NEVADA GAMING CONTROL BOARD

1919 College Parkway, Suite 110, P.O. Box 8003, Carson City, Nevada 89702
7 State of Nevada Way, Las Vegas, Nevada 89119
3650 S. Pointe Circle, Suite 203, P.O. Box 31109, Laughlin, Nevada 89028
557 W. Silver Street, Suite 207, Elko, Nevada 89801
9670 Gateway Drive, Reno, Nevada 89521

JOE LOMBARDO
Governor

MIKE DREITZER, *Chairman*
HON. GEORGE ASSAD (RET.), *Member*
CHANDENI K. SENDALL, *Member*

NOTICE TO LICENSEES

Notice # 2026-21 Issuing Division: Administration

DATE: March 6, 2026

TO: All Interested Persons

FROM: Nathan Riggle, Chief of Administration

SUBJECT: **Cybersecurity Awareness Alert**

Please see attached for an important Cybersecurity Awareness Alert from the Governor's Technology Office.

Joe Lombardo
Governor

Timothy D. Galluzi
Executive Director / State CIO

Darla J. Dodge
Senior Deputy Director / COO

Adam Miller
Deputy Director / OISCD

STATE OF NEVADA
GOVERNOR'S TECHNOLOGY OFFICE

100 N. Stewart Street, Suite 100 | Carson City, Nevada 89701
Phone: (775) 684-5800 | www.it.nv.gov | CIO@it.nv.gov | Fax: (775) 687-9097

Cybersecurity Notice

We are writing to alert you to an increase in cybersecurity incidents that have been observed across organizations and critical Nevada industries, including incidents involving phishing and voice phishing, also called vishing. Phishing typically uses deceptive emails, texts, or links to trick someone into revealing credentials, financial information, or other sensitive data. Vishing uses phone calls or voicemail to create the same pressure, often by impersonating a trusted organization, executive, vendor, or technical support contact.

In light of this activity, all staff are encouraged to heighten cyber awareness and remain vigilant in daily operations. This is especially important when handling requests involving account access, password resets, wire transfers, changes to payment instructions, sensitive records, or any action that relies on identity verification.

Please do not take shortcuts in authentication or verification processes. A request that appears urgent, routine, or familiar may still be fraudulent. Attackers often rely on urgency, impersonation, and human trust to bypass normal controls.

We recommend the following immediate actions:

- Reconfirm internal procedures for verifying unusual or high-risk requests.
- Require staff to use known contact information, not call-back numbers or links provided in a suspicious message.
- Verify requests for payments, credential resets, or sensitive data through a second, independent channel.
- Reinforce with staff that urgency is not a reason to bypass established controls.
- Review multi-factor authentication settings and strengthen them where feasible.
- Encourage prompt internal reporting of suspicious emails, calls, texts, and unusual login or account activity.

Practical reminders for staff:

- Be cautious with unexpected emails, text messages, and attachments.
- Do not click links or open files unless you are confident the message is legitimate.
- Be wary of callers who pressure you to act immediately, keep a request secret, or override normal approval steps.

- Never share passwords, MFA codes, or account recovery information by email, text, or phone.
- When in doubt, stop, verify, and escalate.

Helpful resources

- CISA: Recognize and Report Phishing
- CISA: Avoiding Social Engineering and Phishing Attacks
- CISA: More Than a Password / Require Multifactor Authentication
- FTC: How To Recognize and Avoid Phishing Scams

Thank you for your continued attention to this matter and for reinforcing strong security practices within your organization.

Adam Miller
Deputy Director, Office of Information Security & Cyber Defense
Governor's Technology Office