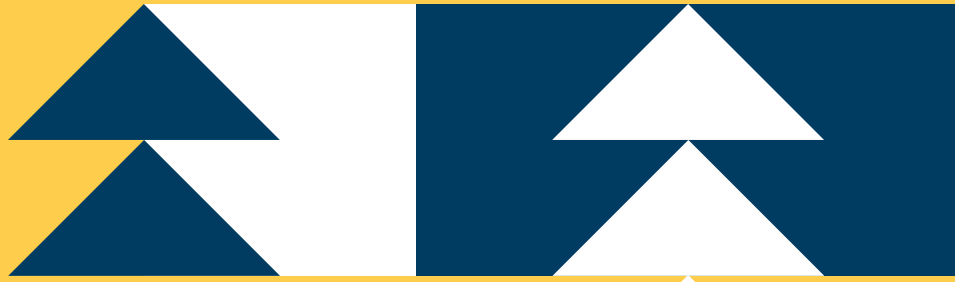




**OREGON
STATE
TREASURY**



Inside the Vault

Local Government Edition

Security Spotlight: Social Engineering

It is the end of a long day and you finally get around to checking the voicemail left by an unknown number that called earlier. A voice informs you that you owe back taxes to the IRS and there is a warrant out for your arrest, so please call back. Did you remember to mail your local taxes? Did your mortgage company make that payment? Maybe it is someone with the same name? It has to be a mistake, but you need to know for sure. Do you call the number?

What Is Social Engineering?

Social engineering is the art of capitalizing on relationships and social behavior to manipulate people into providing access, supplying information, or performing an action. An attack can be as simple as an unsolicited e-mail that appears to be from a friend pleading for help or as elaborate as a request from your supervisor directing you to perform an action immediately. In every case, people are the key to whether an attack succeeds or fails.



What Are Some Different Types of Social Engineering?

Attacks are usually distinguished by the medium used or the type of pressure exerted on a victim. One of the most common examples are “phishing attacks.” These e-mails look like legitimate requests and usually come with a degree of urgency to get a victim to act quickly. If a recipient accepts the e-mail as legitimate, they may click a link, provide confidential information, and continue about their business unaware that sensitive information is now in the hands

(Continued on page 2)

Upcoming Holiday

The pool will be closed on Thursday, November 27, for Thanksgiving. Connect will be available, but the system will not allow transactions to settle on the holiday.

Interest Rates

Average Annualized Yield

October 4.5710%

Interest Rates

October 1–22 4.60%

October 23–31 4.50%

(Continued from page 1)

of hackers. The access provided can allow hackers to lurk in a system, exploiting any information available to achieve their ultimate goal.

A simple phishing attack can be just the beginning. The more information hackers have about an individual or organization, the more they are able to make their attacks convincing, potentially leading to “spear phishing.” Spear phishing is when hackers understand the relationships within an organization and send e-mails designed to mimic requests within the organization. Many people refuse to click on links in a strange e-mail, but suppose it is an urgent request from supervisor? Many recipients are less likely to verify if the request is legitimate or an attack before reacting.

Attacks are not limited to e-mail communication or a specific tactic. Any mode of communication or predictable tendency can be exploited. Here is a list of some of the other common attacks:

- ▲ **Vishing** (voice-phishing) attacks are the same as both phishing and spear phishing attacks, but are done through telephone calls
- ▲ **Smishing** (SMS-phishing) attacks utilize text messages
- ▲ **Pretexting** presents victims with the false “pretext” of verifying their information
- ▲ **Baiting** offers victims a prize for information
- ▲ **Tailgating** takes advantage of holding a door open to compromise a secure location
- ▲ **Quid Pro Quo** attacks give victims a gift to make them feel obligated to respond



Ultimately, hackers employ these methods because they are much easier than trying to hack into software. Every software system is designed to be used by users, so the surest way to gain control is to manipulate the user.

How Can I Help Protect against Social Engineering Attacks?

We encourage all of our customers to think about their readiness, specifically how your organization can prepare by deploying technology, processes, and education designed to enhance security.

Attacks are a product of technology, but technology can also play a role in protection. For instance, spam filters are effective at stopping most phishing e-mails from reaching intended targets. Another tool is multi-factor authentication (MFA). MFA is a method of confirming a user’s identity utilizing factors beyond the standard username and password. Sometimes simple procedures like regularly resetting passwords can limit damage or frustrate attacks.

