Technology Services and the Office of Human Resources

Phishing

APRIL 2021
Audit Team
- Jared Miller, CISA, CFE, IT Audit Supervisor
- Samuel Gallaher, PhD, Audit Analytics Supervisor
- Ryan Dougherty, CIA, CISA, CFE, CRMA, MAcc, Audit Supervisor
- Robert Persichitte, CPA, CFE, Lead Data Analytics Auditor
- Brian Cheli, CISSP, CISA, Senior IT Auditor

Audit Management
- Timothy M. O’Brien, CPA, Auditor
- Valerie Walling, CPA, CMC, Deputy Auditor
- Dawn Wiseman, CRMA, Audit Director
- Katja E. V. Freeman, MA, MELP, Audit Director

Audit Committee
- Timothy M. O’Brien, CPA, Chairman
- Rudolfo Payan, Vice Chairman
- Jack Blumenthal
- 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 | Fax (720) 913-5253

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

Cover illustration by Denver Auditor’s Office staff.
April 15, 2021

Our objective in auditing the City and County of Denver’s phishing defenses was to determine whether the city offers effective cybersecurity awareness training based on leading practices. I am pleased to present the results of this audit.

The audit found that employees who took the city’s cybersecurity awareness training courses were less likely to submit sensitive information, such as usernames and passwords, when attacked with a phishing email compared to employees who took no training. The audit also found that employees who completed their training recently performed better than those who had not. However, the city has not adequately defined which specific employees should be required to complete the training. Lastly, the audit found Technology Services could improve its process for communicating phishing metrics to other city agencies.

The city can better protect against phishing attacks by implementing recommendations to more accurately identify employees’ job types in the city’s system of record and to better define the risks associated with each job type. This will allow the city to determine who should receive cybersecurity awareness training and ensure that those individuals are being offered training each year.

Our audit work identified additional details related to the risks described in this report as well as other risks for the city to address. Because these details are sensitive in nature, we provided them directly to the relevant city agencies for remediation.

This performance audit is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, “General Powers and Duties of Auditor.” We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We extend our appreciation to the personnel in the city’s Technology Services agency and Office of Human Resources who assisted and cooperated with us during the audit. For any questions, please feel free to contact me at 720-913-5000.

Denver Auditor's Office

Timothy M. O’Brien, CPA
Auditor
Phishing
APRIL 2021

Objective

To assess:
1. How well the city identifies, prevents, detects, and responds to cybersecurity phishing incidents.
2. The effectiveness of the city’s cybersecurity awareness training by conducting internal and external phishing campaigns.
3. 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 Improves Employee Behavior to a Limited Extent but Lacks Recommended Content and Not All Employees Complete 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 complete cybersecurity training because the city has not yet identified which specific employees need to take it.

Technology Services Should Track Phishing Metrics and Communicate Them to Other City Agencies

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>BACKGROUND</td>
<td>1</td>
</tr>
<tr>
<td>FINDING 1 AND RECOMMENDATIONS</td>
<td>5</td>
</tr>
<tr>
<td>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</td>
<td></td>
</tr>
<tr>
<td>FINDING 2 AND RECOMMENDATIONS</td>
<td>14</td>
</tr>
<tr>
<td>Technology Services Should Track Phishing Metrics and Communicate Them to Other City Agencies</td>
<td></td>
</tr>
<tr>
<td>AGENCY RESPONSE TO AUDIT RECOMMENDATIONS</td>
<td>17</td>
</tr>
<tr>
<td>OBJECTIVE, SCOPE, AND METHODOLOGY</td>
<td>22</td>
</tr>
<tr>
<td>APPENDICES</td>
<td>23</td>
</tr>
<tr>
<td>Appendix A – Methodologies for a Random Control Trial of an Internal Phishing Simulation</td>
<td>23</td>
</tr>
<tr>
<td>Appendix B – Phishing Message Cues</td>
<td>25</td>
</tr>
</tbody>
</table>
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.¹

In classic email phishing attacks, cybercriminals send out mass emails—also known as a phishing campaign—to a large target audience of individuals' personal accounts or company accounts.² These mass phishing emails are often not personalized because they go to numerous people. Email phishing scams may attempt to entice recipients into clicking a link that leads them to a malicious webpage. These pages then attempt to trick recipients into providing their personal information or installing malicious files on their devices. The phishing email may also contain a malicious file or link to malicious content that may include viruses or malware.

For example, opening a harmful attachment from a phishing email—like a PDF file or a Microsoft Word document—can trigger a process that installs malware. Malware, or malicious software, can be used to compromise computer functions, steal data, bypass controls, or cause other harm to its host. The various types of malware include rootkits, spyware, and viruses.

Other types of phishing include “smishing,” “vishing,” and “spear phishing.”

- **Smishing** — derived from the words “SMS” and “phishing” — is phishing via text message.
- **Vishing**, or voice phishing, is a form of cyberattack where hackers call their targets instead of using email or text message. When vishing, hackers often use an autodialer to send robotic calls to a mass audience to steal information.

---

Spear-phishing attacks occur when a cybercriminal sends targeted, more personalized emails. Instead of a mass phishing campaign, the cybercriminal identifies specific individuals and personalizes each email by using the target's name and information about them gathered from social media or websites.

“Whaling” is a form of spear phishing aimed at high-level officials, such as a company's chief executive officer or chief financial officer. In whaling attacks, cybercriminals often attempt to trick the target into making high-value money transfers.

