

Joe Lombardo
Governor



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 | CIO@it.nv.gov | Fax: (775) 687-9097


Timothy D. Galluzi
State Chief Information Officer

Darla J. Dodge
Deputy CIO / COO

David Axtell
Deputy CIO / CTO

Robert 'Bob' Dehnhardt
Deputy CIO / CISO

Cyber Security Awareness Update – Email Spoofing

To: All Agencies
From: Robert 'Bob' Dehnhardt, State Chief Information Security Officer 
Subject: Email Spoofing Awareness
Date: January 17, 2024

In light of recent cybersecurity and fraud attempts, it's essential that we remain vigilant and informed about the risks associated with email spoofing. We've witnessed an increase in email spoofing attempts across several states, including Nevada. These attacks involve malicious individuals impersonating others and requesting sensitive information or actions.

While our technology infrastructure in Nevada is robust and effective at blocking such threats, it's not foolproof, and some malicious emails may still slip through. In such cases, you, as the recipient, play a crucial role in our overall security.

To help you identify potentially spoofed emails, please refer to the indicators provided by our State of Nevada Chief Information Officer, Timothy D Galluzi's October 2023 memo (attached for your reference). If you ever doubt the legitimacy of an email you receive, it's best to reach out to the sender through alternative means, such as a message in Teams or a phone call to a known, legitimate number. This not only verifies the email's authenticity but also alerts the sender to potential email spoofing.

Your proactive approach and heightened security awareness are instrumental in protecting our digital assets and maintaining the integrity of our state's systems. Here are some common indicators of spoofed emails to watch out for:

- **Mismatched Email Addresses:** Check for discrepancies between the display name and the actual email address, especially when different domains or free email services are used.
- **Unexpected Attachments or Links:** Be cautious when urged to click on links or open attachments, particularly if you weren't expecting them.

- **Grammar and Spelling Mistakes:** Spoofed emails may contain noticeable errors in language, spelling, or punctuation.
- **Urgent or Threatening Language:** Be cautious of emails creating a sense of urgency, such as threats of account access loss.
- **Requests to Only Communicate via Email:** Some spoofed attempts may claim that phone communication is not possible, insisting on email or text.
- **Attempts to Circumvent Processes and Controls:** Be wary of requests that deviate from standard processes and fiscal controls.

When in doubt, verify requests using official state email addresses, listed phone numbers, or consult with our IT Service Desk, or your Agency's Information Security Professionals.

Our collective responsibility in securing Nevada's digital infrastructure cannot be overstated. By remaining informed and proactive, we can effectively mitigate threats. Thank you for your dedication and commitment to our state's safety and well-being.

If you have any questions or concerns, please feel free to reach out.