Unfortunately, deploying more secure technology in an organization does not mean it gets used every time, a fact that highlights the importance of assessing organizational processes. Process assessment should extend to third-party service providers as well, and be understood by all parties.

Finally, education should underpin any readiness effort. Any person with even low levels of access to data should have a basic knowledge of what attacks are possible through e-mail, text, and

(Continued on page 3)

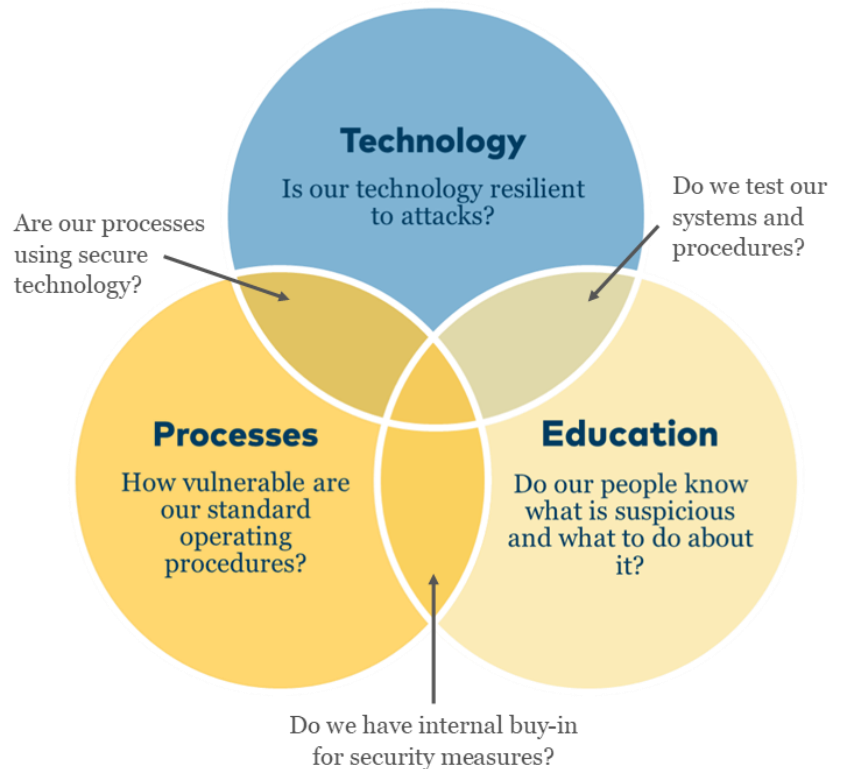
(Continued from page 2)

phone. Employees of public organizations face a unique challenge in that they are responsible for providing transparency but any information—such as organizational charts, contact information, and biographical information—could be used to hijack internal communications. Educational efforts should highlight what is possible and underscore the security reasons behind the processes and technology that employees execute or interact with on a daily basis.

So Do You Call Them Back?

We hope that after understanding the possibilities that technology has opened for both good and malicious purposes, you know that the best course of action is to delete the voicemail mentioned in the opening scenario. If you wanted to go the extra step, you could contact the IRS directly, being careful not to use any contact information from the message. Although these attacks can be alarming, hackers using social engineering have no way to keep you from simply deleting an e-mail or independently verifying any suspicious requests.

A Framework for Education, Technology & Processes



LGIP Redemptions: Wire Transfer vs. ACH

Participants have two options when redeeming (withdrawing) funds. Understanding the differences between wire transfer and ACH will help you best meet your business needs.

Wire Transfer	ACH
Can settle as soon as same day (must be initiated by 10:00 a.m.)	Can settle as soon as next business day (must be initiated by 1:00 p.m.)
Same-day wire transfers cannot exceed \$1.5 million (no dollar limit for future-dated wire transfers)	No dollar limit
\$10.00 fee per transaction	\$0.05 fee per transaction