Phishing attacks can have severe consequences for an organization, such as:

- Downtime hours for end users.
- Time spent by information security teams remediating the phish.
- Damage to the organization's reputation.
- Direct monetary losses, such as from wire transfer fraud.
- Compliance issues and/or fines.
- Legal fees.
- Lost revenue from system or operational downtime.

City Cybersecurity Training Program

The city's Technology Services agency, in collaboration with the Information Governance Committee and the Office of Human Resources, is responsible for creating, developing, and delivering the content of the city's cybersecurity program. City employees are supposed to complete cybersecurity training annually to ensure they understand the risks and comply with their role in keeping the City and County of Denver's information secure.

The city's Executive Order No. 143 authorized the formation of the Information Governance Committee — which provides guidance and oversight for the development, adoption, and revision of policies, standards, and procedures so that the city can meet regulatory rules, contractual terms, or recognized standards of data privacy, security, and information governance.

In July 2018, the committee issued a policy that overlays the requirements for cybersecurity with fair information practice principles, which are “a set of standards governing the collection and use of sensitive information and addressing issues of privacy and accuracy.”

---


The purpose of the policy is “to establish the expectations and requirements for completing all required training.” It applies to all City and County of Denver employees who comprise the city’s career-service employees, classified-service employees, volunteers, and contingent workers who connect to the city’s network.

In 2019, Technology Services began offering mandatory cybersecurity trainings each quarter. Figure 1 shows a timeline of these required quarterly trainings from the fourth quarter of 2019 through the fourth quarter of 2020.

---

**FIGURE 1. Training Timeline**

<table>
<thead>
<tr>
<th>Q4 2019</th>
<th>Q1 2020</th>
<th>Q2 2020</th>
<th>Q3 2020</th>
<th>Q4 2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security Essentials</td>
<td>• Data Privacy</td>
<td>• Password Management</td>
<td>• Phishing Emails in Real Life</td>
<td>• What Is It, My Child? (Incident Reporting)</td>
</tr>
<tr>
<td>• Introduction to Phishing</td>
<td></td>
<td>• Email Protection Tools</td>
<td>• Ethical Use of Data</td>
<td></td>
</tr>
<tr>
<td>• Protecting Against Ransomware</td>
<td></td>
<td>• Report a Phish</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: Graphic designed by Auditor’s Office staff using information from Technology Services.

---

**Protecting Employees through Training**

Reports show that 91% of all cyberattacks begin with a phishing email to an unsuspecting user.⁶ According to Proofpoint, organizations should aim for less than 5% of their employees to fall victim to a phishing attack and for 70% of their employees to report an attempted phishing attack.

Simulated phishing attacks help organizations assess these rates, and as of 2020, 66% of U.S. organizations used simulated phishing attacks on their employees.⁷ Employees who are tested more frequently tend to fall victim less when faced with a phishing attack.

A successful cybersecurity awareness program within an organization may include having a designated team of cybersecurity awareness professionals, offering role-based cybersecurity awareness trainings, incorporating metrics, and communicating cybersecurity awareness within the organization.

---


Organizations like the city can use other tools beyond training to help protect their employees from phishing attacks. For example, the City and County of Denver uses Proofpoint, which provides a set of tools to protect end users from phishing attacks.

Proofpoint helps protect the city by filtering incoming emails for messages that may contain viruses, spam, or inappropriate content. Using machine learning, Proofpoint can quarantine email messages that it suspects are malicious so that they can be reviewed by an information security professional in the city.

The city’s email security tools also include a “Report Phish” button for employees to report potential phishing emails to Technology Services. The city provided employees with instructions on how to report a phishing email when checking their email in Microsoft Outlook, the city’s email platform. When an employee clicks the “Report Phish” button, it engages another security protocol that then pulls the email from the city’s entire email system.

Finally, the city uses multifactor authentication across many of its systems. Multifactor authentication, also known as “two-factor authentication,” requires users to present two types of credentials when logging in to an account or system (e.g., a password and a code sent to the user’s cellphone). Multifactor authentication is an added layer of protection because a malicious actor who acquires a user’s password would still be blocked from accessing the system unless they had a second type of authentication.
FINDING 1 AND RECOMMENDATIONS

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

We conducted a citywide experiment to test both the city’s organizational security and city employees’ behavior when faced with an email sent by a malicious actor seeking to send malware or gather sensitive information — a type of fraud known as “phishing.”

While we found city employees are not meeting recommended standards for responding to and reporting phishing emails, our analysis did find a positive but limited impact of the city’s cybersecurity training on the employees who engaged with a phishing email. We also found that some of the employees who are not required to take the city’s cybersecurity trainings are among the employees who engaged with the simulated phishing emails.

INTERNAL PHISHING SIMULATION – Our experiment consisted of a randomized control trial with two simulated phishing emails. Each email included a link-based test and a data entry-based test. URLs are a primary method for delivering malicious files like malware, so a link-based test includes an embedded hyperlink in the email.

One email served as the experiment’s control, or baseline. The audit team designed this email to be easily identifiable by including multiple cues of a phishing email (e.g., misspelled words, a hyperlink with a nonsensical domain name, and a login page with obvious visual errors and errors within the URL).

The second email was the test of the experiment. The team designed this hard-to-identify email to replicate a well-manicured phishing email.

