

FOLLOW-UP REPORT

Technology Services and the Office of Human Resources **Phishing**

MARCH 2024



TIMOTHY M. O'BRIEN, CPA
DENVER AUDITOR

OFFICE OF THE AUDITOR
AUDIT SERVICES DIVISION, CITY AND COUNTY OF DENVER

Audit Team

Nicholas Jimroglou, CISA, CDPSE, Acting Information Systems Audit Manager

Rob Farol, CISA, CIA, CGAP, Information Systems Audit Senior

Dave Hancock, CISA, CISM, MURP, Information Systems Audit Senior

Other Contributors

Kristen M. Clark, Senior Communication and Reporting Specialist

Stelios Pavlou, Reporting Specialist

Jeff Neumann, Graphics and Visual Information Specialist

Audit Management

Timothy M. O'Brien, CPA, Auditor

Valerie Walling, CPA, Deputy Auditor

Dawn Wiseman, CRMA, Audit Director

Audit Committee

Timothy M. O'Brien, CPA, Chairman

Jack Blumenthal, Vice Chairman

Frank Rowe

Leslie Mitchell

Florine Nath

Charles Scheibe

Ed Scholz

You can obtain
copies of this
report by
contacting us:



Office of the Auditor

201 West Colfax Avenue, #705

Denver, CO 80202

(720) 913-5000

Or download and view
an electronic copy by
visiting our website at:
www.DenverAuditor.org.

Cover illustration by Denver Auditor's Office staff.

City and County of Denver



TIMOTHY M. O'BRIEN, CPA
AUDITOR

201 West Colfax Avenue, #705, Denver, Colorado 80202
(720) 913-5000 | www.DenverAuditor.org

AUDITOR'S LETTER

March 7, 2024

In keeping with generally accepted government auditing standards and Auditor's Office policy, as authorized by city ordinance, we have a responsibility to monitor and follow up on audit recommendations to ensure city agencies address audit findings through appropriate corrective action and to aid us in planning future audits.

In April 2021, we audited the City and County of Denver's phishing defenses and found risks involving which employees should be required to complete cybersecurity awareness trainings and how the Technology Services agency communicates phishing metrics to other agencies. Technology Services and the Office of Human Resources agreed to implement all seven of our recommendations.

We recently followed up on our original report and found the Office of Human Resources fully implemented its one recommendation, while Technology Services fully implemented only three recommendations and the three others remain not implemented.

Although Technology Services has made some progress, it did not fully address all the risks associated with our original findings. Consequently, we may revisit these risk areas in future audits to ensure the city takes appropriate corrective action.

We appreciate the leaders and team members at Technology Services and the Office of Human Resources who shared their time and knowledge with us throughout the audit and the follow-up process. Please contact me at 720-913-5000 with any questions.

Denver Auditor's Office

A handwritten signature in black ink, appearing to read "Timothy M. O'Brien".

Timothy M. O'Brien, CPA
Auditor

ORIGINAL REPORT HIGHLIGHTS

Phishing

Original Report Issued:

APRIL 2021

Follow-up Report Issued:

MARCH 2024

Objective

To assess:

- How well the city identifies, prevents, detects, and responds to cybersecurity phishing incidents.
- The effectiveness of the city’s cybersecurity awareness training by conducting internal and external phishing campaigns.
- The effectiveness of the city’s email security tools, such as Proofpoint, to determine whether the tools are configured appropriately to provide adequate email security.

Background

“Phishing” is a type of cybercrime where a nefarious actor, posing as a legitimate person or business, attempts to lure an unsuspecting person or organization into sharing sensitive information. The information can then be used to access systems or important accounts – which can result in identity theft, data loss, and financial loss.

The city’s Cybersecurity Awareness Training Program improved employee behavior to a limited extent but lacked recommended content and not all employees completed routine training

We found employees who took all six city training courses offered in the first three quarters of 2020 were 9.6 percentage points less likely to submit sensitive information, such as their username and password, after receiving a phishing email compared to employees who took no training.

We also found that those who completed trainings recently performed better than those who had not. However, not all employees within the city completed cybersecurity training because the city had not yet identified which specific employees needed to take it.

Technology Services needed to track phishing metrics and communicate them to other city agencies

We found the city’s Technology Services agency did not formally communicate phishing metrics to other City and County of Denver agencies.