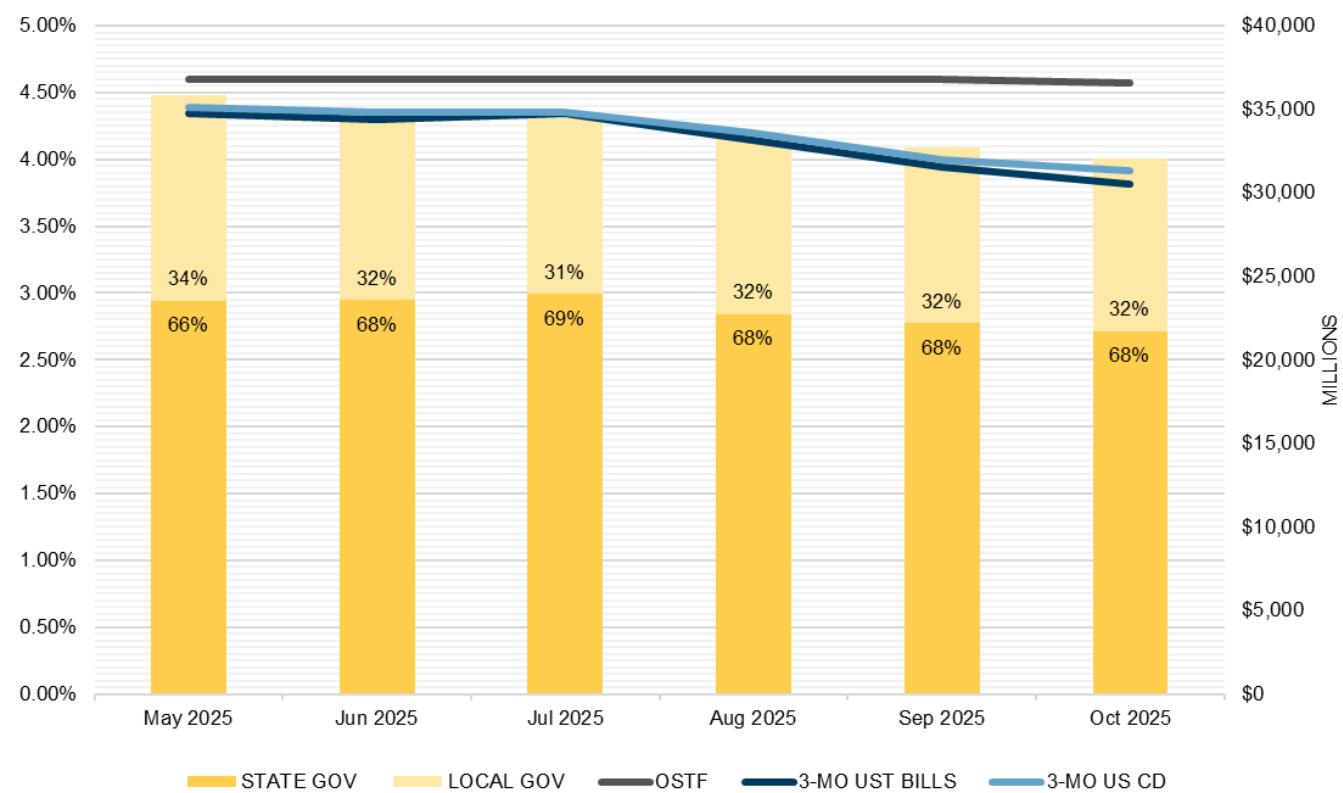
If you need to redeem funds quickly, wire transfer is the only option available that settles as soon as same day (note that same-day wire transfers cannot exceed \$1.5 million). If you do not need funds the same day, ACH may be the best option given its lower cost. Both types of transactions can be scheduled up to almost a year in advance. *Note that neither wire transfer nor ACH is guaranteed to settle by a specific time on the scheduled settlement date.* Contact PFMAM Client Services at 855.OST.LGIP or csgmww@pfmam.com if you have questions about which redemption option best meets your needs.

2026 LGIP Holiday Schedule

To help you in your investment planning, the following are holidays that will be observed by the Local Government Investment Pool during 2026. Connect will be available, but the system will not allow transactions to settle on a holiday.

