September 2021

OREGON STATE TREASURY

Inside the Vault

Local Government Edition

Security Spotlight: Ransomware

Ransomware is a type of malicious software designed to make files and systems inaccessible to the rightful owner in order to demand a price, or "ransom," for restoring access. It can take advantage of the myriad of ways hackers gain illicit access of computing devices.

Common Types of Attacks

- **Phishing Attacks:** An e-mail using social engineering techniques to influence a user to click a link or run a program.
- **Trojan Horses:** Viruses that are embedded or disguised within innocuous programs or even seemingly necessary software that an unwitting user runs on their machine.
- **Worms:** A self-replicating program that moves through computer networks. Unlike the methods above, a worm does not depend on tricking users—all this form of ransomware needs is a device to access an infected network.
- **Hacking Weak Passwords:** Described as using "brute force attacks," this type of hacking uses a program to try common passwords until one works. This approach may seem like a fool's errand, however, it is actually simply a numbers game. Careless or simple passwords and poor network security features can turn an impossibility into an inevitability.

(Continued on page 2)

Interest Rates

Average Annualized Yield

August	0.55%

Interest Rates

August 1–31	0.55%

Upcoming Holiday

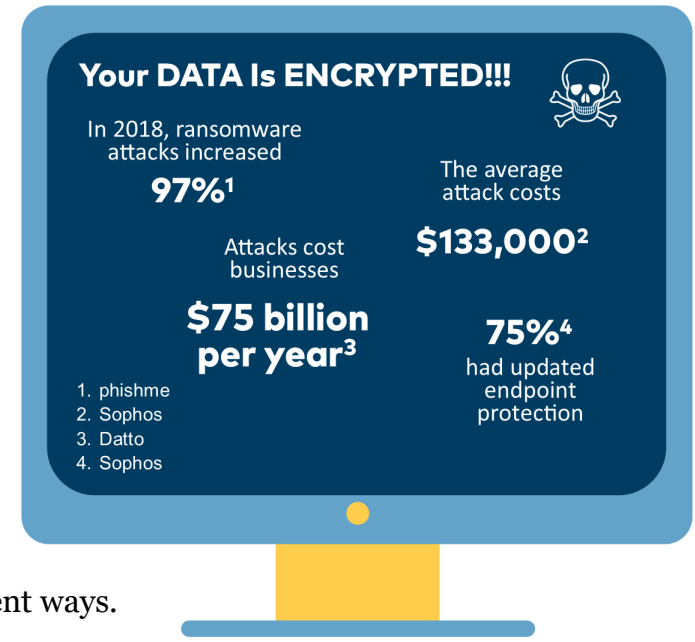
The pool will be closed on Monday, October 11, for Columbus Day. EON will be available but the system will not allow transactions to settle on the holiday.

(Continued from page 1)

- **Networking Vulnerabilities:** Some of the biggest, most newsworthy attacks have been launched through vulnerabilities identified by hackers related to missing operating system patches, outdated software releases, misconfigured firewalls, and the use of default passwords.

Unlike other types of malicious attacks (spyware, phishing, etc.), ransomware will make itself known. Usually, there is a pop-up informing the user that their data has been taken hostage. There may be a countdown clock, a description of how the data has been made inaccessible, and what the user may need to do to get it back.

Invariably, there is a price requested and instructions for how to pay it. The most frequent demand is for Bitcoin or some other cryptocurrency. However, gift cards, premium-rate SMS, or long distance telephone fees have also been reported. Some programs even employ negotiating tactics, such as offering some non-essential files back as a goodwill gesture, or using a tiered pricing structure based on how long it takes to pay the ransom. Ransomware attacks also often involve taking control of data and system resources used by public sector entities to deliver essential services (*e.g.*, healthcare, law enforcement, utilities, etc.), which increases the likelihood of a ransom getting paid.



Ransomware can take control of your device in many different ways. Some of the most common are listed below:

- A **Blocker** is a program that inhibits your ability to use the infected device. It could be a browser window that cannot be closed through the usual means, a fake software update window that demands action, a fake message from a law enforcement agency, or a program that floods the screen with unwanted images.
- **Encryption** is a technology that scrambles data to protect it from being read by anyone except those with the "key." The key is usually a random string of alphanumeric characters. Some forms of encryption can be reversed, but not without significant time and cost that is often beyond the value of the data. For this reason, blockers often claim encryption even if the data is not actually encrypted.
- **Leakware** is a form of ransomware that threatens to release sensitive information publicly instead of inhibiting access.

