October 2022

OREGON STATE TREASURY

Inside the Vault

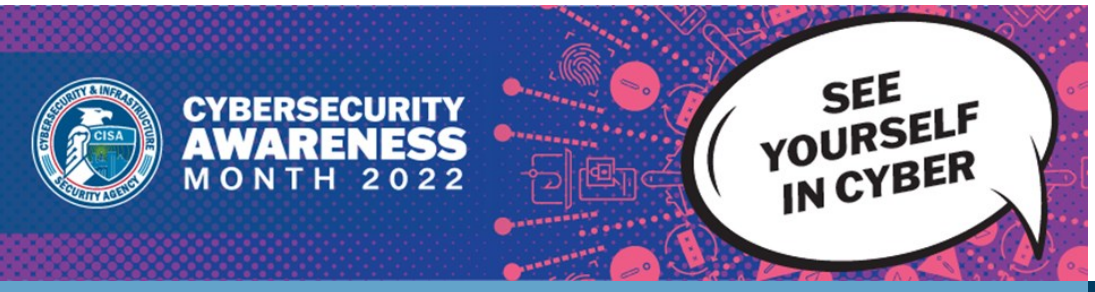
State Agency Edition

Cybersecurity Awareness Month

Since 2004, the President of the United States and Congress have declared October to be Cybersecurity Awareness Month to help individuals protect themselves online as threats to technology and confidential data become more commonplace. The Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance (NCA) lead a collaborative effort between government and industry to raise cybersecurity awareness nationally and internationally.

See Yourself in Cyber

This year's campaign demonstrates that while cybersecurity may seem like a complex subject, it's ultimately about people. This October focuses on the "people" part of cybersecurity and provides information and resources to help educate CISA partners and the public to ensure all individuals and organizations make smart decisions whether on the job, at home, or at school – now and in the future. We encourage each of you to engage in this year's efforts by creating your own cyber awareness campaigns and sharing this messaging with your peers.



- For individuals and families, we encourage you

(Continued on page 2)

Upcoming Holiday

Due to Veterans Day, Treasury, the Federal Reserve, and financial institutions will be closed on Friday, November 11. Customer statements and files will not be produced for November 11 due to the closures. In addition, ACH files sent to Treasury after the deadline on Thursday, November 10, will be sent to the bank on Monday, November 14, and must have an effective date of November 15 or later.

Interest Rates

Average Annualized Yield

September	1.8417%

Interest Rates

September 1–7	1.65%
September 8–30	1.90%

(Continued from page 1)

to **See Yourself taking action to stay safe online**. That means enabling basic cyber hygiene practices: update your software, think before you click, have good strong passwords or a password keeper, and enable multi-factor authentication on all your sensitive accounts.

- For those considering joining the cyber community, we encourage you to **See Yourself joining the cyber workforce** with a focus on a cybersecurity workforce that is bigger, more diverse, and dedicated to solving the problems that will help keep the American people safe.
- For our partners in industry, we encourage you to **See Yourself as part of the solution**. That means putting operational collaboration into practice, working together to share information in real-time, and reducing risk and build resilience from the start to protect America's critical infrastructure and the systems that Americans rely on every day.

More information about Cybersecurity Awareness Month is available at www.cisa.gov/cybersecurity-awareness-month.

Employment Opportunities

Treasury is currently recruiting for an Operations & Policy Analyst 3 (Business and Change Management Analyst). This position has the primary responsibility to provide business analyst activities for banking, cash management, public funds, and related programs. This includes responsibility for leading change management activities as well as participation in business process mapping and evaluation activities aimed at replacing, refining, or validating core business processes and supporting technology for Finance Division programs. The position will also work with Treasury customers and business partners as needed to define and achieve project goals. The recruitment is scheduled to close November 6.

Treasury is also recruiting for an Operations & Policy Analyst 3 (Business Analyst). This is a job rotation, and it will start in November or December of 2022 and last through the end of June 2023. This position has the primary responsibility to provide business analyst activities for banking, cash management, public funds, and related programs. This includes responsibility for business process mapping and evaluation activities aimed at replacing, refining, or validating core business processes and supporting technology for Finance Division programs. The position will also work with Treasury customers and business partners as needed to define and achieve project goals. The recruitment is scheduled to close October 28.