To identify participants in our simulation, we randomly selected 6,590 individuals from a total population of 13,147 city employees from across almost all agencies who had either a denvergov.org or denverda.org email account.

Additional Risks

Our audit work identified additional details related to the risks described in this finding as well as other risks for the city to address. Because these details are sensitive in nature, we provided them directly to the relevant city agencies for remediation.

8 A city employee includes all full-time and part-time employees, interns, contingent employees, sworn officers, cadets, or individuals with an active email account with the city.
email. We did not include the Auditor’s Office in this simulation. Next, we randomly assigned half the sampled individuals to receive the test email and the other half to receive the baseline.

Each group included VIP and non-VIP employees. A VIP user is someone who has elevated access to city systems. In total, we included 342 VIP employees and 6,248 non-VIP employees in our sample.

We sent the two emails concurrently and they were active for about four hours before the city’s email security controls activated and pulled the emails from all inboxes.

We measured four outcomes from this test:

- When an employee clicked on the link in the phishing email, or link-based test failures.
- When those who clicked the link then submitted their credentials through the fake login page, or data entry-based test failures.
- When the employee notified Technology Services they received a potential phishing email using the “Report Phish” option in Microsoft Outlook, or the reporting rate.
- When an employee took no action.

We analyzed these results using logistic regression models — a statistical tool to isolate the effects of different variables on binary outcomes (e.g., whether the participant attempted to submit information). The models included the employee’s tenure with the city, job type, management level, VIP status, and the number of cybersecurity trainings they completed in 2018, 2019, and the first three quarters of 2020. Because of the random and baseline elements of the research design and because of the large sample size, the results showed with high levels of confidence the efficacy of the city’s training program and identified high-risk groups in the city.

Overall, and as seen in Figure 2 on the next page, our results showed city employees clicked the links in the emails about 10% of the time and submitted credentials through the fake login page about 7% of the time. City employees reported phishing emails only 2% of the time.

---

9 Because of the proximity in time of the simulation to the 2020 presidential election, we also did not include the Office of Emergency Management and Homeland Security nor the Clerk and Recorder’s Office in the experiment. Denver.gov and Denverda.org are both protected by the same security control structure. Other domains used by the city (e.g., flydenver.com) have different controls and therefore were not included in this experiment. The simulation for emails included in the District Attorney’s Office domain was ended early upon request. Therefore, analyses presented in this report should not be attributed to the denverda.org group.

10 When no action was taken, we could not determine how many participants did not see the email, saw the email in their inbox and did nothing, or read the email and did nothing.
FIGURE 2. Results of Internal Phishing Simulation compared to Suggested Rates and Industry Averages

<table>
<thead>
<tr>
<th></th>
<th>Link-based failure rate</th>
<th>Data entry-based failure rate</th>
<th>Reporting rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proofpoint suggested rate</td>
<td>5%</td>
<td>5%</td>
<td>70%</td>
</tr>
<tr>
<td>Government average rate</td>
<td>14%</td>
<td>4%</td>
<td>15%</td>
</tr>
<tr>
<td>Baseline email (3,295 participants)</td>
<td>2.5% (81)</td>
<td>0.03% (1)</td>
<td>7.1% (235)</td>
</tr>
<tr>
<td>Test email (3,295 participants)</td>
<td>10.4% (344)</td>
<td>7.2% (238)</td>
<td>2% (65)</td>
</tr>
</tbody>
</table>

Source: Auditor’s Office analysis of phishing simulation results.

Proofpoint recommends organizations have a failure rate lower than 5%. Proofpoint also says the average failure rates for government entities are 14% for link-based tests and 4% for data entry-based tests at the organizational level.\(^{11}\) Proofpoint further recommends organizations have over 70% reporting rates for phishing emails.

While we found the city is not meeting recommended standards for link-based and data entry-based failure rates and for reporting rates, our analysis shows city training has a positive but limited impact on the employees engaging with a phishing email.

The City’s Cybersecurity Trainings Should Be Evaluated for More Recommended Content

The City and County of Denver offered six cybersecurity trainings to city employees in the first three quarters of 2020, and we found these were effective in reducing employees’ likelihood of falling victim to a phishing attack.\(^{12}\)

For example, if an individual had taken all required cybersecurity trainings in the first three quarters of 2020, the probability of submitting information on the phishing landing page of the hard-to-identify (i.e., test) email reduced from 18.6% with no training to 9% with all six trainings completed — a decrease of 9.6 percentage points.\(^{13}\) However, while the probability of submitting information reduced with training, even those

---


\(^{12}\) The city provided a total of eight trainings in 2020, but the phishing simulation was completed before the final two trainings were held in the last quarter of the year.

\(^{13}\) Only one individual submitted information for the easy-to-identify email. Our analysis showed the likelihood of submitting information from the hard-to-identify email was 267% higher than the easy-to-identify email. We observed similar reductions in click-based failure rates for those who took six trainings compared to zero trainings.
who completed all trainings submitted sensitive information at higher rates than standards recommend.

Furthermore, our internal phishing simulation showed city employees reported phishing emails to Technology Services at a lower-than-recommended rate. For example, when looking at the reporting levels from our easy-to-identify (i.e., baseline) email, a city employee who did not take any cybersecurity training in the first three quarters of 2020 reported the email 3.3% of the time, while those who completed the six trainings during that time reported the email 12.3% of the time — an increase of 9 percentage points.

