ENTERPRISE
information services

CYBER SECURITY SERVICES

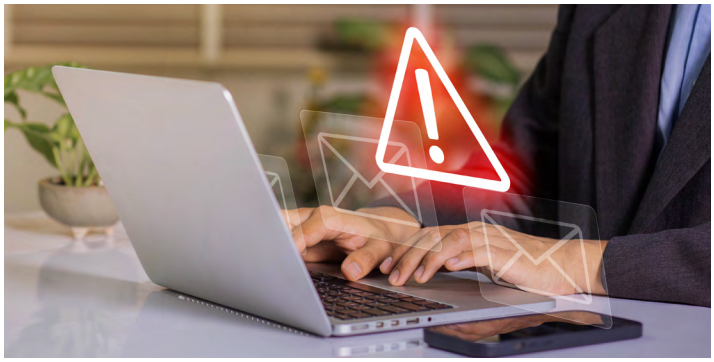
RANSOMWARE AWARENESS CAMPAIGN

September 2023 | Volume 4

DETECT

Detect

Detect - The third of five core functions within the NIST Cybersecurity Framework (CSF) - focuses on improving the ability to monitor and identify anomalous events and malicious attempts from threat actors such as ransomware in a timely manner and is an effort needed from all levels within an organization.



What Can All Personnel Do?

By staying vigilant and cautious, users can play a crucial role in detecting ransomware and protecting their systems and the organization:

- Be cautious of unexpected emails, attachments, and links, even from known contacts. When in doubt, reach out to the person or group from a known email or phone number to verify.
- Promptly report to IT any unusual system behaviors or suspicious computer activity.

GOAL: The goal of this campaign is to provide business leaders, IT teams, and stakeholders shareable and actionable information to protect, detect, respond, and recover in the event of a ransomware attack. Over the course of the next few months, the State of Oregon Cyber Security Services team will be sending out additional awareness fliers to share and help educate as many organizations and people as possible. A webinar will be conducted at the end of the campaign, to provide a discussion and answer session for interested parties.

Cyber Security Services Webinar - Save the Date!

» October 11, 2023 1pm – 2pm
» October 13, 2023 9am – 10am

SOME EXAMPLES OF OUTCOMES WITHIN DETECT:

» Ensuring malicious anomalies and events are detected, their potential impact is understood
» Maintaining detection processes to provide awareness of anomalous events
» Implementing security capabilities to continuously monitor for cybersecurity events
» Verify the effectiveness of protective measures including network and physical activities

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

ENSURING ACCESSIBLE, RELIABLE, AND SECURE STATE TECHNOLOGY SYSTEMS THAT SERVE OREGONIANS.

What Can Business Leaders Do?

Business leaders can improve their organization's ability to detect malicious activity, such as ransomware threats, by engaging with their IT/security folks and having conversations around activities and areas of consideration such as:

Detection processes:

- How these processes are tested and updated.
- What processes and procedures exist for detecting unauthorized entities and actions including personnel activity.
- What defined roles and responsibilities exist for detection and reporting both internal and external.

Activity logs:

- How logs are maintained and monitored to identify anomalies in your organization's computers and applications.

Organization data flows:

- What the expected data flows are in the organization.
- What an unexpected data flow might look like.
- If using contracted work to a cloud or managed service provider, how their data flows are tracked and reported, including unexpected events.

The impact of cybersecurity events:

- What business-essential functions are impacted by possible cybersecurity events, and how they align with the data flows and needs of IT/security personnel.
- What communication policies and procedures exist to effectively outreach to stakeholders and constituents during an event.

QUESTIONS FOR YOUR IT PERSONNEL:

» What obstacles exist that inhibit our ability to log activity and detect anomalous events?
» What gaps exist in our current policies and governance around monitoring?
» Are processes for monitoring organizational network activity established and effective?

Additional Resources:

National Institute of Standards and Technology (NIST)
csrc.nist.gov

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

FBI Field Office - Cyber Task Forces
fbi.gov/contact-us/field
Portland Office 503-224-4181
Ransomware Safety Resource

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

Oregon Cybersecurity State Incident Response Team
503-378-5930 | eso.soc@das.oregon.gov

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

Statewide Interoperability Team
503-373-7251 | swic.or@das.oregon.gov

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

ENTERPRISE information services

ENSURING ACCESSIBLE, RELIABLE, AND SECURE STATE TECHNOLOGY SYSTEMS THAT SERVE OREGONIANS.