If you have questions about either position, contact Brady Coy, CMIRP Manager, at 503.378.2457 or brady.coy@ost.state.or.us.

Spear Phishing

All organizations, including state agencies and other governmental entities, must be vigilant in combatting ever-sophisticated cybercriminals. Spear phishing, in which cybercriminals use target-specific approaches and social engineering, is a particularly challenging scam that often circumvents traditional technological defenses such as spam filters.

While spear phishing attacks can come in many forms, payment instruction switch is a common scam based on a legitimate customer or vendor relationship. In this type of attack, an organization has been regularly paying a customer or vendor via direct deposit. The organization then receives a form, fax, or e-mail updating the customer's or vendor's bank account information used to process payments. In actuality, the update was submitted by a cybercriminal. If undetected, the organization starts sending payments to the cybercriminal's bank account instead of to the customer's or vendor's bank account. Without proper controls and prevention strategies, the organization may lose multiple payments until the customer or vendor notifies the organization of the missing payments. Funds lost in these kinds of attacks are often difficult or impossible to recover.

How to Protect Your Organization

While spear phishing is a sophisticated scam that relies on inside information, there are processes that your organization can use to avoid becoming a victim. In the example above, the organization could have uncovered the attempted fraud by calling the customer or vendor at a known phone number in order to confirm the update. When performing such a call-back process, it is important to use a phone number already on file and not one provided with the requested change.

For more tips related to spear phishing and other social engineering attacks, visit the U.S. Computer Emergency Readiness Team's website at www.cisa.gov/uscert/ncas/tips/ST04-014.

Service Spotlight

Safekeeping is a free service that allows agencies to store items of value in Treasury's vaults. Items placed in safekeeping are usually being held to insure performance, cover a liability, or provide some other means of financial protection. Items placed in safekeeping are inventoried, and agencies receive a receipt for each item. Agencies must submit a written request to retrieve items from safekeeping, and items must be picked up in person. If you are interested in safekeeping or have questions regarding cash management services generally, contact Customer Solutions at customer.solutions@ost.state.or.us.

Data Security

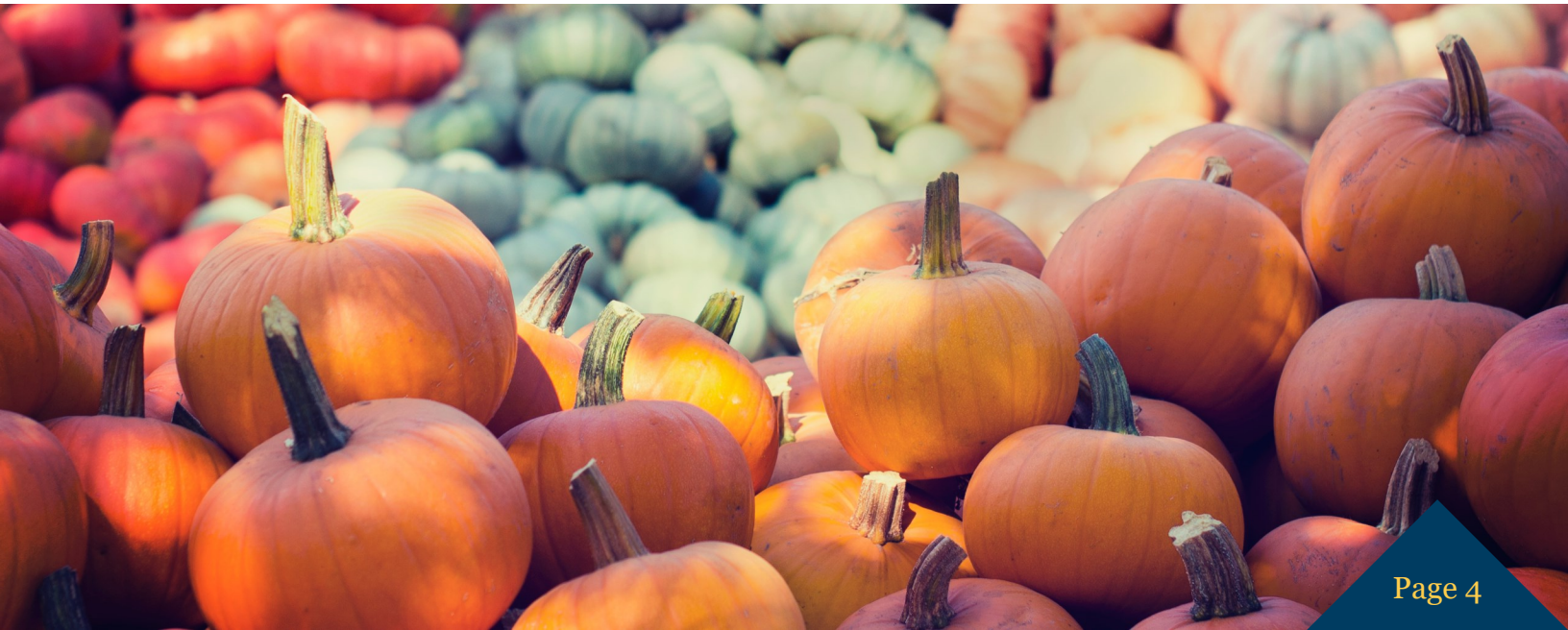
According to the Identify Theft Resource Center, data breaches in 2021 surpassed those in 2020 by 68%, and 2022 has seen results similar to 2021. While each breach is unique, each results in the possibility of data being compromised. Such data can include credit card numbers, bank account information, social security numbers, or other personally identifiable information. Since most agencies transmit, process, or store this same information in electronic or physical format, it is vitally important for agencies to be diligent about keeping data security at the forefront of business decisions and processes.

