



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

Business Email Compromise Advisory

This advisory is relevant to all Tongan individuals, businesses and organisations. This alert is intended to be understood by both general and technical audiences. Individuals and organisations that use and rely email for business purposes are encouraged to remain vigilant and aware of cyber threats, and to apply available mitigations as soon as possible.

What's Happened?

Over the last few months, CERT Tonga has observed multiple threat actors increasingly leveraging the compromise of business email accounts for malicious purposes, across the entire global but particularly in the South Asia and Pacific Region.

Most notably, just a few weeks ago, a threat actor was able to infiltrate a business email account belonging to a manager in a Pacific Island Government Agency. The threat actor exploited the following vulnerabilities:

-  Weak Passwords
-  No Conditional Access Policies
-  Insufficient Response Capabilities
-  Lack of Multi-Factor Authentication

These threat actors leveraged these vulnerabilities to cause operational disruptions, such as compromising further email accounts and send mass-phishing emails.

While there were no major disruptions for the communities impacted, a similar attack in the future has the potential to cause significant cyber and digital harm.

What can we learn from this?

There is the opportunity to learn from this event to better protect Tongan government agencies and businesses and the communities they serve.

Threat Mitigations

Mitigating Controls: *Reduce the likelihood of your business email systems being breached:*

- Harden Business Email Systems to increase resilience.** Leverage access-based rules, email filtering and the like to improve defensive measures against business email compromise.
- Implement Multi-Factor Authentication (MFA)** on all devices and accounts, especially those with higher levels of access and permissions.
- Ensure public servants use business emails,** and that all work-related email is done using official business emails and not personal ones, as these systems are better protected.
- Increase Awareness around BEC,** so that employees are able to remain more vigilant and thus are less susceptible to phishing etc.

Where can I go for help?

If you suspect you have been impacted by business email compromise, or If you require assistance / advice on how to respond to this alert, please contact CERT Tonga directly:



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

TLP: CLEAR

Appendix: Business Email Compromise Advisory

This appendix intends to provide a more in-depth explanation of the threat mitigations mentioned on page 1. Introducing mitigations for access management and network security vulnerabilities is critical because these weaknesses are directly tied to who (or what) can access and control systems. In the case of critical infrastructure, that access often translates into real-world operational impact for the communities that rely on these critical infrastructure systems. Below are access management and network security-based control mitigations that can be implemented to strengthen critical infrastructure systems against common attack vectors. Detection is also important because it helps critical infrastructure quickly identify and respond to active threats before they cause serious damage or disruption.

Threat Mitigations



Harden Business Email Systems. Implement email security controls including advanced email filtering, anti-spoofing and anti-malware protections, as well as attachment and URL scanning. Further hardening measures include restrictions on external forwarding and continuous monitoring of mailbox activity. All of these aid in reducing the likelihood of successful phishing and other email-based attack vectors.



Conditional Access Policies. Enforce contextual and risk-based access controls that evaluate factors such as user risk, location, device compliance and sign-in behaviour to reduce the risk of authorised access and account compromise from unmanaged devices.

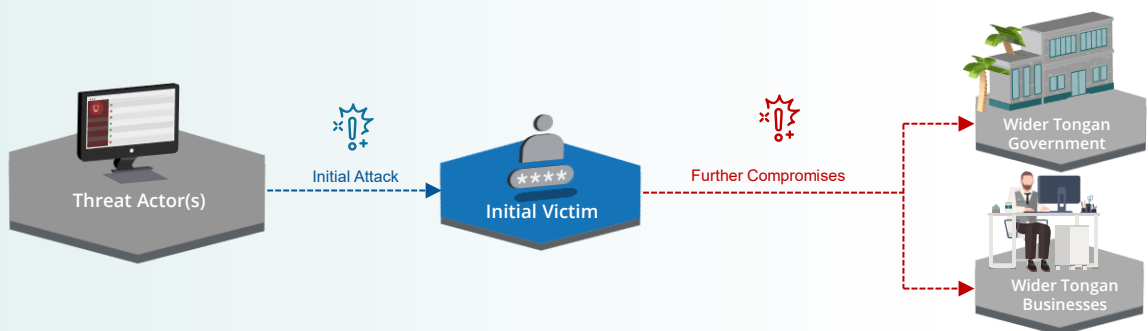


Multi-Factor Authentication. Extra factors of authentication, beyond passwords, include one-time-passwords (through authenticator apps, emails etc), biometrics, hardware tokens and more.. Requiring users to provide more than 1 way of authentication significantly strengthens user authentication measures further reducing the likelihood of adversaries gaining access to a system.



Insufficient Response Capabilities. Ensure proper setup of account permissions for accounts used for response and investigation, to enable such efforts to be able to effectively contain, eradicate and investigate an incident when it occurs.

Why Is This Important?



The impact of Business Email Compromise is often far-reaching and extends beyond the initial victim. A compromised email account provides attackers with a trusted foothold from which further malicious activity can be conducted.

Consequently, organisations should view BEC not as an isolated email security issue, but as a significant risk with potential operational, financial, legal and reputational consequences. As a result of this risk, appropriate threat mitigation methods, such as the ones above, should be implemented as a matter of priority.