November 2024

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 28, for Thanksgiving. Connect will be available, but the system will not allow transactions to settle on the holiday.

Interest Rates

Average Annualized Yield

October	5.1113%

Interest Rates

October 1	5.30%
October 2–22	5.15%
October 23–31	5.00%

(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

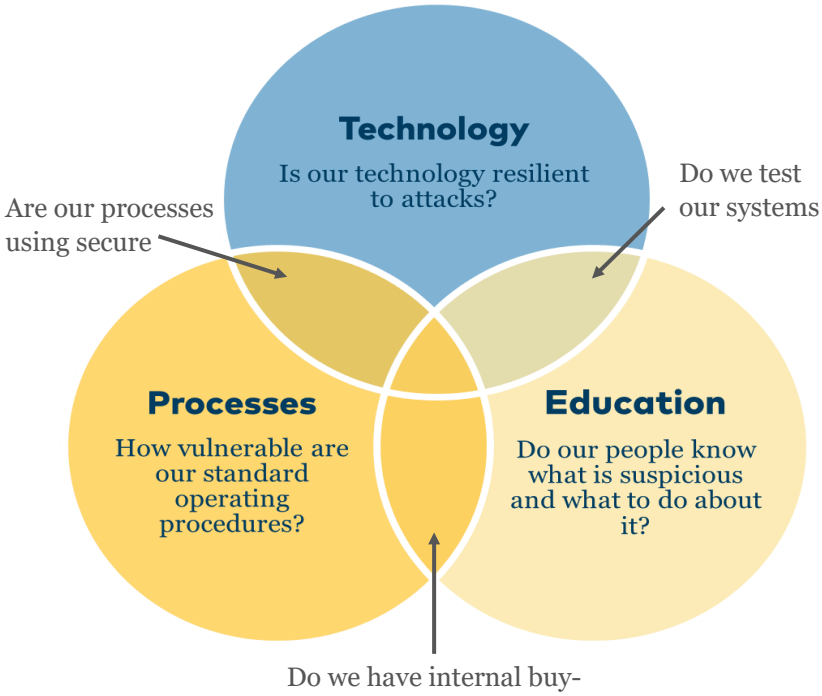
Ultimately, hackers employ these methods because they are much easier than trying to hack into software. Every software system is designed to be used by users, so the surest way to gain control is to manipulate the user.

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

A Framework for Education, Technology & Processes



(Continued on page 3)

(Continued from page 2)

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 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.

Employment Opportunity

Treasury is currently recruiting for an Operations & Policy Analyst 3 (Cash Management Business Continuity Analyst). This position has the primary responsibility to develop, maintain, and implement ongoing business continuity strategies to ensure that Treasury meets its “no fail” operational requirements within Oregon State Treasury’s Finance Division. The recruitment is scheduled to close December 15.

If you have questions about the position, contact Kelsea Bennett, Cash Management Improvement and Renewal Program Manager, at 503.378.3048 or kelsea.bennett@ost.state.or.us.

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

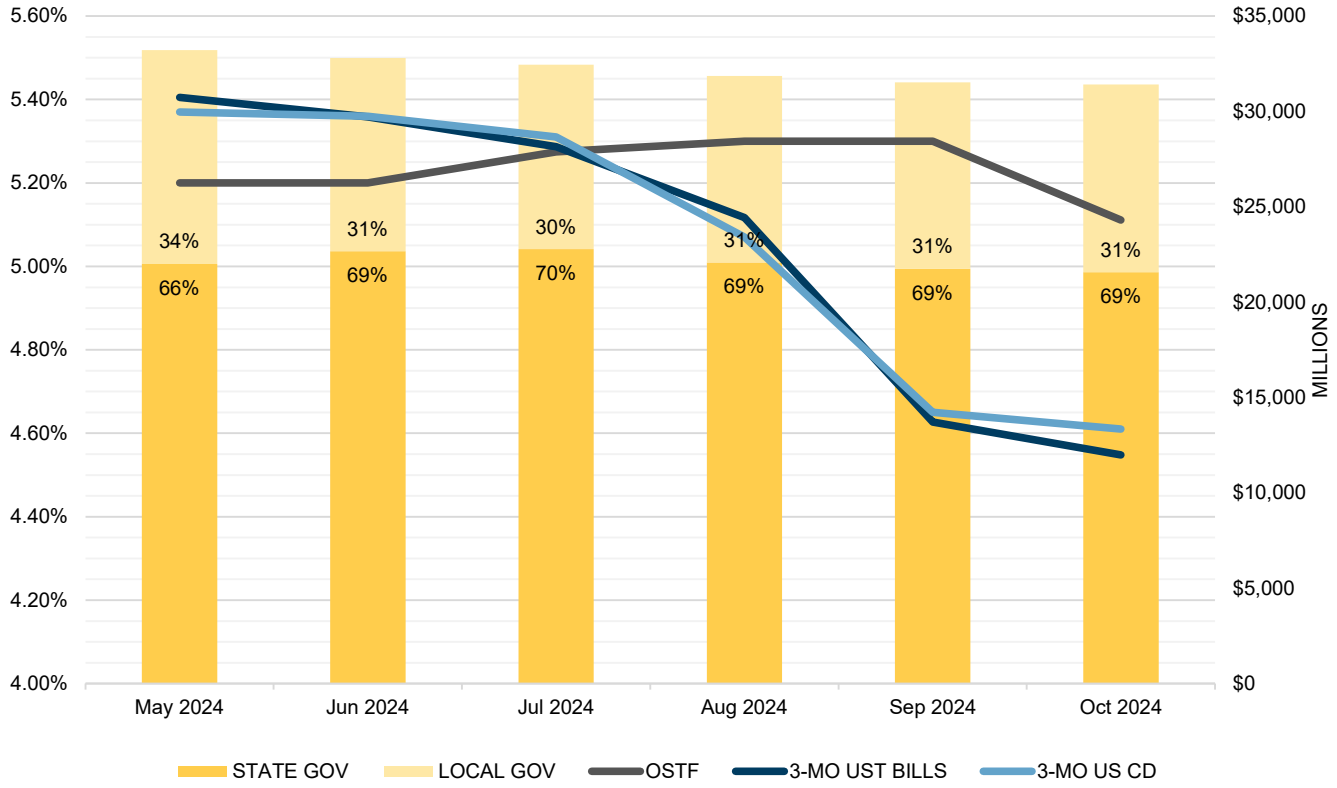
If you need to redeem funds immediately, wire transfer is the only option available (note that same-day wire redemptions cannot exceed $1.5 million). If you do not need funds the same day, ACH may be the best option given its lower cost. Both types of transactions can be scheduled up to almost a year in advance. Contact PFMAM Client Services at 855.OST.LGIP or csgmww@pfmam.com if you have questions about which redemption option best meets your needs.