Day	Date	Holiday
Thursday	January 1	New Year’s Day
Monday	January 19	Martin Luther King, Jr. Day
Monday	February 16	Presidents Day
Friday	April 3	Good Friday
Monday	May 25	Memorial Day
Friday	June 19	Juneteenth
Friday	July 3	Independence Day (observed)
Monday	September 7	Labor Day
Monday	October 12	Columbus Day
Wednesday	November 11	Veterans Day
Thursday	November 26	Thanksgiving Day
Friday	December 25	Christmas Day

Oregon Short Term Fund Analysis



	May 2025	Jun 2025	Jul 2025	Aug 2025	Sep 2025	Oct 2025
TOTAL OSTF AVG DOLLARS INVESTED (MM)	35,826	34,673	34,477	33,295	32,701	32,077
STATE GOV PORTION (MM)	23,540	23,588	23,926	22,737	22,182	21,715
LOCAL GOV PORTION (MM)	12,286	11,085	10,551	10,558	10,519	10,362
OSTF ANNUAL YIELD (ACT/ACT)	4.60	4.60	4.60	4.60	4.60	4.57
3-MO UST BILLS (BOND EQ YLD)	4.342	4.298	4.341	4.146	3.939	3.816
3-MO US CD (ACT/360)*	4.39	4.35	4.35	4.20	4.00	3.92

NOTE: The OSTF ANNUAL YIELD represents the average annualized yield paid to participants during the month. Since interest accrues to accounts on a daily basis and the rate paid changes during the month, this average rate is not the exact rate earned by each account.

3-MO UST BILLS yield is the yield for the Treasury Bill Issue maturing closest to 3 months from month end. 3-MO US CD rates are obtained from Bloomberg and represent a composite of broker dealer quotes on highly rated (A1+/P1/F1+ from Standard & Poor's Ratings Services, Moody's Investors Service and Fitch Ratings respectively) bank certificates of deposit and are quoted on a CD equivalent yield basis.

Market Data Table

	10/31/2025	1 Month	3 Months	12 Months		10/31/2025	1 Month	3 Months	12 Months
7-Day Agency Discount Note**	3.76	3.90	4.21	4.59	Bloomberg Barclays 1-3 Year Corporate YTW*	4.08	4.07	4.42	4.69
30-Day Agy Nt Disc**	3.81	3.80	4.23	4.55	Bloomberg Barclays 1-3 Year Corporate OAS*	0.49	0.46	0.47	0.52
90-Day Agy Nt Disc**	3.77	3.77	4.21	4.41	Bloomberg Barclays 1-3 Year Corporate Modified Duration*	1.83	1.84	1.86	1.82
180-Day Agy Nt Disc**	3.68	3.65	4.10	4.28					
360-Day Agy Nt Disc**	3.53	3.45	3.92	3.99	7-Day Muni VRDN Yield**	3.22	2.89	2.29	3.24
					O/N GGC Repo Yield**	4.21	4.23	4.40	4.98
30-Day Treasury Bill**	3.84	3.98	4.23	4.59					
60-Day Treasury Bill**	3.82	3.91	4.23	4.53	Secured Overnight Funding Rate (SOFR)**	4.22	4.24	4.39	4.90
90-Day Treasury Bill**	3.79	3.85	4.22	4.47					
6-Month Treasury Yield**	3.82	3.84	4.28	4.46	US 10 Year Inflation Break-Even**	2.32	2.37	2.39	2.33
1-Year Treasury Yield**	3.69	3.62	4.10	4.27					
2-Year Treasury Yield**	3.58	3.61	3.96	4.17	1-Day CP (A1/P1)**	3.91	4.12	4.30	4.82
3-Year Treasury Yield**	3.58	3.62	3.90	4.13	7-Day CP (A1/P1)**	3.91	4.11	4.31	4.78
					30-Day CP (A1/P1)**	3.85	4.09	4.33	4.71
1-Month SOFR**	4.00	4.13	4.35	4.66					
3-Month SOFR**	3.89	3.98	4.30	4.56	30-Day CD (A1/P1)**	3.92	4.11	4.34	4.69
6-Month SOFR**	3.79	3.85	4.19	4.41	90-Day CD (A1/P1)**	3.99	4.08	4.40	4.72
12-Month SOFR**	3.61	3.66	4.00	4.17	6-Month CD (A1/P1)**	3.95	4.02	4.40	4.61
Sources: *Bloomberg Index Services, **Bloomberg					1-Year CD (A1/P1)**	3.95	3.95	4.34	4.53

Director of Finance

Cora Parker
503.378.4633

Deputy Director of Finance

Bryan Cruz González
503.378.3496

Newsletter Questions

Kari McCaw
503.378.4633

Local-Gov-News Mailing List

[omls.oregon.gov/mailman/listinfo/
local-gov-news](https://omls.oregon.gov/mailman/listinfo/local-gov-news)