WHY THIS MATTERS

Simulated phishing attacks, trainings, and gathering metrics on these simulations and trainings help raise awareness among city employees and managers on how to recognize and avoid malicious cyber threats. Proactive steps taken by the city help reduce the overall risk cyber threats pose.



4

FULLY IMPLEMENTED



0

PARTIALLY IMPLEMENTED



3

NOT IMPLEMENTED

March 7, 2024



Action Since Audit Report

Phishing

7 recommendations proposed in April 2021

The Office of Human Resources fully implemented the one recommendation we made to it in the original audit report. Meanwhile, Technology Services fully implemented three recommendations, but it has not taken steps to address the risks the three remaining recommendations had sought to resolve.

By fully implementing four recommendations, the city is conducting phishing simulations and offering similar cybersecurity awareness trainings to the employees who need it most. These trainings will help make users of city systems aware of risks when clicking a link from a malicious email and deter them from doing so.



FULLY
IMPLEMENTED

4



PARTIALLY
IMPLEMENTED

0



NOT
IMPLEMENTED

3

REMAINING RISKS

The three recommendations Technology Services did not implement present several lingering risks. Among them:

- By not developing key phishing metrics — such as reconciling who has completed trainings, monitoring click rates, and identifying targeted agencies — the city remains vulnerable to cyber threats. And it lacks standard performance indicators to make informed decisions.
- Not communicating phishing metrics to other city agencies limits the city's ability to collectively share knowledge about which agencies are more vulnerable to cyber threats. This weakens the overall security defenses of the city.

FINDING 1 | The city's Cybersecurity Awareness Training Program improves employee behavior to a limited extent but lacks recommended content and not all employees complete routine training

RECOMMENDATION	IMPLEMENTATION STATUS
1.1 Identify employee job types	● FULLY IMPLEMENTED
1.2 Offer training to the correct sets of employees	● FULLY IMPLEMENTED
1.3 Reconcile trainings	● NOT IMPLEMENTED
1.4 Evaluate training content	● FULLY IMPLEMENTED
1.5 Train employees every six months	● FULLY IMPLEMENTED

Recommendation 1.1



FULLY IMPLEMENTED

IDENTIFY EMPLOYEE JOB TYPES – The Office of Human Resources should complete its work to accurately identify employees' job types in Workday and better define the data associated with each job type.

Agency's original target date for completion: Dec. 31, 2021

SUMMARY OF AGENCY ACTION

Since our original audit, the Office of Human Resources improved information for active workers in Workday, the city's system of record. This project resulted in accurately identifying employees' job types in Workday as well as the data associated with each job type. We verified this through a Workday report of active employees.

That report included changes like:

- Recognizing the newly identified intergovernmental affiliated workers.
- Reducing election judge job profile categories from four to one.
- Adding independent contractor and vendor information.

Office of Human Resources leaders said further changes to employee job types will not be required. Once job types are entered into Workday correctly, there is no further need to update them. Any remaining incorrect Workday active user data will be addressed through continued quarterly cybersecurity training that may contain phishing topics. These quarterly trainings are now required of all active users on the network. Additionally, Technology Services conducts frequent phishing simulation campaigns and

remedial trainings for all users of the network throughout the year.

Therefore, we consider this recommendation fully implemented.

Recommendation 1.2

OFFER TRAINING TO THE CORRECT SETS OF EMPLOYEES – Technology Services should work with the Office of Human Resources to gather the necessary data to better define which employees should receive cybersecurity awareness trainings and ensure that those individuals are being offered training throughout the year.



**FULLY
IMPLEMENTED**

Agency's original target date for completion: Dec. 31, 2022

SUMMARY OF AGENCY ACTION

As we discussed in the implementation of Recommendation 1.1, the Office of Human Resources included employee detail in Workday to further assist Technology Services in defining which employees should receive cybersecurity awareness trainings. This additional information allows Technology Services to identify which trainings and simulations each employee should receive according to their job type.

In addition to these changes, Technology Services developed a policy for cyber and data protection awareness. Technology Services intends to have all city employees who have access to a computer connected to the network – or application access through any connection including their phone – take all quarterly cybersecurity trainings for awareness. However, this is not yet written into the policy and a date for completing this change has not been established.

