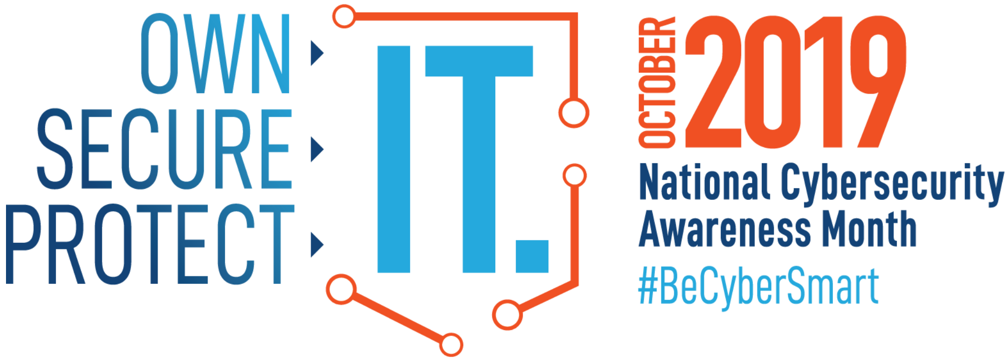
October 2019

OREGON STATE TREASURY

Inside the Vault

State Agency Edition

National Cybersecurity Awareness Month



Protecting your customers' cardholder, bank account, or other sensitive information is a continuous, ongoing process—not a single event or action. Recognizing the importance of cybersecurity awareness, the United States Department of Homeland Security has designated October as National Cybersecurity Awareness Month—an annual campaign to raise awareness about cybersecurity. Treasury participates in this national month of awareness by taking the opportunity to remind our customers of the importance of information security.

2019 marks the 16th year of this important effort, which emphasizes that cybersecurity is a shared responsibility and that we all must work together to improve our nation's cybersecurity. Following that theme, this month's newsletter includes a few items related to security practices. While it's important for our agency customers to ensure that your systems are secure, employees continue to be the single biggest threat to sensitive data by opening and/or clicking links in phishing e-mails. More information about National Cybersecurity Awareness Month is available at www.dhs.gov/national-cyber-security-awareness-month.

Upcoming Holiday

Due to Veterans Day, Treasury, the Federal Reserve, and Oregon banks will be closed on Monday, 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 Friday, November 8, will be sent to the bank on Tuesday, November 12, and must have an effective date of November 13 or later.

Interest Rates

Average Annualized Yield	
September	2.565%

Interest Rates	
September 1–23	2.60%
September 24–30	2.45%

CONNECT WITH CONFIDENCE

HELPFUL HINTS TO KEEP YOU CYBER SAFE

OWN ▸ SECURE ▸ PROTECT ▸ IT.

OCTOBER 2019 National Cybersecurity Awareness Month #BeCyberSmart

OWN IT.

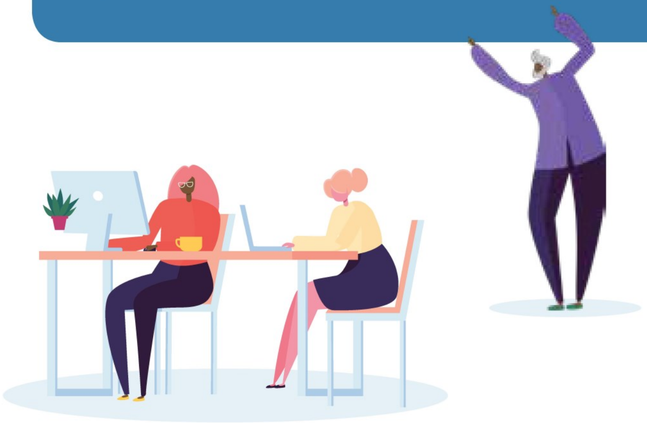
- Only use sites that begin with https:// when shopping or banking online.
- Understand the personal information you knowingly (or unknowingly) put on social media.
- Don't respond or click on links from people or organizations you don't recognize.
- Never share your personal information if you're unsure who's asking.

SECURE IT.

- Apply multi-factor authentication to your accounts ASAP!
- Always lock your personal or work laptop or mobile device when unattended in a public place.
- Use the longest password possible and be creative.
- Check your app permissions frequently.

PROTECT IT.

