**TLP: White**[1]

# An Advisory on Ransomware Attack

Dear Constituents,

Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid, even cause damage or loss of data.
Although ransomware is usually aimed at individuals, it's only a matter of time before business is targeted as well.


## What to do

Please follow these steps to prevent from any future malicious activities;

1. **Do not open suspicious email attachments**: Ransomware can also find its way to your device through email attachments. Avoid opening any dubious-looking attachments. To make sure the email is trustworthy, pay close attention to the sender and check that the address is correct. Never open attachments that prompt you to run macros in order to view them. If the attachment is infected, opening it will run a malicious macro that gives malware control of your computer.

   The following clues indicate that an email may be a phishing scam:
   - The email is not addressed to a specific person, but rather uses a generic greeting such as “Dear customer.”
   - The email encourages you to click on a link.

1 CERT Tonga adopts the Traffic Light Protocol

- The email contains grammatical errors.
- The email asks you to confirm personal information.
- The email contains a suspicious attachment.
- The email is written to create panic and encourage you to act quickly.
- The email has a fake invoice attached.
- The email contains an offer that seems too good to be true.
- The email include claims there's a problem with your account or your payment information, or that there have been too many login attempts or suspicious activity on your account.
- The email has a mismatch between email addresses or URLs that appears in the body of an email and the address shown when you hover your cursor over it.

2. **Never click on unsafe links** - Think before clicking: Avoid clicking on links in inbox or spam messages or on unknown websites. If you click on malicious links, an automatic download could be started, which could lead to your computer being infected. Try to recognize and report phishing, e.g., suspicious email addresses, generic greeting (Hi there!), an unusual email or instant message that contain grammatical errors, links outside the organization, an effort to create panic to prompt hasty action.

3. **Change your existing password**: You should consider using the longest password you can. Combine random words together, with numbers, capitalise some characters and add in some punctuation.

4. **Double your login protection to stop data breaches in their tracks**: Enable multi-factor authentication (MFA) for added protection. It ensures that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that supports it. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token.

5. **Back up your data:** Back up all your data to another device or third-party cloud service in case your device is compromised. Remember, Synchronisation services such as OneDrive and Dropbox are not data backup solutions. The changes ransomware makes, can damage synchronised copies too.

6. **Never use unknown USB sticks:** Never connect USB sticks or other storage media to your computer if you do not know where they came from. Cybercriminals may have infected the storage medium and placed it in a public place to entice somebody into using it.

7. **Use only known download sources:** To minimize the risk of downloading ransomware, never download software or media files from unknown sites. Rely on verified and trustworthy sites for downloads. Websites of this kind can be recognized by the trust seals. Make sure that the browser address bar of the page you are visiting uses "https" instead of "http". A shield or lock symbol in the address bar can also indicate that the page is secure. Also exercise caution when downloading anything to your mobile device. You can trust the Google Play Store or the Apple App Store, depending on your device.

8. **Use VPN services on public Wi-Fi networks:** Conscientious use of public Wi-Fi networks is a sensible protective measure against ransomware. When using a public WiFi network, your computer is more vulnerable to attacks. To stay protected, avoid using public Wi-Fi for sensitive transactions or use a secure VPN service.

## Reference


- https://www.cisa.gov/uscert/ncas/alerts/aa22-181a
- https://www.cyber.gov.au/ransomware


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