By comparison, when examining the reporting of the test email, those who completed no trainings in the first three quarters of 2020 reported the email less than 0.8% of the time, while those who completed all six trainings during that time reported the email 3.3% of the time, an increase of 2.5 percentage points. These differences, depicted in Figure 3, are statistically significant.

![FIGURE 3. Change in Employee Behavior after Completing Cybersecurity Training](image)

**Note:** Graphic designed by Auditor’s Office staff using information from Auditor’s Office’s phishing experiment data.

Our experiment shows a higher link-based and data-entry failure rate for the test email than the baseline email and a lower reporting rate for the test email than the baseline. Because of the random assignment of the two emails, we can conclude the differences observed in the failure and reporting rates between the two emails were because of the different cues designed in those emails.

In 2020, the National Institute of Standards and Technology — a laboratory and nonregulatory federal agency within the U.S. Department of Commerce — identified a list of cues objectively present in phishing messages.¹⁴

Phishing cues can be taught during phishing awareness trainings to help employees identify current real-world threats. Federal standards say, at a minimum, the entire workforce should be exposed to awareness material annually. A continuous awareness program, using various methods of delivery throughout the year, can be very effective.\(^{15}\)

Furthermore, a study presented at the 2020 Symposium on Usable Privacy Security found the effect of phishing training diminishes after six months.\(^{16}\)

After we assessed the content of the city's cybersecurity training program — in conjunction with our analysis of the simulation results — we concluded the trainings do not fully prepare employees to respond to phishing emails or ensure employees fully understand the material.

For example:

- Role-based training was not part of any of the five quarterly cybersecurity and data protection trainings we reviewed.
- Surveys were given in only one of the five quarterly cybersecurity and data protection trainings we reviewed.
- Assessments and/or quizzes were given in only two of the five quarterly cybersecurity and data protection trainings we reviewed.

The following “phishing cues” exceeded a six-month period without being part of quarterly cybersecurity and data protection trainings offered from the fourth quarter of 2019 to the fourth quarter of 2020:

- Spoofed email addresses were not a part of quarterly trainings for a nine-month period.
- Branding and/or logos were not a part of quarterly trainings for a nine-month period.
- “Too good to be true” scenarios were not a part of quarterly trainings for a nine-month period.
- Humanitarian appeals were not a part of any of the five quarterly trainings we reviewed.

This assessment aligns with the results of our experiment.

The city’s cybersecurity trainings also did not always include information or guidance on how to report a phishing email using city-specific tools.

---


like the “Report Phish” button in Microsoft Outlook. While some of this information was provided at the recommended cadence of at least every six months, it could be helpful going forward to have a static reminder that focuses on city-specific functionality and tools as well as a broader set of phishing-related information.

Our analysis found older trainings had less effect on behavior, which highlights the importance of frequent trainings. For example, our analysis showed that only the city's 2020 cybersecurity awareness trainings reduced an individual's likelihood of submitting information when phished.

Furthermore, our testing found that even though training reduced the risk of an individual engaging with a phishing email, when city employees were presented with a phishing email with specific elements, the rate of engagement with the phishing email increased, and city employees reported phishing emails to Technology Services at a lower-than-recommended rate. As such, we determined that the lack of consistent content in these trainings is a cause for these issues.

The city may be more susceptible to a phishing attack and subsequent data loss if an attack includes elements not covered by the cybersecurity training. Link-based and data entry-based engagement with a phishing email can cause data breaches or system failures.

Furthermore, while the city has multiple automated controls that prevent phishing emails from reaching city employees’ inboxes, the “Report Phish” function is also important. When city employees do not report a phish to Technology Services and Technology Services’ other controls do not block a phishing email, dangerous emails could be left in employee inboxes.

City employees whose last training was before 2020 had higher rates of failure when presented with a phishing email — which leads to a higher risk to the city of falling victim to phishing attacks and malware.

**Not All City Employees Complete Cybersecurity Training**

We found not all city employees complete cybersecurity training. Among those who did not complete the training during the periods we looked at were employees who are not required to take the training. Our phishing experiment revealed such individuals were among those who fell victim to the simulated phishing attack. Additional details about these groups were provided confidentially to relevant city agencies.

According to the National Institute of Standards and Technology's standards on training, organizations should provide cybersecurity and privacy training to system users — including managers, senior executives, and contractors.17

---

For the City and County of Denver, the city’s Executive Order No. 18 gives Technology Services the authority to organize and direct information technology activities and information technology personnel operating on the city’s network, which includes email and cybersecurity.18

Lastly, according to payment card industry standards, training employees about phishing improves organizational security.19 The city collects payment card information for various services and fees, and in order for such an organization to comply with payment card industry standards, a formal security awareness program must be in place.

We learned Technology Services evolved its training platform since 2019 to incorporate trainings from Proofpoint, which expanded the amount of training content available. The city’s curriculum requires city employees to complete an annual cybersecurity awareness training as well as quarterly refresher trainings that cover various elements of information security — such as phishing, online behavior, and mobile devices.

However, Technology Services personnel told us they have struggled to define which specific employees should be required to complete cybersecurity training. They said employee information in the city’s system of record, Workday, does not offer enough detail about individuals’ job types to assist in their decision-making as to whether an employee should take the trainings.