According to Technology Services' policy, every city employee is required to receive phishing simulations with a certain number of employees by agency receiving the simulations during each six-week campaign cycle. Technology Services monitors phishing simulations to see which employees click on them.

If a user fails two simulated phishing attacks in a row, the user is required to complete remedial training. If the user continues to fail simulated attacks, Technology Services is considering taking further disciplinary action.

Because Technology Services officials demonstrated they have fully addressed the identified risk, we consider this recommendation fully implemented.

Recommendation 1.3



**NOT
IMPLEMENTED**

RECONCILE TRAININGS – Technology Services should reconcile the list of individuals who should receive trainings with a list of those who actually complete it through Workday Learning.

Agency’s original target date for completion: June 30, 2021

SUMMARY OF AGENCY ACTION

When we followed up on this recommendation, Technology Services officials said they had fully implemented it but we found no evidence to support this claim.

Cybersecurity training and phishing simulations are required by the Cyber and Data Protection Awareness policy and are conducted quarterly. However, Technology Services is not tracking completion or providing statistics to agencies for phishing simulations to ensure completion and compliance.

When we specifically asked about metrics the agency tracks for compliance, Technology Services personnel and managers said the agency is not maintaining any dashboards to monitor compliance for training or phishing campaigns.

Technology Services plans to collect this information, but there is no timetable for when collection and reporting will start. As a result, we could not compare the individuals who should receive trainings with a list of those who completed it using Workday Learning, as prescribed by the recommendation.

By not collecting and reporting standard metrics on training completion and phishing simulation data for agencies, Technology Services will miss opportunities to make informed decisions on which employees need it most.

Therefore, we consider this recommendation not implemented.

Recommendation 1.4

EVALUATE TRAINING CONTENT – Technology Services should evaluate the content of the trainings it offers each quarter and each year to ensure the training is effective. It should make selections to improve employees’ behavior and knowledge. Specific reminders to use end-user tools, such as the “Report Phish” button, are recommended and should be in line with best practices. Trainings should include assessments to ensure employees understand the knowledge being taught and surveys should be provided to solicit employees’ feedback on the trainings



**FULLY
IMPLEMENTED**

Agency’s original target date for completion: Dec. 31, 2022

SUMMARY OF AGENCY ACTION

Technology Services staff said the content of trainings is evaluated through Proofpoint, the city’s vendor for email security. They said Proofpoint’s platform reflects current threat simulations.

Technology Services officials select the cybersecurity trainings to be completed by city employees each quarter, which include topics focused on phishing scams. The proposed cybersecurity trainings are reviewed by agency leaders and, if approved, provided to employees as quarterly trainings in Workday Learning.

We reviewed an email seeking leadership feedback and approval for the proposed security awareness training. This email demonstrates Technology Services’ continuous efforts to evaluate the content of its trainings.

Employee awareness is a top concern for Technology Services, so phishing simulations using Proofpoint provide an important learning tool to try to prevent successful phishing scams. As discussed in the implementation of Recommendation 1.2, Technology Services performs targeted phishing simulations, which are also carried out through Proofpoint. Technology Services considers these phishing simulation campaigns to be training since they have the same outcomes for the employee by teaching them awareness and informing them of the risks of clicking on a phishing email scam.

The city’s Proofpoint consultant conducts research to determine which phishing topics are most relevant for the upcoming quarter and selects simulations they believe are the best fit for the city’s employees.

Because trainings and campaigns are being evaluated, we consider this recommendation fully implemented.

Recommendation 1.5

TRAIN EMPLOYEES EVERY SIX MONTHS – Technology Services should train employees on a comprehensive set of phishing cues and do so at least once every six months. This should include such phishing cues as those noted in Appendix B of (the original) report.



**FULLY
IMPLEMENTED**

Agency’s original target date for completion: Dec. 31, 2022

SUMMARY OF AGENCY ACTION

As discussed, Technology Services uses Proofpoint to conduct regular

phishing simulations twice a quarter on users of the city's network. Users targeted for phishing campaigns are randomly selected by agency, with periodic coverage for all users.

Technology Services also focuses on people more likely to be attacked based on the employee's role. If a "very attacked" user clicks on a phishing simulation email and subsequently fails the simulation, they receive a warning and are offered retraining.

Technology Services officials said the agency's intent is to have all city employees who access the city's network take all quarterly cybersecurity trainings in Workday Learning, including those focused on phishing.