How Big of a Problem Is This Really?

According to industry experts, the damages caused by ransomware attacks have increased. This is partly due to hackers getting better at targeting institutions and organizations directly, especially those that have the resources to pay larger ransoms. In other words, your personal computer is less likely to be targeted or taken "hostage," but your work files could be a prized objective for cybercriminals.

(Continued on page 3)

Reporting Unclaimed Property

Earlier this year, Oregon's Unclaimed Property Program moved to Treasury. While the state agency behind the program may have changed, the program itself and the team that runs it remain focused on reuniting Oregonians with their uncashed checks, forgotten deposits and refunds, and other unclaimed money.

Across the state, Oregon governments, businesses, and nonprofits are doing their part, too. Each year, organizations in Oregon do their best to reach out to customers and contacts who may have unclaimed property. If those people can't be reached, the organizations then itemize and report any unclaimed funds to the state.

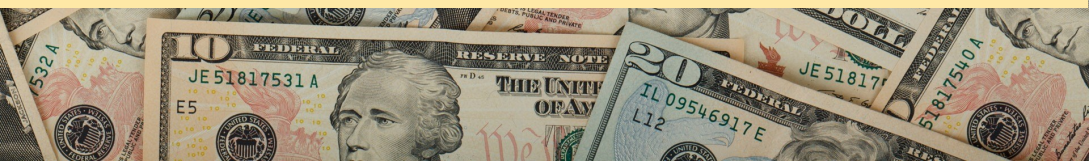
Oregon's annual unclaimed property reporting window runs from October 1 to November 1, 2021. All Oregon businesses—no matter how big or small they are—are required by law to report unclaimed funds to the state during the window. The same goes for state agencies, local governments, and nonprofits that hold unclaimed property.

Organizations can even report *incidental* unclaimed property for other states to Oregon unless having received specific instructions to report from the other state. Incidental property is no more than 10 items totaling $1000 or less for any state. *Note that an organization may be charged penalties and/or interest by the other state.*

After organizations report and remit unclaimed property to the state, the funds are held by Treasury in perpetuity. Oregonians can search for their names at unclaimed.oregon.gov to see if they are entitled to any unclaimed funds.

Learning how to report unclaimed property is just as easy. Treasury's Unclaimed Property website has information about reporting requirements, holding periods for different types of property, and instructions for requesting a reporting extension. We realize many organizations have faced extra hurdles during the pandemic, and we encourage you to request an extension if you need more time to report.

We welcome your questions about Oregon's Unclaimed Property Program. Visit unclaimed.oregon.gov/app/contact-us to reach out to staff. And spread the word to your employees and customers that a quick search at unclaimed.oregon.gov can help them see if Oregon is holding unclaimed property that belongs to them.



(Continued from page 2)

It is also important to note that the damages of a ransomware attack go well beyond the actual ransom—in fact, paying the ransom could be only the beginning. A ransomware attack can cost an organization millions in lost productivity and reputational damages, not to mention the time and resources it could take to get affected systems in working order again.

One reported attack on a large municipality was estimated to cost close to $17 million. That price tag may make it seem like a necessity to pay a few thousand in Bitcoin and move on. However, according to a survey conducted by betanews.com, paying the ransom resulted in the stolen files being returned only 26% of the time. Another source suggests the number is closer to 40%, but it underscores the point that there are often no easy answers to ransomware attacks once they have succeeded in locking users out.

Guidelines for Protecting against Ransomware

The good news is that there are ways to help prevent these kind of attacks.

