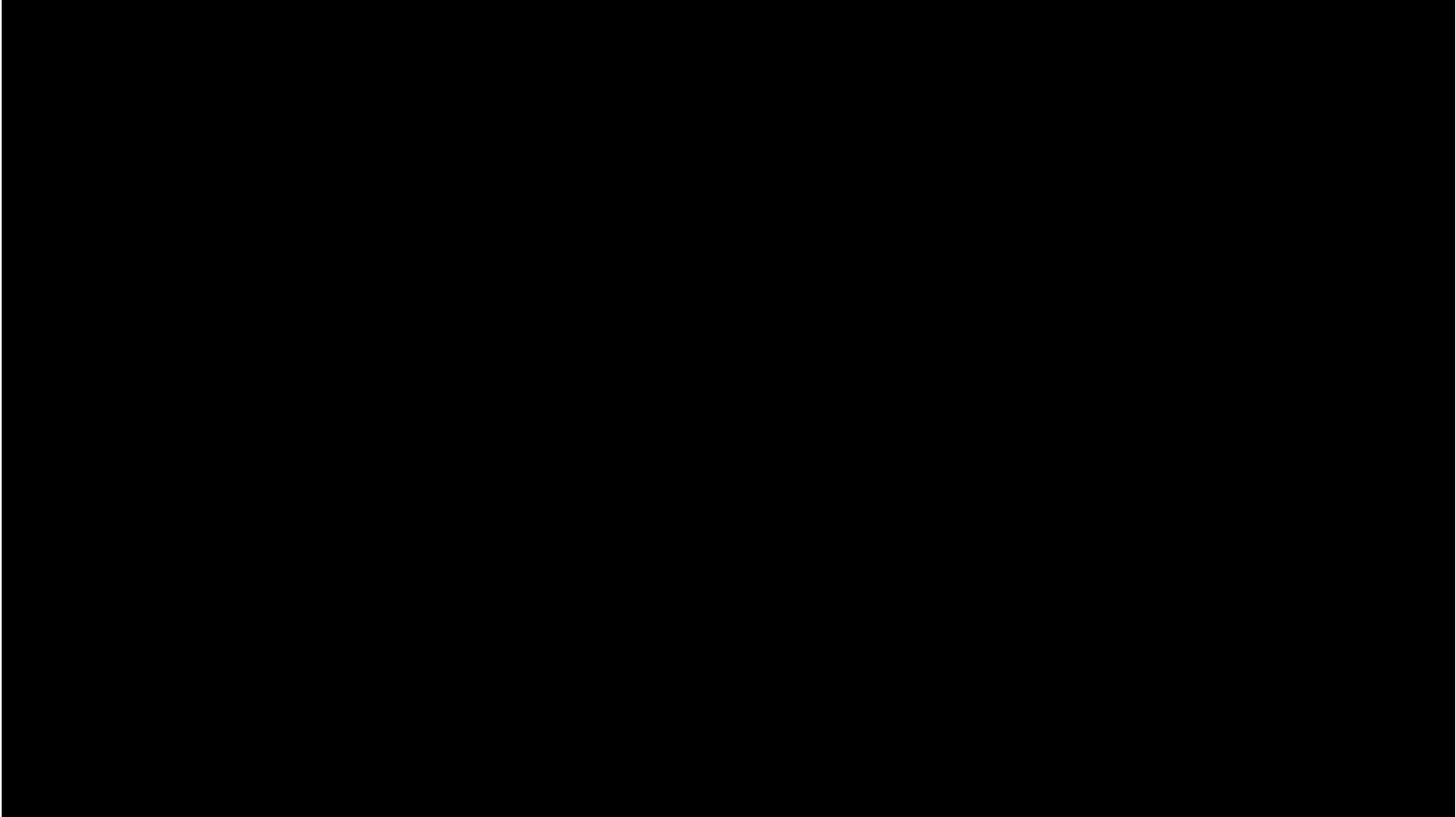


CYBERSECURITY
AWARENESS MONTH
2024

WaTech
Washington Technology Solutions

Cybersecurity Awareness Month

Protect yourself from online threats





Ralph Johnson, State CISO

Ralph Johnson leads the Office of Cybersecurity, focusing on risk prevention and strengthening the state's cybersecurity. With 28 years of IT experience, he has served as a Chief Information Security Officer (CISO) since 2005, supporting organizations like the Los Angeles Times and King County, where he was also the Privacy Officer. His expertise as a Holistic Information Security Practitioner underpins his success in managing cybersecurity risks effectively.



