CERT Tonga

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

TLP: White[1]

Security Guide – Working Remotely

A number of Tongan business and organisations are planning to allow staff to work from home as part of the preparations for the COVID-19 pandemic. We would like to ensure that both organisations and staff are implementing this in a secure way, as such we highlight the following pointers for consideration.

Guide for Organisations

- **Secure systems that enable remote access**
  - Ensure Virtual Private Network and other remote access systems are fully patched.
  - Enhance system monitoring to receive early detection and alerts on abnormal activity.
  - If available, Implement multi-factor or 2FA authentication
  - Ensure all machines have properly configured firewalls, as well as anti-malware and intrusion prevention software installed and updated
- **Test remote access solutions capacity or increase capacity**
- **Update continuity of operations plans or business continuity plans if required**
- **Ensure that all employees are trained on how to use remote access and they are aware of the cyber threats when accessing remotely.**
- **Increase awareness of information technology support mechanisms for employees who work remotely**
- **Ensure that your organisation is protected against Denial of Service (DoS) threats.**

1 CERT Tonga adopts the Traffic Light Protocol

Guide for Staff

- **Only use WiFi you trust**

  There are significant security risk in using some "free" wifi access points and you should be cautious about it. Attackers can intercept information being transmitted and can read or change that information.

- **If you use a remote desktop client, ensure it is secure (updated and patched)**
- **Ensure your devices, such as laptops and mobile phones, are secure and updated**
- **Avoid clicking on links in unsolicited emails and be wary of email attachments.**

  It has been known that threat actors are using COVID-19/Coronavirus themed attacks in emails and websites. Please be extra cautious when you receive this on email.

- **Do not reveal personal or financial information in emails, and do not respond to emails soliciting for this information.**
  - Ensure that you always verify the person sending you the email that requires personal information
- **Ensure when in a public place, no one can read what you are typing on your device and can read what is on your screen over your shoulder**
- **Business communication - Ensure the platform you use to instant message with your team is secure and has end-to-end encryption**
- **Ensure your devices and data storage are password protected with a strong password and encrypted**

  In the case where it is stolen or lost, the information contained therein doesn't fall into the wrong hands.

- **Use trusted source, such as legitimate, government websites for up-to-date, fact-based information about COVID-19 - Think Twice about sharing what your friends shares on FB**

Reference

- https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus_0.pdf
- https://www.cyber.gov.au/news/cyber-security-essential-when-preparing-covid-19
- https://www.cert.govt.nz/individuals/guides/stepping-up-your-cyber-security/working-remotely/
- https://www.cert.govt.nz/business/guides/policies-and-processes/working-remotely-securely/
- https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security?curPage=/collection/10-steps-to-cyber-security/the-10-steps/home-and-mobile-working

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

=SV\AT