- **Spam filters** can stop many attack e-mails, especially if they carry suspicious

(Continued on page 4)

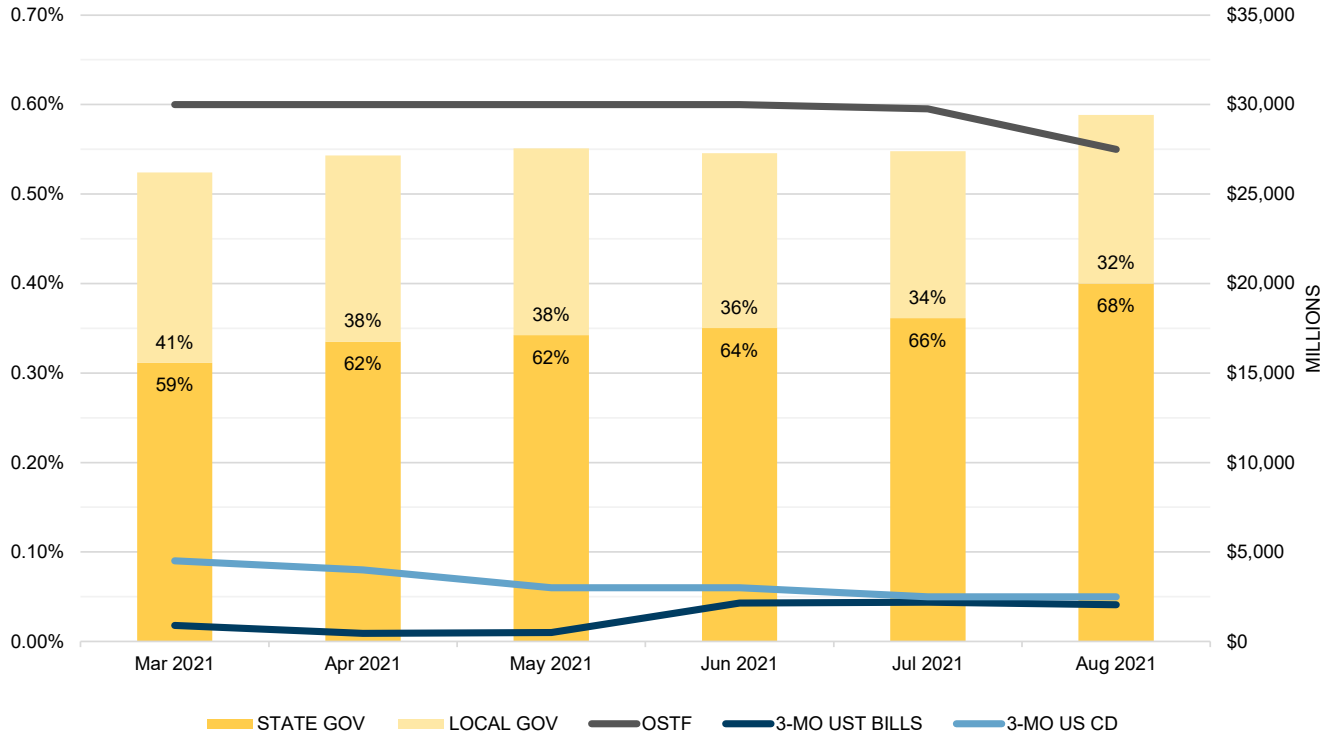
(Continued from page 3)

attachments, links, etc. Unfortunately, it takes only one e-mail to get through to cause significant damage. Therefore, end-users must be vigilant as well, understanding the risks associated with clicking on unknown links and downloading attachments. It is important for everyone to understand the current cyber risks that exist and their role in helping to avoid potential breaches, and to protect against cyber threats like ransomware. Nowadays, it is more likely you will need to use your cyber safety training than fire safety or medical emergency training.

- **Antivirus software** also plays an important role in protecting against ransomware, since it is a type of malware. While antivirus software may not prevent the next big breach, if kept up-to-date, it can be a good way to protect against more well-known forms of malware. To keep antivirus software and signatures up-to-date, it is recommended that regular computer scans be conducted.
- **Vigilance** applies to information technology processes and professionals as well. Some of the largest ransomware attacks took place after the weakness in a common operating system was already identified and a security patch was made available. A notable example of this is the WannaCry ransomware worm, which wrought an estimated $4 billion in damages by exploiting a loophole that was patched weeks before the worm became widespread. All organizations should have a routine process for distributing and installing critical security patches. They should also have trained security professionals who understand the vulnerabilities of their system and can take proactive steps to mitigate the risks.
- A **back-up system** that is largely independent from the regular network that users operate on a daily basis is one of the chief ways to mitigate ransomware risk. The separation is needed to ensure that a ransomware attack does not infect the back-up as well. Installing a back-up system will not prevent a cybersecurity threat, but it is a process that can make an attack less damaging, especially if ransomware is identified quickly.

