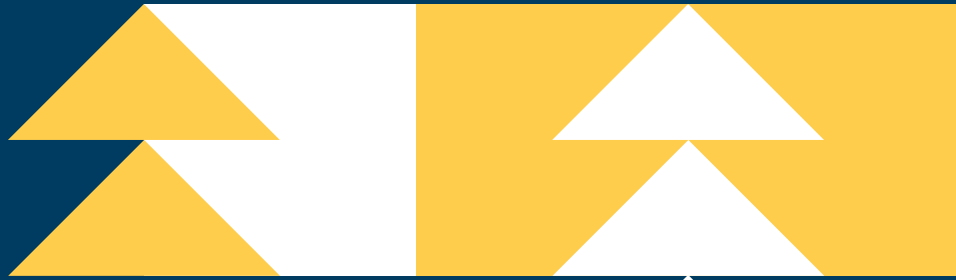# Inside the Vault

State Agency Edition

Spear Phishing Alert

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.

One Treasury customer recently fell victim to a spear phishing attack based on a legitimate vendor relationship. The customer received what appeared to be a legitimate request from a vendor to change the bank account information used to process payments. In actuality, the request was sent by a cybercriminal.

Service Spotlight

Remote Deposit Capture (RDC) is a service that allows an organization to deposit checks electronically by capturing an image of a check and sending the image to the organization's financial institution. The service requires use of a desktop check scanner and specialized software (either on-premises or software as a service). Because the check image becomes a legal substitute for the paper check, scanners must comply with industry standards for image quality.

RDC is an innovative and efficient alternative to processing paper checks and can result in enhanced cash flow and reduced processing costs—especially for agencies with multiple departments or locations receiving checks. Agencies can access RDC through Treasury or approved third party vendors. If you are interested in evaluating your business needs and available options or have questions regarding remittance processing methods generally, contact Customer Solutions at customer.solutions@ost.state.or.us.

Interest Rates

Average Annualized Yield

June	5.20%

Interest Rates

June 1–30	5.20%

(Continued from page 1)

The cybercriminal even provided a falsified bank verification letter. The customer subsequently sent payment to what the customer thought was the vendor's new bank account. After the payment was sent, the actual vendor contacted the customer indicating payment had not been received. It was then discovered that the updated bank account information had not been provided by the vendor but that the customer had been defrauded by a cybercriminal. The customer is currently working to recover some or all of the payment.

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 customer could have uncovered the fraud by calling the vendor at a known phone number and speaking with an authorized individual in order to confirm the requested change. When performing such a call-back process, it is important to use a phone number already on file and *not* one provided in connection with the requested change.

Read more about avoiding social engineering and phishing attacks on the U.S. Cybersecurity & Infrastructure Security Agency's blog.

Director of Finance
Cora Parker
503.378.4633

Deputy Director of Finance
Bryan Cruz González
503.378.3496

Business Continuity Analyst
Mara DuShane
503.378.8465

Policy Analyst
Ken Tennies
503.373.7453

Administrative Specialist
Kari McCaw
503.378.4633

▲ ▲ ▲

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

Analysts
Lyndsie DeOlus
Heidi Lancaster
Ellis Williams

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

ACH Origination
Ashley Moya
503.373.1944

**Check Fraud/Check Imaging/
Check Stock/Stop Payments**
Rebecca Jordan
503.566.9432

Fed Wires/Merchant Card
Shannon Higgins
503.378.5043

Local Government Investment Pool
Sarah Kingsbury
503.373.1501

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

Safekeeping/Debt Service
Sherry Hayter
503.378.2895

U.S. Bank
Nikki Main
503.378.2409

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

Manager
Brady Coy
503.378.2457

Cash Management Analyst
Natalya Cudahey
503.378.8256

Senior Business Analyst
Angel Bringelson
503.378.5865

Business Analyst
Cole Johnson
503.378.3359

**Contracted Project Manager
(TEK Systems)**
David Riffle
503.373.7864