CERT Tonga

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

TLP: CLEAR[1]

Security Alert: Phishing Email containing Ransomware

Dear Constituents,

CERT Tonga received reports of an increase of phishing emails that are being used by cyber criminals to deliver ransomware payloads. These phishing emails often appears legitimate, imitating trusted brands, suppliers, or from a government agency. Once the user interacts with a malicious link or downloads an infected attachment, ransomware is deployed — encrypting files, disrupting operations, and demanding payment for decryption keys.

However, there are also reports of government personnel using personal email accounts for official work correspondence. Personal emails are not monitored or secured by government cybersecurity defenses and may also lead to serve as entry points for attackers, jeopardizing both personal and work-related files.

Examples of attack path:

- Victim receives an email pretending to be from a known service.
- Email contains a malicious link or attachment.
- Once clicked or opened, a malware loader is installed silently.
- Loader downloads and executes ransomware.
- Files are encrypted and a ransom note appears demanding payment in cryptocurrency.

Threat Indicators:

- Urgent or threatening language: e.g
  - " MV MARY GOLD APPOINTMENT// PDA Request
  - “Your account will be suspended!"
  - "Immediate payment required!"
- Suspicious email addresses: Slight misspellings of real domains (e.g., paypal.com instead of paypal.com).
- Unexpected attachments: Especially .zip, .exe, .js, .xlsm, or documents asking you to enable macros.

[1] CERT Tonga adopts the Traffic Light Protocol

- Links that don’t match the display text: Hover over the link to see the real URL before clicking.
- Poor grammar and unusual formatting email messages.

Potential Impact:

- Loss of critical data through encryption.
- Operational downtime affecting productivity.
- Financial loss from ransom payments, recovery costs, and regulatory fines.
- Reputation damage if customer or company data is leaked.
- Potential legal liabilities if personal or confidential data is exposed.

What to do:

Email Vigilance

- Do **NOT** click links or open attachments from unknown or unexpected senders.
- Verify suspicious messages through another communication channel.

System Protection

- Keep antivirus and endpoint protection updated.
- Enable spam filtering and advanced email threat protection.

User Training

- Provide Awareness campaign
- Teach staff to report suspicious emails.

Data Backup

- Maintain offline or immutable backups of critical data.
- Test backups regularly to ensure they can be restored quickly.

Patch Management

- Apply software and system updates promptly to close vulnerabilities.

If You Suspect a Phishing Email

- Do **NOT** reply or interact with the email message.
- Affected users are instructed to contact the Digital Transformation support team promptly at ictsupport@digital.gov.to or via phone at 20-189 for assistance.
- Users who have already opened the email or attachments must change their system passwords immediately.

Phishing remains as one of the most common entry point for ransomware attacks. The best defense is a combination of user awareness, layered security controls, and backups. Be aware and stay vigilant and treat every unexpected email with caution.

For more information, please contact us:

CERT Tonga
Ministry of MEIDECC
Nuku'alofa
Tel: 2378 (CERT)
Email: cert@cert.gov.to
Web: www.cert.gov.to
Twitter: @CERTTonga | Facebook: @CERTTonga

Disclaimer Notice:

The information in this notice is intended solely for public knowledge and awareness, and not intending to harm, fright or disturb any person(s), legal entity or the receiver of this information. Under no circumstances shall the Ministry of MEIDECC be liable for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with your access or use of or inability to access or use the information and any third-party content and services