

Joe Lombardo  
Governor



Timothy D. Galluzi  
State Chief Information Officer

Darla J. Dodge  
Deputy CIO – COO

David 'Ax' Axtell  
Deputy CIO – CTO

Robert 'Bob' Dehnhardt  
Deputy CIO - CISO

STATE OF NEVADA  
GOVERNOR'S OFFICE


*Office of the Chief Information Officer*


100 N. Stewart Street, Suite 100 | Carson City, Nevada 89701

Phone: (775) 684-5800 | [it.nv.gov](http://it.nv.gov) | [CIO@it.nv.gov](mailto:CIO@it.nv.gov) | Fax: (775) 687-9097

CYBER SECURITY AWARENESS MONTH – EMAIL SPOOFING

**To:** All Agencies

**From:** Timothy D. Galluzi, State Chief Information Officer 

Robert 'Bob' Dehnhardt, State Chief Information Security Officer 

**Subject:** Email Spoofing Awareness

**Date:** October 16, 2023

Last month, Governor Lombardo proclaimed that October 2023 is **Cybersecurity Awareness Month** in Nevada. It serves as a timely reminder for all of us to stay vigilant and proactive in our digital habits. We want to take this opportunity to raise awareness of a type of attack that we need everyone's vigilance to defend against.

Over the past few weeks, the Office of the CIO has observed a concerning uptick in attempts by malicious actors using spoofed (fictitious) email accounts, impersonating state leaders, in fraudulent schemes. These attempts are **not** an indication that state systems have been compromised in any way, as the bad actors are using publicly available information.

Firstly, I want to express my gratitude to the many vigilant staff members who have detected these suspicious emails and brought them to our attention. Your proactive approach and heightened security awareness play a critical role in ensuring the safety and integrity of our state's digital assets.

Here are some common indicators to help you identify potentially spoofed emails:

1. **Mismatched Email Addresses:** The display name might seem legitimate, but the actual email address is off by a letter or uses a different domain. Often using free email services (Yahoo, Gmail, etc.).
2. **Unexpected Attachments or Links:** Be wary of emails urging you to click on a link or open an attachment, especially if you weren't expecting it.
3. **Grammar and Spelling Mistakes:** These emails may contain noticeable errors in language, spelling, or punctuation.

4. **Urgent or Threatening Language:** Spoofed emails often create a sense of urgency, e.g., claiming you'll lose access to an account unless immediate action is taken.
5. **Requests to only communicate via email:** Some attempts may say that the leader is unavailable to discuss over the phone or is running from meeting to meeting so email or text is preferred.
6. **Attempts to circumvent processes and controls:** Bad actors may request that you take actions that are outside of normal processes and fiscal controls.

All these indicators should raise your suspicions. When in doubt, verify the requests using official state email addresses, listed phone number, or with your IT Helpdesk.

Our collective responsibility in securing our State's digital infrastructure cannot be overstated. Together, with an informed and proactive stance, we can mitigate the threats that come our way.

Thank you for your dedication and ongoing commitment to the safety and wellbeing of our great state.