- Look for the "green lock" icon when online, it signifies a secure connection.
- Use your personal hotspot in public places, they're more secure than free WIFI.
- Make sure you're using the latest security software, web browser, and operating system.
- Secure your WIFI network and digital devices by changing the factory set password and username.



For more information about connecting with confidence visit: https://niccs.us-cert.gov/national-cybersecurity-awareness-month-2019

CISA CYBER+INFRASTRUCTURE | NATIONAL CYBERSECURITY ALLIANCE | CyberAware

Data Security Reminder

It is becoming more commonplace for major retailers, restaurants, and government organizations to announce a data security breach. 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, as well as Treasury Cash Management Policies. Please check in with your agency's security team, CFO, or manager responsible for financial controls about the status of your organization's compliance with such requirements as they may reduce the risk of a data breach.

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 customersolutions@ost.state.or.us.

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 some form of security 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 customersolutions@ost.state.or.us.

Stop.Think.Connect

Homeland Security has a number of resources available to the public regarding cyber security. One of those resources is the Stop.Think.Connect campaign, which is a continuous national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Cybersecurity is a shared responsibility. We each have to do our part to keep the Internet safe. When we all take simple steps to be safer online, it makes using the Internet a more secure experience for everyone.

This October, and every day, follow these simple online safety tips:

- **Enable stronger authentication.** Always enable stronger authentication for an extra layer of security beyond the password that is available on most major email, social media and financial accounts. Stronger authentication (*e.g.*, multi-factor authentication that can use a one-time code texted to a mobile device) helps verify that a user has authorized access to an online account. For more information about authentication, visit the Lock Down Your Login Campaign at www.lockdownyourlogin.org.
- **Make your passwords long and strong.** Use complex passwords with a combination of numbers, symbols, and letters. Use unique passwords for different accounts. Change your passwords regularly, especially if you believe they have been compromised.
- **Keep a clean machine.** Update the security software, operating system, and web browser on all of your Internet-connected devices. Keeping your security software up to date will prevent attackers from taking advantage of known vulnerabilities.
- **When in doubt, throw it out.** Links in email and online posts are often the way cyber criminals compromise your computer. If it looks suspicious (even if you know the source), delete it.
- **Share with care.** Limit the amount of personal information you share online and use privacy settings to avoid sharing information widely.
- **Secure your Wi-Fi network.** Your home's wireless router is the primary entrance for cybercriminals to access all of your connected devices. Secure your Wi-Fi network, and your digital devices, by changing the factory-set default password and username.

Learn more about the Stop.Think.Connect campaign at www.dhs.gov/stopthinkconnect.

Tips for keeping your personal information safe, your family protected, and our national security intact.

Stop hackers from accessing your accounts — set secure passwords.
Stop sharing too much information — keep your personal information personal.
Stop — trust your gut. If something doesn't feel right, *stop what you are doing.*

Think about the information you want to share before you share it.
Think how your online actions can affect your offline life.
Think before you act — don't automatically click on links.

Connect over secure networks.
Connect with people you know.
Connect with care and be on the lookout for potential threats.

STOP | THINK | CONNECT™

Securing one citizen, one family, one Nation against cyber threats.

www.dhs.gov/stopthinkconnect

Director of Finance
Cora Parker
503.378.4633

Deputy Director of Finance
Mike Auman
503.378.2752

Policy & Strategy Manager
Bryan Cruz González
503.378.3496

Cash Management Analyst
Natalya Cudahey
503.378.8256

Administrative Specialist
Kari McCaw
503.378.4633

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

Business Analyst
Angel Bringelson
503.378.5865

Contracted Project Manager (TEK Systems)
David Riffle
503.373.7864

Banking Fax
503.373.1179

Banking Operations Manager
Brady Coy
503.378.2457

Banking Operations Coordinator
Ellis Williams
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
Brady Coy
503.378.2457

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
customersolutions@ost.state.or.us

Customer Solutions Regulatory Manager
Sharon Prentice
503.373.7312

Customer Solutions Services Manager
Edie Kessel
503.373.1897

Customer Solutions Consultant
Shannon Kammerman
503.378.8562

Public Funds Coordinator
Sharon Prentice
503.373.7312

OREGON STATE TREASURY
350 Winter Street NE, Suite 100 ▸▸ Salem, OR 97301-3896
oregon.gov/treasury