We followed up with the Office of Human Resources, because that office is responsible for inputting data about city employees’ job types. Human Resources personnel told us that as of January 2021, they were working on a cleanup project to help identify specific groups of employee data and better define them. This included clearly defining contingent workers’ job types, on-call workers’ job types, and more. They said that once this information is updated, the data will help Technology Services identify the correct audiences for future cybersecurity awareness trainings.

Absent this more-detailed information, Human Resources and Technology Services are excluding significant portions of employees from certain job types from having to complete the cybersecurity training program. For example, among active employees who had logged into their email in 2020, 97% of one job type was not included in annual training nor quarterly training assigned in the third quarter of 2020.

Human Resources personnel acknowledged many of the trainings are targeted at full-time employees and exclude some other employee groups. While all employees are generally included in a cybersecurity training once a year, there is some movement in employee populations as people take

---

18 Executive Order No. 18, City and County of Denver (2005), accessed Feb. 7, 2021, https://www.denvergov.org/content/dam/denvergov/Portals/executiveorders/18-Establishment-of-Technology-Services.pdf. The order defines the “network” as hardware and software components and systems that support the digital services for users — including connectivity, email, storage, cybersecurity, and all other digital technology systems.

on new roles in the city. Smaller subsets of employees also move from a nontargeted group to full-time status and vice versa, which may cause them to not be targeted for a training.

Nonetheless, as our phishing simulation and analysis showed, employees who take cybersecurity training are less likely to engage with phishing emails and more likely to report phishing emails than those who did not take the training. As such, those who did not take the training expose the city to higher risk of data loss or risks of systems being breached. Other controls, such as multifactor authentication, can help reduce the risk of an employee submitting sensitive information through a phish, but malicious files such as ransomware can still be transmitted to victims of phishing attacks when they click a link or open an attachment in such emails.  

<table>
<thead>
<tr>
<th>1.1</th>
<th>RECOMMENDATION</th>
<th>Identify Employee Job Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AGENCY RESPONSE: AGREE, IMPLEMENTATION DATE – DEC. 31, 2021</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEE PAGE 17 FOR THE AGENCY’S FULL RESPONSE TO OUR RECOMMENDATIONS.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1.2</th>
<th>RECOMMENDATION</th>
<th>Offer Training to the Correct Sets of Employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AGENCY RESPONSE: AGREE, IMPLEMENTATION DATE – DEC. 31, 2022</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEE PAGE 17 FOR THE AGENCY’S FULL RESPONSE TO OUR RECOMMENDATIONS.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1.3</th>
<th>RECOMMENDATION</th>
<th>Reconcile Trainings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology Services should reconcile the list of individuals who should receive trainings with a list of those who actually complete it through Workday Learning.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AGENCY RESPONSE: AGREE, IMPLEMENTATION DATE – JUNE 30, 2021</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEE PAGE 17 FOR THE AGENCY’S FULL RESPONSE TO OUR RECOMMENDATIONS.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

20 The city uses multifactor authentication, which reduces the risk of unauthorized access. Multifactor authentication requires two independent ways to verify a user. For example, a system may ask for both a password and a code texted to the user’s phone.
1.4 RECOMMENDATION 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.

AGENCY RESPONSE: AGREE, IMPLEMENTATION DATE – DEC. 31, 2022
SEE PAGE 17 FOR THE AGENCY’S FULL RESPONSE TO OUR RECOMMENDATIONS.

1.5 RECOMMENDATION 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 this report.

AGENCY RESPONSE: AGREE, IMPLEMENTATION DATE – DEC. 31, 2022
SEE PAGE 17 FOR THE AGENCY’S FULL RESPONSE TO OUR RECOMMENDATIONS.
FINDING 2 AND RECOMMENDATIONS

Technology Services Should Track Phishing Metrics and Communicate Them to Other City Agencies

After we interviewed Technology Services personnel, they told us they communicate some phishing metrics to specific agencies but Technology Services was unable to provide evidence to verify this.

The National Institute of Standards and Technology says managing information system-related security and privacy risk is an undertaking that requires involvement from the entire organization. This includes involvement from:

- Senior leaders who provide a strategic vision and goals.
- Mid-level leaders who plan, execute, and manage projects.
- Individuals who develop, implement, operate, and maintain the systems supporting the organization’s mission and business functions.

As shown in Figure 4, the National Institute of Standards and Technology also says communication and reporting should flow both ways across three levels — the organization, the mission and business process, and the information system — to ensure risk is addressed throughout an organization.

![FIGURE 4. Organizationwide Risk Assessment Approach](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf)

---

The SANS Institute’s “Security Awareness Maturity Model” recommends having a robust metrics framework to track progress and measure impact with regard to a cybersecurity awareness program. The institute says the model can be used as a tool to communicate to leadership the goals and values of the program and organization.

SANS recommends identifying key stakeholders, tracking phishing metrics, and delivering metrics to different target audiences. SANS also has a matrix for cybersecurity awareness metrics that discusses what metrics should be tracked. This includes phishing metrics such as click rates, reporting rates, and rates for repeat offenders.

Additionally, Proofpoint — the main vendor Technology Services uses to prevent phishing attacks — says phishing metrics, such as reporting rates, should be communicated to stakeholders and employees so that the organization can be better protected.

