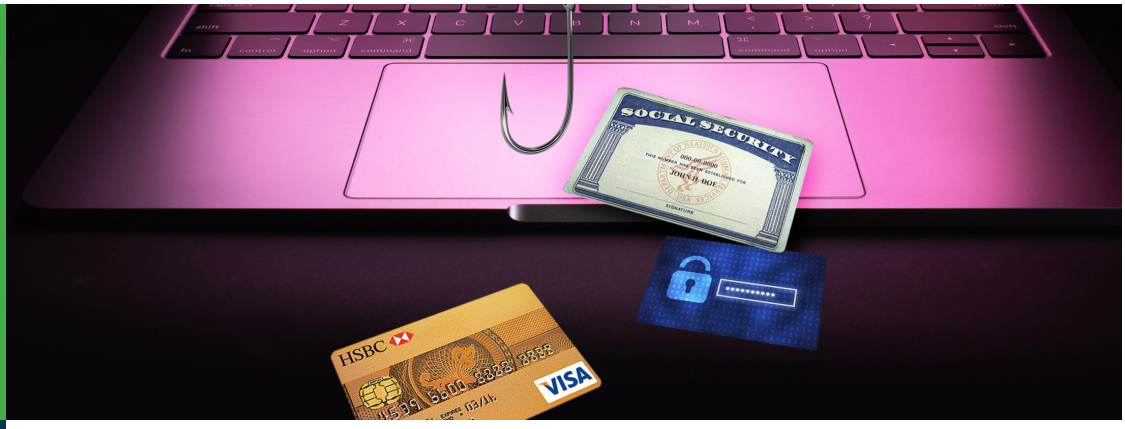
Audit at a glance



Phishing

APRIL 2021

ABOUT | "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.

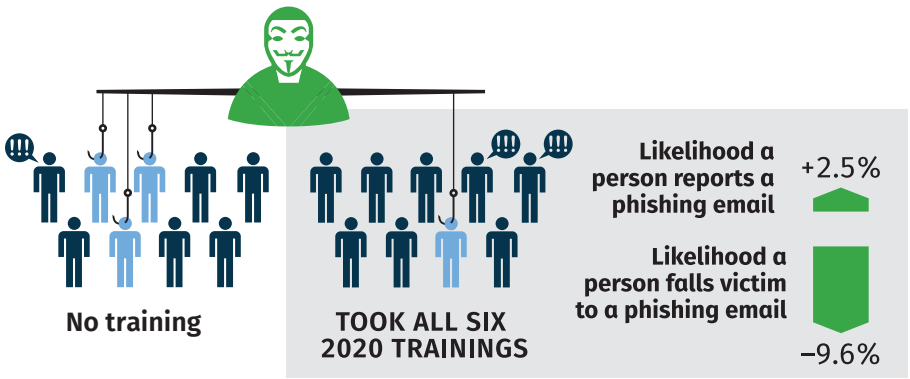
Phishes can occur via email, text message, or phone call. They can be sent to broad audiences or targeted to specific people because of their high-level status in an organization.

In the report

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

- 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.
- We conducted a citywide experiment to test both the city's organizational security and city employees' behavior when faced with a simulated phishing email sent by a malicious actor seeking to send malware or gather sensitive information.
- We found city employees are not meeting recommended standards for responding to and reporting phishing emails. But we also found a positive but limited impact of the city's cybersecurity training on the employees who engaged with our simulated phishing emails. For instance, city employees who took all required cybersecurity trainings in the first three quarters of 2020 were 9.6 percentage points less likely to submit sensitive information through our phish.

Change in Employee Behavior after Completing Cybersecurity Training



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

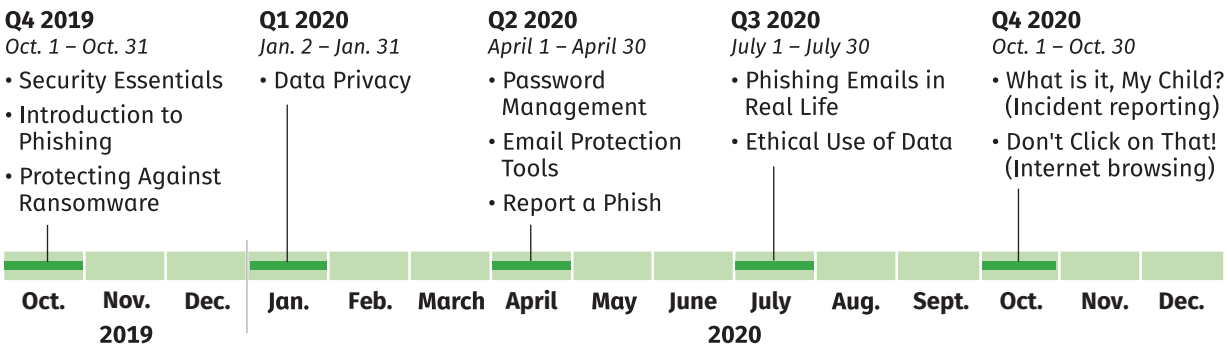
TURN OVER FOR MORE →

Timothy M. O'Brien, CPA | Denver Auditor

For a copy of this report, visit **www.denverauditor.org** or call the Auditor's Office at **(720) 913-5000**.

← CONTINUED FROM OTHER SIDE

Training timeline



Source: *Graphic designed by the Auditor's Office staff using information from Technology Services.*

- We also assessed the content of the city's cybersecurity training program. We concluded the trainings do not fully prepare employees to respond to phishing emails or ensure employees fully understand the material. Older trainings had less effect on behavior, which highlights the importance of frequent trainings.
- Some employees who are not required to take the city's cybersecurity trainings are among those who engaged with our simulated phishing emails. Employees who did not take the training expose the city to higher risk of data loss or of systems being breached.
- We recommended the city more accurately identify the employee job types that should receive cybersecurity awareness training and that the city evaluate the training content to ensure the training is regularly provided and effective in improving employees' behavior and knowledge.

Results of Internal Phishing Simulation compared to Suggested Rates and Industry Averages

	Link-based failure rate	Data entry-based failure rate	Reporting rate
Proofpoint suggested rate	*5%*	*5%*	*70%*
Government average rate	*14%*	*4%*	*15%*
Control email *(3,295 participants)*	*2.5% (81)*	*0.03% (1)*	*7.1% (235)*
Test email *(3,295 participants)*	*10.4% (344)*	*7.2% (238)*	*2% (65)*

Source: *Auditor's Office analysis of phishing simulation results.*

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

- 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 training program. However, Technology Services does not formally let other city agencies know about various metrics related to phishing attempts, such as how frequently employees report a phish to Technology Services.
- Technology Services personnel told us they do not communicate phishing metrics to other city agencies, in part, because they are still trying to gather more information to develop the metrics (e.g., information on whether the same individuals are falling victim to phishing emails).
- By not communicating phishing metrics to other city stakeholders, city agencies may be unaware of how their agency and their employees are performing when phishing incidents occur. Agencies also may be unable to monitor and track their performance to see whether they are at, above, or below expectations.
- We recommended Technology Services develop specific phishing metrics and communicate them with other city agencies.