

August 2026

Priority Level: High

Threat Overview: Social Engineering

Threat actors are actively leveraging social engineering, AI-generated content, exploitation of internet-facing edge infrastructure, and human vulnerabilities to compromise organizations. State-sponsored adversaries are also using generative artificial intelligence (Gen AI) to increase the speed and effectiveness of cyber attacks against State, Local, Tribal, and Territorial (SLTT) governments and critical infrastructure, including water and wastewater systems that rely on operational technology (OT). Disruption of these essential services can quickly create fear, uncertainty, and distrust. This bulletin highlights current cyber risks and recommended defensive measures to reduce exposure and protect critical systems and services.

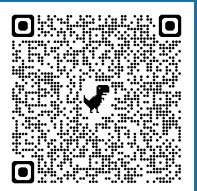
Threat Vectors to Watch

- **AI-Enhanced Phishing & Smishing:**
Cybercriminals are using generative AI to create context-aware, error-free emails and SMS lures. These attacks mimic internal leadership, HR updates or vendor invoices to harvest credentials or approve fraudulent transactions.
- **Session Hijacking & MFA Fatigue:** Attackers bypass Multi-Factor Authentication (MFA) via adversary-in-the-middle (AiTM) phishing kits or repeated authorization requests (MFA fatigue) to trick employees into approving unauthorized sign-ins.
- **Malicious Attachments & QR Code Scams (Quishing):** Embeds malicious links inside QR codes in PDF attachments or emails, bypassing standard email filters and forcing users to switch to less-secure personal mobile devices.
- **Remote Work & Unapproved Software (Shadow IT):** Unauthorized tools and unsecured home networks remain primary vectors for data exposure and vulnerability exploitation.

GOAL: The goal of this campaign is to give business leaders, IT teams, and operational staff simple, actionable guidance to strengthen defenses against modern cyber threats. While attackers use complex and evolving methods, many successful intrusions still exploit basic weaknesses. The foundational controls show that doing the simple things, such as patching, authentication, access control, visibility, and backup, can make a biggest difference. More awareness materials will follow through October's Cybersecurity Awareness Month.

Remember: Security is a Shared Responsibility

- ✓ When in doubt, verify through official internal channels before interacting with unexpected requests.
- ✓ If you click on a suspicious link or enter credentials on a suspicious website, notify your security operations center or responsible IT support immediately.



For more information, scan the QR code or visit
ransomwareinfo.oregon.gov



CYBER READINESS TIPS

Best Practices For Organizations

- **Strengthen security** by evaluating and enhancing your organization's security posture to prevent future cybersecurity attacks.
- **Implement security controls**, such as vulnerability management, advanced threat detection systems, and network segmentation.
- **Continuously monitor** systems and networks for any signs of malware or suspicious activities.
- **Review and update** your incident response plan and recovery procedures based on emerging threats and changes to your organization's IT environment.
- **Participate** in industry information sharing to stay informed about emerging threats and attack techniques.

Best Practices For Individuals

- **Use strong, unique passwords** by using a different password for every account, and consider using a reputable password manager to securely store them.
- **Turn on multi-factor authentication (MFA)** which adds an extra layer of protection to important accounts.
- **Think before you click.** Be cautious with unexpected and urgent emails, texts, links, and attachments.
- **Keep devices and apps updated** with security updates and patches for your operating system, apps, browsers, and other devices as soon as practical.

Questions For Organizations



- Do we have **immutable backups** in place?
- Are backups **tested** regularly?
- Does our disaster recovery plan include **recovery time objectives and recovery point objectives** for our most mission critical systems?
- How are we making our users aware of **approved AI usage**?
- Do we provide an environment that promotes **continuing education**?
- Are conducting regular exercises to test our **Incident Response Plan**?
- How are we achieving **defense in depth**?

Questions For Individuals

- **What am I sharing online?** Could information I post publicly help someone guess my passwords, answer security questions, impersonate me, or target me with a scam?
- **Who has access to my accounts?** Have I reviewed old accounts, connected apps, browser sessions, and devices that may still have access?
- **What happens if I lose my phone or laptop?** Are my devices protected with a strong passcode, encryption, and the ability to locate or remotely wipe them?

Additional Resources:

Oregon Emergency Response System
(OERS) 1-800-452-0311

Cybersecurity & Infrastructure Security Agency (CISA)
888-282-0870 | www.cisa.gov

FBI Field Office - Cyber Task Forces
Portland Office 503-224-4181
<https://www.ic3.gov/fbi.gov/contact-us/field>

Multi-State Information Sharing and Analysis Center®
(MS-ISAC®) 866-787-4722

State of Oregon Security Operations Center
503-378-5930 | css.soc@eis.oregon.gov

National Institute of Standards and Technology (NIST)
<https://www.nist.gov/cybersecurity-and-privacy>



For more information on strengthening your cybersecurity posture, refer to the FBI's Operation Winter SHIELD guidance.

<https://www.fbi.gov/investigate/cyber/wintershield>