As we discussed in Finding 1, the results of our phishing simulation found more training is associated with higher reporting rates. However, even those who took all trainings in the first three quarters of 2020 reported the phishing at a lower rate than recommended. Proofpoint recommends a target of 70% or greater for reporting rates in phishing.

And while Technology Services personnel told us they communicate phishing metrics to targeted city agencies, they were unable to provide evidence to support that claim. Furthermore, Technology Services personnel told us they are still trying to gather more information to develop metrics (e.g., information on whether the same individuals are falling victim to phishing emails) and they said metrics would confuse other agencies.

But by not communicating phishing metrics to other city stakeholders, other city agencies may be unaware of how their agency and their employees are performing with regard to phishing incidents. Other city agencies may be unable to monitor and track their performance to see whether they are at, above, or below expectations.

---


If managers do not receive phishing metrics, they cannot identify the needs of their units to prevent employees from falling for phishing attacks. The lack of tracking and communicating of phishing metrics could lead to phishing attacks being more successful among City and County of Denver employees.

<table>
<thead>
<tr>
<th>2.1</th>
<th>RECOMMENDATION</th>
<th>Develop Phishing Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AGENCY RESPONSE: AGREE, IMPLEMENTATION DATE – SEPT. 30, 2021</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SEE PAGE 17 FOR THE AGENCY’S FULL RESPONSE TO OUR RECOMMENDATIONS.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.2</th>
<th>RECOMMENDATION</th>
<th>Communicate Phishing Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AGENCY RESPONSE: AGREE, IMPLEMENTATION DATE – DEC. 31, 2021</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SEE PAGE 17 FOR THE AGENCY’S FULL RESPONSE TO OUR RECOMMENDATIONS.</td>
<td></td>
</tr>
</tbody>
</table>
AGENCY RESPONSE TO AUDIT RECOMMENDATIONS

April 7th, 2021

Auditor Timothy M. O’Brien, CPA
Office of the Auditor
City and County of Denver
201 West Colfax Avenue, Dept. 705
Denver, Colorado 80202

Dear Mr. O’Brien,

The Office of the Auditor has conducted a performance audit of Phishing Audit.

This memorandum provides a written response for each reportable condition noted in the Auditor’s Report final draft that was sent to us on March 16, 2021. This response complies with Section 20-276 (c) of the Denver Revised Municipal Code (D.R.M.C.).

AUDIT 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 1.1
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.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>12/31/2021</td>
<td>Christopher Longshore 720.547.5345</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.1
The Office of Human Resources agrees with this recommendation and is actively working a project to define worker sub types to target training. The project is scheduled to complete by 12/31/2021.
RECOMMENDATION 1.2
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.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>12/31/2022</td>
<td>Julie Sutton, Information Security Manager 720.913.4964</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Chris Longshore 720.547.5345</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.2
Agree. TS requires that all employees and individuals with access to CCD resources have cyber training. The training can be provided by either CCD or, in the case of a contingent worker, through their parent organization as agreed to through their contractual obligation. TS is working with OHR to more correctly identify workers in the Workday system so that the assignment of training is more clearly defined and trackable. This first step will be completed before 06/30/2021.

In addition, when the Role Based Access Control (RBAC) project has completed and the cyber training has transitioned to the Proofpoint training platform, more specialized training will be employed to both those that require additional training due to previous actions and those that have specialized permissions that require additional training (i.e. administrative permissions). Timeline for this is 12/31/2022.

The transition plan is contingent on an agreed upon timeline from OHR.
RECOMMENDATION 1.3
Technology Services should reconcile the list of individuals who should receive trainings with a list of those who actually complete it through Workday Learning.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>6/30/2021</td>
<td>Julie Sutton, Information Security Manager 720.913.4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.3
Agree. We complete a reconciliation at the conclusion of each quarter’s training. The reconciliation will continue to occur each quarter and will reflect the employee categorization in recommendation 1.2 when completed.

RECOMMENDATION 1.4
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.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>12/31/2022</td>
<td>Julie Sutton, Information Security Manager 720.913.4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.4
Agree. When the Role Based Access Control (RBAC) project has completed and the cyber training has transitioned to the Proofpoint training platform, more specialized training will be employed to both those that require additional training due to previous actions and those that have specialized permissions that require additional training (i.e. administrative permissions).
RECOMMENDATION 1.5
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 this report.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>12/31/2022</td>
<td>Julie Sutton, Information Security Manager 720.913.4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.5
Agree. TS will continue to conduct quarterly training to cover the evolving security threat landscape, including phishing as needed.

AUDIT FINDING 2
Technology Services Should Track Phishing Metrics and Communicate Them to Other City Agencies

RECOMMENDATION 2.1
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.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>9/30/2021</td>
<td>Julie Sutton, Information Security Manager 720.913.4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 2.1
Agree. TS will continue to gather information and develop metrics related to phishing. TS will make continuous improvements on the metrics with adaptation of RBAC and other training tools. TS will communicate the metrics with city agencies once the information becomes available.
RECOMMENDATION 2.2
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).

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>12/31/2021</td>
<td>Julie Sutton, Information Security Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>720.913.4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 2.2
Agree. TS will continue to gather information and develop metrics related to phishing. TS will make continuous improvements on the metrics with adaptation of RBAC and other training tools. TS will communicate the metrics with city agencies once the information becomes available.

Please contact Samantha Shih at 720-913-5485 with any questions.