2025 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 2025. Connect will be available, but the system will not allow transactions to settle on a holiday.

Day	Date	Holiday
Wednesday	January 1	New Year's Day
Monday	January 20	Martin Luther King, Jr. Day
Monday	February 17	Presidents Day
Monday	May 26	Memorial Day
Thursday	June 19	Juneteenth
Friday	July 4	Independence Day
Monday	September 1	Labor Day
Monday	October 13	Columbus Day
Tuesday	November 11	Veterans Day
Thursday	November 27	Thanksgiving Day
Thursday	December 25	Christmas Day

Oregon Short Term Fund Analysis



	May 2024	Jun 2024	Jul 2024	Aug 2024	Sep 2024	Oct 2024
TOTAL OSTF AVG DOLLARS INVESTED (MM)	33,215	32,804	32,452	31,861	31,521	31,405
STATE GOV PORTION (MM)	22,004	22,671	22,776	22,079	21,742	21,572
LOCAL GOV PORTION (MM)	11,211	10,133	9,676	9,782	9,779	9,833
OSTF ANNUAL YIELD (ACT/ACT)	5.20	5.20	5.27	5.30	5.30	5.11
3-MO UST BILLS (BOND EQ YLD)	5.405	5.358	5.287	5.117	4.627	4.548
3-MO US CD (ACT/360)*	5.37	5.36	5.31	5.07	4.65	4.61

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

	10/31/2024	1 Month	3 Months	12 Months		10/31/2024	1 Month	3 Months	12 Months
7-Day Agency Discount Note**	4.59	4.56	5.25	5.27	Bloomberg Barclays 1-3 Year Corporate YTW*	4.69	4.23	4.86	5.99
30-Day Agy Nt Disc**	4.55	4.65	5.25	5.30	Bloomberg Barclays 1-3 Year Corporate OAS*	0.52	0.56	0.56	0.96
90-Day Agy Nt Disc**	4.41	4.46	5.12	5.32	Bloomberg Barclays 1-3 Year Corporate Modified Duration*	1.82	1.84	1.85	1.82
180-Day Agy Nt Disc**	4.28	4.14	4.90	5.30					
360-Day Agy Nt Disc**	3.99	3.67	4.49	5.16	7-Day Muni VRDN Yield**	3.24	3.15	3.51	4.09
					O/N GGC Repo Yield**	4.98	5.29	5.46	5.39
30-Day Treasury Bill**	4.59	4.63	5.25	5.28					
60-Day Treasury Bill**	4.53	4.59	5.23	5.33	Secured Overnight Funding Rate (SOFR)**	4.90	4.96	5.38	5.35
90-Day Treasury Bill**	4.47	4.51	5.19	5.36					
6-Month Treasury Yield**	4.46	4.41	5.09	5.57	US 10 Year Inflation Break-Even**	2.33	2.19	2.23	2.42
1-Year Treasury Yield**	4.27	4.01	4.75	5.46					
2-Year Treasury Yield**	4.17	3.64	4.26	5.09	1-Day CP (A1/P1)**	4.82	4.80	5.30	5.29
3-Year Treasury Yield**	4.13	3.55	4.06	4.93	7-Day CP (A1/P1)**	4.78	4.80	5.31	5.27
					30-Day CP (A1/P1)**	4.71	4.82	5.34	5.35
1-Month SOFR**	4.66	4.85	5.34	5.32					
3-Month SOFR**	4.56	4.59	5.24	5.38	30-Day CD (A1/P1)**	4.69	4.83	5.37	5.38
6-Month SOFR**	4.41	4.25	5.08	5.44	90-Day CD (A1/P1)**	4.72	4.75	5.37	5.52
12-Month SOFR**	4.17	3.78	4.74	5.37	6-Month CD (A1/P1)**	4.61	4.49	5.27	5.93
Sources: *Bloomberg Index Services, **Bloomberg					1-Year CD (A1/P1)**	4.53	4.14	5.04	5.07

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

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