

What to do

- Before opening an email, consider who is sending it to you and what they're asking you to do. If you are unsure, call the organisation the suspicious message is supposedly from, using contact details from a verified website or other trusted source.
- Do not open attachments or click on links in unsolicited emails or messages.
- Do not provide personal information to unverified sources and never provide remote access to your computer.
- Protect your passwords and login credentials, don't enter these into any websites relating to the COVID-19 virus. Remember that reputable organisations locally and overseas - including banks, government departments will not call or email to verify or update your personal information.
- Keep all your software on your devices up-to-date.
- Keep your antivirus up to date and run regular checks.
- Report suspected malware or phishing attempts to CERT Tonga.

Reference

https://www.cert.govt.nz/individuals/alerts/attackers-using-covid-19-themed-scams-updated-alert/
https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity

Please for more information you can contact us:

CERT Tonga
Ministry of MEIDECC
Nuku'alofa
Tel: 2378 (CERT)
email: cert@cert.gov.to
web: www.cert.gov.to