Ransomware attacks have become a major feature of the cyber threat landscape for institutions of all sizes. Like phishing and social engineering attacks, it is no longer a question of whether or even when, but rather of how many attacks institutions will be exposed to on a daily basis. While the most sophisticated attacks may require equally sophisticated prevention measures, the majority can be avoided with widely available technology, a well-thought-out institutional approach to networks and data protection, and end-user education.

Oregon Short Term Fund Analysis



	Mar 2021	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021
TOTAL OSTF AVG DOLLARS INVESTED (MM)	26,212	27,154	27,554	27,281	27,393	29,416
STATE GOV PORTION (MM)	15,564	16,749	17,113	17,513	18,065	20,004
LOCAL GOV PORTION (MM)	10,648	10,405	10,441	9,768	9,328	9,412
OSTF ANNUAL YIELD (ACT/ACT)	0.60	0.60	0.60	0.60	0.60	0.55
3-MO UST BILLS (BOND EQ YLD)	0.018	0.009	0.010	0.043	0.044	0.041
3-MO US CD (ACT/360)*	0.09	0.08	0.06	0.06	0.05	0.05

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 respectivley) bank certificates of deposit and are quoted on a CD equivalent yield basis.

Market Data Table

	8/31/2021	1 Month	3 Months	12 Months		8/31/2021	1 Month	3 Months	12 Months
7-Day Agency Discount Note**	0.01	0.01	0.00	0.07	Bloomberg Barclays 1-3 Year Corporate YTW*	0.50	0.48	0.44	0.59
30-Day Agy Nt Disc**	0.01	0.03	0.00	0.08	Bloomberg Barclays 1-3 Year Corporate OAS*	0.33	0.33	0.31	0.52
90-Day Agy Nt Disc**	0.03	0.04	0.01	0.08	Bloomberg Barclays 1-3 Year Corporate Modified Duration*	1.83	1.85	1.88	1.89
180-Day Agy Nt Disc**	0.03	0.03	0.02	0.08					
360-Day Agy Nt Disc**	0.02	0.06	0.04	0.08	7-Day Muni VRDN Yield**	0.02	0.02	0.05	0.09
					O/N GGC Repo Yield**	0.06	0.05	(0.02)	0.12
30-Day Treasury Bill**	0.02	0.03	(0.00)	0.07					
60-Day Treasury Bill**	0.03	0.04	0.00	0.08	Secured Overnight Funding Rate (SOFR)**	0.05	0.05	0.01	0.09
90-Day Treasury Bill**	0.03	0.04	0.00	0.08					
6-Month Treasury Yield**	0.05	0.05	0.03	0.11	US 10 Year Inflation Break-Even**	2.34	2.40	2.45	1.80
1-Year Treasury Yield**	0.07	0.07	0.04	0.12					
2-Year Treasury Yield**	0.21	0.19	0.14	0.13	1-Day CP (A1/P1)**	0.14	0.13	0.03	0.07
3-Year Treasury Yield**	0.41	0.34	0.30	0.15	7-Day CP (A1/P1)**	0.12	0.12	0.03	0.10
					30-Day CP (A1/P1)**	0.09	0.08	0.04	0.12
1-Month LIBOR**	0.08	0.09	0.09	0.16					
3-Month LIBOR**	0.12	0.12	0.13	0.24	30-Day CD (A1/P1)**	0.08	0.06	0.04	0.12
6-Month LIBOR**	0.15	0.15	0.17	0.31	90-Day CD (A1/P1)**	0.11	0.11	0.10	0.19
12-Month LIBOR**	0.23	0.24	0.25	0.45	6-Month CD (A1/P1)**	0.15	0.16	0.14	0.26
Sources: *Bloomberg Index Services, **Bloomberg					1-Year CD (A1/P1)**	0.21	0.21	0.26	0.31

Director of Finance
Cora Parker
503.378.4633

Deputy Director of Finance
Mike Auman
503.378.2752

Newsletter Questions
Kari McCaw
503.378.4633

Bryan Cruz González
503.378.3496

Local-Gov-News Mailing List
omls.oregon.gov/mailman/listinfo/local-gov-news

Local Government Investment Pool
oregon.gov/lgip

PFM Client Services
855.OST.LGIP
cswestregion@pfm.com

- EON 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
350 Winter Street NE, Suite 100 ›› Salem, OR 97301-3896
oregon.gov/treasury