Technology Services' data protection team and security team coordinate phishing trainings that include various phishing cues for city staff. These simulations include spelling and grammar errors, URL hyperlinking, domain spoofing, corporate brand imitation, and mimicking common business processes.

Therefore, we consider this recommendation fully implemented.

FINDING 2 | Technology Services should track phishing metrics and communicate them to other city agencies

RECOMMENDATION

IMPLEMENTATION STATUS

2.1 Develop phishing metrics

● NOT IMPLEMENTED

2.2 Communicate phishing metrics

● NOT IMPLEMENTED

Recommendation 2.1



**NOT
IMPLEMENTED**

DEVELOP PHISHING METRICS – Technology Services should gather the information necessary to develop key phishing metrics that can be reported to other city agencies. This could include click rates, reporting rates, repeat offenders, etc.

Agency's original target date for completion: Sept. 30, 2021

SUMMARY OF AGENCY ACTION

During our follow-up, we learned Technology Services has not developed standard metrics for quarterly Workday cybersecurity trainings, which may or may not contain phishing topics, nor does the agency have standard metrics to measure phishing campaigns conducted throughout the year.

The Technology Services analyst overseeing Proofpoint's phishing campaigns said a data analytics team is collecting available data in Proofpoint to create a dashboard that may include recommendations such as click-through rates, reporting rates, and users or agencies who repeatedly fail to identify phishing attempts.

But during our follow-up, we found these changes had not been implemented.

For quarterly Workday cybersecurity training, user data can be extracted by employee, agency, and cost center to determine whether the quarterly training was done. But we were not provided with tracking reports over time to identify trends like those employees who repeatedly do not complete or who fail quarterly training. Furthermore, there is no reporting specific to a standard set of phishing metrics.

By not developing standard phishing metrics to communicate results to stakeholders as recommended, other city agencies continue to be unaware

of how their agency and their employees are performing with regard to phishing incidents. City agencies may be unable to monitor and track their performance to see whether they are at, above, or below expectations. This lack of communication enhances the risk that malicious threats succeed, resulting in possible data loss, fines, and reputational damage.

As a result, we consider this recommendation not implemented.

Recommendation 2.2

COMMUNICATE PHISHING METRICS – Once Technology Services develops phishing metrics, Technology Services should communicate the phishing metrics to other city agencies and explain why the metrics are being communicated to them and what to do with the metrics (e.g., identify areas of improvement for employees).



**NOT
IMPLEMENTED**

Agency's original target date for completion: Dec. 31, 2021

SUMMARY OF AGENCY ACTION

As discussed related to Recommendation 2.1, Technology Services has not created standard phishing metrics for its Proofpoint campaigns nor its quarterly cybersecurity trainings in Workday Learning. Therefore, we could not test implementation for this recommendation.

By not tracking and reporting out on quarterly cybersecurity training completion rates, Technology Services is not enforcing requirements that employees complete quarterly cybersecurity trainings and the agency is also not monitoring and reporting on those employees who repeatedly fail to recognize phishing attacks in simulated campaigns.

Because it has not chosen standard phishing metrics to track and report out on, it cannot communicate agency compliance and employee awareness to agency and Technology Services leadership periodically. Therefore, agencies may not be aware to discipline or properly train employees to comply on time, which continues to put agencies and the city at risk for data loss, fines, reputational damage, etc.

Therefore, we consider this recommendation not implemented.

Office of the Auditor

The **Auditor** of the City and County of Denver is independently elected by the residents of Denver. He is responsible for examining and evaluating the operations of city agencies and contractors for the purpose of ensuring the proper and efficient use of city resources. He also provides other audit services and information to City Council, the mayor, and the public to improve all aspects of Denver's government.

The **Audit Committee** is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities regarding the integrity of the city's finances and operations, including the reliability of the city's financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of city operations, thereby enhancing residents' confidence and avoiding any appearance of a conflict of interest.



201 West Colfax Avenue, #705

Denver, CO 80202

(720) 913-5000

www.DenverAuditor.org

Our Mission

We deliver independent, transparent, and professional oversight in order to safeguard and improve the public's investment in the City and County of Denver. Our work is performed on behalf of everyone who cares about the city, including its residents, workers, and decision-makers.