Sincerely,

David Edinger
Chief Information Officer

cc: Valerie Walling, CPA, Deputy Auditor
Dawn Wiseman, CRMA, Audit Director
Katja E. V. Freeman, MA, MELP, Audit Director
Jared Miller, CISA, CFE, IT Audit Supervisor
David Edinger, Chief Information Officer
Christine Binnicker, Deputy Chief Information Officer
Paul Kresser, Chief Data Officer
Christopher Todd, Chief Technology Officer
Julie Sutton, Information Security Officer
Patricia Rowe, Human Resources Learning and Development Director
Christopher Longshore, Human Resources Technology and Innovation Director
**OBJECTIVE**

To assess:

1. How well the city identifies, prevents, detects, and responds to cybersecurity phishing incidents.
2. The effectiveness of the city's cybersecurity awareness training by conducting internal and external phishing campaigns.
3. 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.

**SCOPE**

We evaluated the city's cybersecurity awareness training program for the period of Jan. 1, 2018, through Dec. 31, 2020.

**METHODOLOGY**

We used a variety of methodologies to collect and assess information related to the audit objectives. The methodologies included but were not limited to:

- Interviewing and performing walk-throughs with managers of the city's Technology Services agency and Office of Human Resources.
- Researching leading practices in the information technology industry related to cybersecurity awareness training.
- Evaluating cybersecurity awareness trainings offered by the City and County of Denver.
- Conducting a random control trial with a citywide simulated phishing campaign, as detailed in Appendix A.
APPENDICES

Appendix A – Methodologies for a Random Control Trial of an Internal Phishing Simulation

Design

The audit team designed a type of experiment called a “random control trial” to assess the likelihood that city employees would click links or submit credentials from a phishing email and how likely they were to report a phishing email to Technology Services.

The population for the experiment included 13,147 active city employees across almost all agencies who had either a denvergov.org or denverda.org email — as these two domains are both protected by the same email security measures. From this population, we randomly sampled 6,590 individuals to maintain at least a 95% confidence in our results.

That population included VIP users: those who have elevated access to city systems. Therefore, we ensured the sample of employees included VIP and non-VIP users. We included 342 VIP users and 6,248 non-VIP users in our phishing simulation experiment.

We developed two fake phishing emails for the experiment: an easy-to-identify email, which served as the control of the experiment, and a hard-to-identify email, which served as the test. The ease of identification was based on the number and types of cues in the email and subsequent landing pages that indicated they were fake. Next, we randomly assigned half the participants to receive the control email and the other half to receive the test email.

Our process of randomly selecting the participants and which participants received the two emails improved the internal validity of our results by reducing potential unknown biases related to the respondents or the audit team, which may have otherwise influenced who opened the email, clicked the link in the email, or attempted to submit their credentials on the subsequent landing pages.

Before sending the emails, we considered ethical approaches to the experiment. For example, we weighed the emotional impact on recipients and crafted the emails and responses to ensure they did not fear for their jobs. Additionally, we notified participants of the nature of the experiment immediately after they engaged with the email to ensure they would not fear reprisal.

Deployment

We deployed the two simulated phishing emails simultaneously using a program called Lucy. To ensure the emails reached the intended recipients and that they were not blocked by the city’s cybersecurity protocols, the Auditor’s Office partnered with Technology Services to temporarily allow the emails to be delivered. The emails remained active in the participants’ email inboxes for a limited time.

27 The Auditor’s Office, the city’s Office of Emergency Management and Homeland Security, and the Clerk and Recorder’s Office were not included in the experiment.
Once users reported the emails through the “Report Phish” button, another security measure engaged and removed the emails from the entire system.

We measured four outcomes from the experiment:

1. When a participant clicked on the link in the phishing emails, or a link-based test failure.
2. When a participant submitted credentials through the fake login page after clicking on the link in the phishing emails, or a data entry-based test failure.\(^{28}\)
3. When the employee notified Technology Services they received a potential phishing email using the “Report Phish” option in Microsoft Outlook, or the reporting rate.
4. When no action was taken.

**Analysis**

We analyzed these results using logistic regression models — a statistical tool to isolate the effects of different variables on binary outcomes (e.g., whether the participant attempted to submit information). The models considered the employees’ tenure with the city, their agency, their job type, their management level, their VIP status, and the number of cybersecurity trainings they completed in 2018, 2019, and the first three quarters of 2020.\(^{29}\) This way, we could examine the isolated effect of training or job type on the different outcomes, while controlling for the other variables. To show the impacts of each variable on the different outcome measures, we used a secondary analysis called “marginal effects” based on the regression model’s results.

Finally, we evaluated the randomly selected participants’ training history to look for relationships between how many trainings they completed and their job type, agency, and management level. For this analysis, we used a negative binomial regression — which is appropriate for analyzing count data, such as the number of trainings an employee completed.

---

\(^{28}\) The team designed the landing pages to recognize only the attempt to submit credentials. No credentials were collected through the phishing simulation.