As a reminder, in addition to the Payment Card Industry Data Security Standard (PCI DSS) and Nacha Rules, agencies are required to comply with Office of the State Chief Information Officer policies, Oregon Accounting Manual Chapter 10, and Treasury Cash Management Policies. As they may reduce the risk of a data breach, please check with your agency's security team, CFO, or manager responsible for financial controls about the status of your organization's compliance with such requirements.

Below are a few recurring themes included in many regulatory requirements that are intended to help safeguard sensitive information:

- Maintain updated data security policies and procedures that are aligned with applicable regulatory requirements.
- Ensure that agency management and staff are aware of your organization's liabilities and responsibilities for protecting sensitive information when processing payments including merchant cards, ACH transactions, and onsite electronic deposits.
- Provide training to staff, at least annually, about the data security policies and procedures applicable to their duties.
- Re-evaluate the reason for storing personally identifiable information.

These are but a few reminders about protecting your customers' personally identifiable information. If you have questions about the regulatory requirements for any of the banking services used by your organization, contact Customer Solutions at customer.solutions@ost.state.or.us.



Director of Finance
Cora Parker
503.378.4633

Deputy Director of Finance
Bryan Cruz González
503.378.3496

Cash Management Analyst
Natalya Cudahey
503.378.8256

Policy Analyst
Ken Tennies
503.373.7453

Administrative Specialist
Kari McCaw
503.378.4633

Banking Fax
503.373.1179

Banking Operations Manager
Sarah Kingsbury
503.373.1501

Banking Operations Coordinator
Jeremiah McClintock
503.378.4990

ACH File Issues
ach.exception.notify@ost.state.or.us

Check Fraud/Stop Payments
Check Image Requests
Check Stock Testing
Ashley Moya
503.373.1944

Fed Wires/ACH Origination
Shannon Higgins
503.378.5043

Local Government Investment Pool
Sarah Kingsbury
503.373.1501

Merchant Card/U.S. Bank
Nikki Main
503.378.2409

Online User
Password Resets
ost.banking@ost.state.or.us

Safekeeping/Debt Service
Sherry Hayter
503.378.2895

Customer Solutions Team
customer.solutions@ost.state.or.us
503.373.7312

Analysts
Lyndsie DeOlus
Heidi Lancaster
Ellis Williams

Cash Management Improvement & Renewal Program
cmirp@ost.state.or.us

Manager
Brady Coy
503.378.2457

Business Analyst
Angel Bringelson
503.378.5865

Contracted Project Manager (TEK Systems)
David Riffle
503.373.7864

OREGON STATE TREASURY
867 Hawthorne Ave SE ⏩ Salem, OR 97301-5241
oregon.gov/treasury