Local Government Investment Pool

oregon.gov/lgip

PFMAM Client Services

855.OST.LGIP
csgmww@pfmam.com

- ▲ Connect Access
- ▲ Transactions
- ▲ Reporting
- ▲ Account/User Maintenance
- ▲ Eligibility

Treasury

800.452.0345
lgip@ost.state.or.us

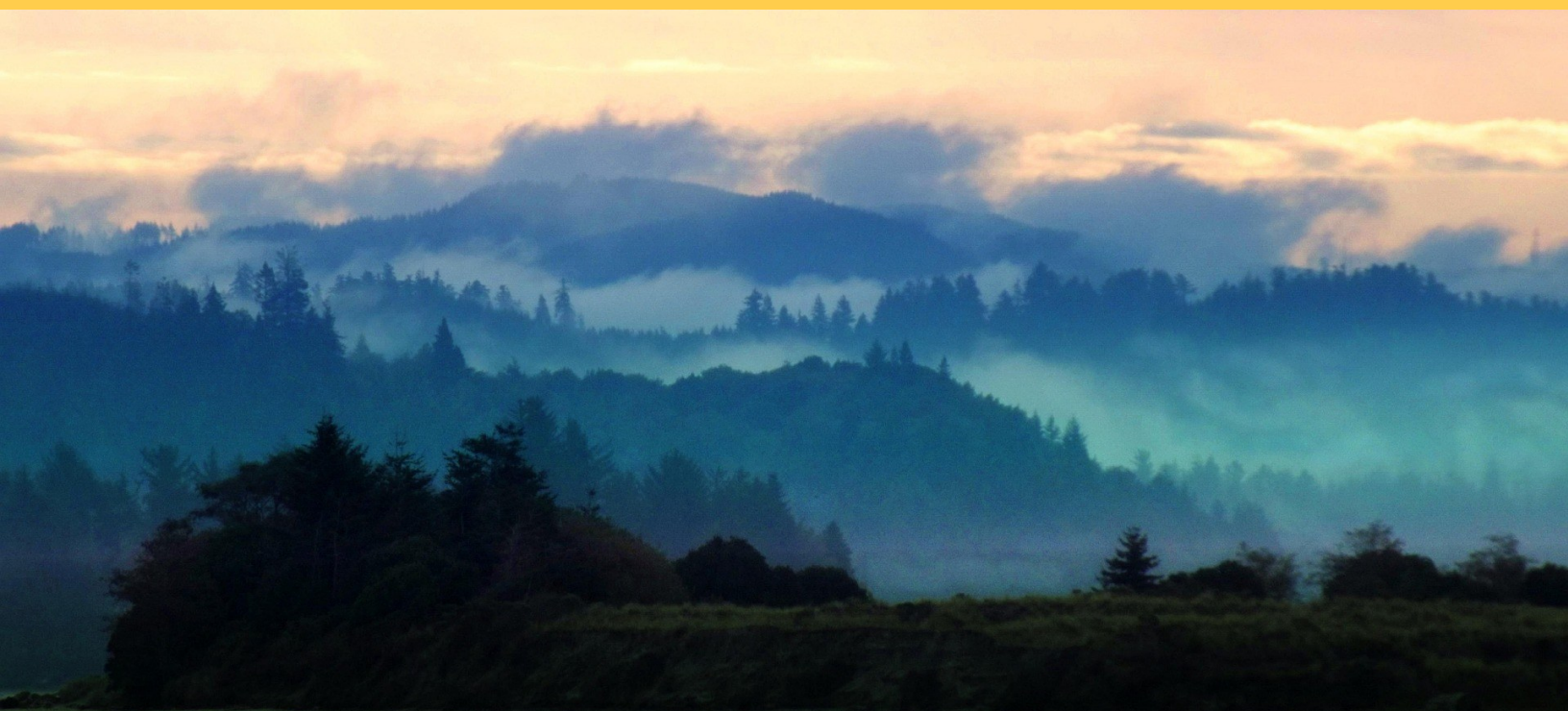
- ▲ Investment Management
- ▲ Statutory Requirements
- ▲ Service Provider Issues
- ▲ General Program Inquiries

Oregon Short Term Fund Staff

503.431.7900

Public Funds Collateralization Program

oregon.gov/pfcp
503.378.3400
public.funds@ost.state.or.us



OREGON STATE TREASURY

867 Hawthorne Ave SE » Salem, OR 97301-5241
oregon.gov/treasury