\(^{29}\) We used training records from 2018, 2019, and the first three quarters of 2020 to determine whether the effectiveness of cybersecurity training reduces over time. We did not examine the content or do other audit work related to the 2018 trainings for this specific experiment.
# Appendix B – Phishing Message Cues

## TABLE 1. Operationalized Phishing Message Cues

<table>
<thead>
<tr>
<th>Cue Type</th>
<th>Cue and Description</th>
<th>Question to Help Identify</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Error</strong></td>
<td><strong>Spelling and grammar errors</strong>: Errors in spelling or grammar, mismatched plurality — such as “a bacteria” — and other irregularities.</td>
<td>Does the message contain spelling or grammar errors, including mismatched plurality?</td>
</tr>
<tr>
<td></td>
<td><strong>Inconsistency</strong>: Inconsistent content within the email.</td>
<td>Are there inconsistencies contained in the email message?</td>
</tr>
<tr>
<td><strong>Technical indicator</strong></td>
<td><strong>Attachment type</strong>: The presence of file attachments, especially an executable file (which contains a program).</td>
<td>Is there a potentially dangerous attachment?</td>
</tr>
<tr>
<td></td>
<td><strong>Sender display name and email address</strong>: Spoofed display names, which hide the sender and reply-to email addresses.</td>
<td>Does a display name hide the real sender?</td>
</tr>
<tr>
<td></td>
<td><strong>URL hyperlinking</strong>: URL hyperlinking hides the true URL behind text; the text can also look like another link.</td>
<td>Is there text that hides the true URL in a hyperlink?</td>
</tr>
<tr>
<td></td>
<td><strong>Domain spoofing</strong>: The domain name used in the email address and links looks similar to a plausible one.</td>
<td>Is a domain name used in addresses or links plausibly similar to a legitimate entity’s domain?</td>
</tr>
<tr>
<td><strong>Visual presentation indicator</strong></td>
<td><strong>No/minimal branding and logos.</strong></td>
<td>Is appropriate branding missing?</td>
</tr>
<tr>
<td></td>
<td><strong>Logo imitation or outdated branding/logos</strong>: Logos do not seem authentic.</td>
<td>Do any branding elements appear to be an imitation or outdated?</td>
</tr>
<tr>
<td></td>
<td><strong>Unprofessional-looking design or formatting.</strong></td>
<td>Do the design and formatting violate any conventional professional practices?</td>
</tr>
<tr>
<td></td>
<td><strong>Security indicators and icons.</strong></td>
<td>Are any inappropriate security indicators or icons present?</td>
</tr>
</tbody>
</table>

*Note: Table 1 continues on the following page.*

*Source: National Institute of Standards and Technology.*
<table>
<thead>
<tr>
<th>Language and content</th>
<th>Cue Type</th>
<th>Cue and Description</th>
<th>Question to Help Identify</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Legal language, copyright information, and disclaimers:</td>
<td>Any legal-type language such as copyright information, disclaimers, or tax implications.</td>
<td>Does the message contain any legal-type language such as copyright information, disclaimers, or tax information?</td>
</tr>
<tr>
<td></td>
<td>Distracting detail.</td>
<td></td>
<td>Does the message contain any detailed aspects that are not central to the content?</td>
</tr>
<tr>
<td></td>
<td>Requests for sensitive information:</td>
<td>Requests for information, like a Social Security number or other identifying information.</td>
<td>Does the message contain a request for any sensitive information, including personally identifying information or credentials?</td>
</tr>
<tr>
<td></td>
<td>Sense of urgency:</td>
<td>Use of time pressure to try to get users to quickly comply with the request.</td>
<td>Does the message contain time pressure, including implied pressure?</td>
</tr>
<tr>
<td></td>
<td>Threatening language:</td>
<td>Use of threats such as legal ramifications.</td>
<td>Does the message contain a threat, including an implied threat?</td>
</tr>
<tr>
<td></td>
<td>Generic greeting:</td>
<td>A generic greeting and an overall lack of personalization in the email.</td>
<td>Does the message lack a greeting or lack personalization in the message?</td>
</tr>
<tr>
<td></td>
<td>Lack of sender details:</td>
<td>Email includes few details about the sender, such as contact information.</td>
<td>Does the message lack detail about the sender, such as their contact information?</td>
</tr>
<tr>
<td>Common tactic</td>
<td>Humanitarian appeals:</td>
<td>Appeals to help others in need.</td>
<td>Does the message make an appeal to help others?</td>
</tr>
<tr>
<td></td>
<td>“Too good to be true” offers:</td>
<td>Contest winnings or other unlikely monetary and/or material offerings.</td>
<td>Does the message offer anything that is too good to be true — such as having won a contest, lottery, free vacation, and so on?</td>
</tr>
<tr>
<td></td>
<td>You’re special:</td>
<td>A “just for you” offering, such as a Valentine’s Day e-card from a secret admirer.</td>
<td>Does the message offer anything just for you?</td>
</tr>
<tr>
<td></td>
<td>Limited time offer:</td>
<td>“This offer won’t last long...”</td>
<td>Does the message offer anything for a limited time?</td>
</tr>
<tr>
<td></td>
<td>Mimics a work or business process or a legitimate email:</td>
<td>Mimics any plausible work process such as a new voicemail, package delivery, order confirmation, notice of invoice, and so on.</td>
<td>Does the message appear to be a work or business-related process?</td>
</tr>
<tr>
<td></td>
<td>Poses as a friend, colleague, supervisor, or authority figure:</td>
<td>Purports to be from someone known.</td>
<td>Does the message appear to be from a friend, colleague, boss, or other authority?</td>
</tr>
</tbody>
</table>

**Note:** Table 1 began on the previous page.

**Source:** National Institute of Standards and Technology.
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 | Fax (720) 913-5253
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.