Bill Kehoe, State CIO

William "Bill" Kehoe became Washington's State CIO and WaTech Director on August 1, 2021. Before this, he was CIO for Los Angeles County (2017-2021), overseeing IT strategy and services for 37 departments. He also advised the Board of Supervisors and CEO on technology policy. Bill has over 15 years of IT leadership experience in Washington state, including roles as King County's CIO (2010-2017) and the Department of Licensing's first CIO (2002-2010). His career highlights his extensive expertise in managing government IT departments at both state and local levels.

Today's Agenda

- **Origins of Cybersecurity Awareness Month.**
- **How Cybersecurity Awareness has evolved over time.**
- **The importance of cybersecurity in 2024.**
- **Key themes for this year.**
- **How you can get involved.**
- **Collaboration of CIOs and CISOs.**

Origins

Launched in October 2004 by the U.S. Department of Homeland Security (DHS) and the National Cyber Security Alliance (NCSA).

Objective: To educate individuals and organizations on the importance of cybersecurity, safeguard online data, and promote safe online practices.



Evolution

Early Years: Initially the focus was on encouraging individuals to update their antivirus software and practice basic security habits.

Present Day: Now the campaign reaches millions globally, guiding advanced security topics such as multi-factor authentication (MFA), phishing attacks, and data breaches. These awareness efforts involve schools, governments, private companies, and individuals.



Why Cybersecurity Matters in 2024

Cybersecurity is no longer a niche issue. It affects every aspect of our lives—business, finance, health, education, and even personal relationships.

Here are some key facts:

- By 2025, cybercrime will cost the world over \$10 trillion annually, surpassing the global drug trade.
- Ransomware attacks are becoming more frequent, targeting everyone from small businesses to large institutions.
- Phishing schemes have evolved, becoming more sophisticated and harder to detect.
- Critical infrastructures like energy grids, hospitals, and government systems are increasingly targeted by cyberattacks.
- Artificial Intelligence (AI) enables even low-skilled threat actors to launch attacks. Given this, we all must play an active role in maintaining cybersecurity.



2024 Focus

**Secure Your
Digital Life**

Key Themes for 2024

- **Secure yourself:** Embrace essential cybersecurity practices such as using strong passwords, enabling multi-factor authentication (MFA), and regularly updating your devices.
- **Know the threats:** Raise awareness about prevalent threats, including phishing, ransomware, and social engineering attacks.
- **Defend your business:** Equip small to medium-sized businesses with strategies to enhance their security measures.
- **Digital privacy:** Emphasize the significance of managing personal data and ensuring organizations handle it responsibly.



How You Can Get Involved

- **Adopt safe online practices:** Use strong passwords, update your devices, and be vigilant about suspicious emails or links.
- **Participate in webinars and workshops:** Take advantage of free training and workshops offered by organizations like Washington state to stay informed about the latest security best practices.
- **Raise awareness:** Share resources on social media, educate friends and family about online safety, and engage in workplace security programs to spread awareness.
- **Stay informed:** Cyber threats are constantly evolving. Continuously learn, adapt, and stay ahead of these threats.

Participate

- Attend 22 engaging presentations and webinars throughout October.
- Challenge yourself with weekly Kahoot quizzes.
- Experience the thrill of our Cyber Escape Room.
- Solve the Data Heist Mystery Game.
- And much more!
- Participation automatically enters you into weekly prize drawings.

Win Prizes

The agency with the highest overall per-employee participation wins a trophy and challenge coins.

Random drawing of all participants throughout the month for a chance to have lunch with the CISO and receive a challenge coin.

Escape Room

- All team members receive a gift/goody bag.
- Each member of the team with the highest score gets a challenge coin.

Weekly

- Random drawing of all presentation participants for a \$25 Amazon eGift Card.
- Kahoot Quiz. The top scorer wins a \$25 Amazon eGift Card.
- Data Heist Mystery – Random drawing for a \$25 Amazon eGift card.



CIO and CISO Collaboration



Shared Leadership and Communication





Joint Risk Management

Align Cybersecurity with Business Objectives





Collaborative Incident Response Planning



Budget Collaboration

Integrate Security Early in Technology Projects



Continuous Education and Awareness



Governance and Compliance Alignment





Shared Metrics and Reporting

Cross- Functional Teams





Conclusion and Final Thoughts

Cybersecurity Awareness Month is an opportunity to not only reflect on the challenges we encounter but also to take proactive steps to safeguard ourselves and our communities.

As technology continues to weave itself into every aspect of our lives, prioritizing cybersecurity becomes essential for everyone. By working together, we can create a safer digital environment.

Thank you for your engagement and commitment. Stay vigilant and secure online!

