March 2015

PERFORMANCE AUDIT
Employees' Response to Phishing Email Put City Information Systems at Risk

Office of the City Auditor
Kansas City, Missouri

Highlights

Why We Did This Audit

In 2013, it was reported that one in 392 emails contained phishing attacks. The damage caused by phishing ranges from computers infected with malware to significant data breaches, and in turn, results in substantial financial loss. Business suffered phishing related losses in the billions.

Data breaches caused by phishing scams can damage city systems, cost the city money, and shake the public's trust and confidence in city government.

Background

Phishing is a social engineering technique used to deceive users and attempt to acquire sensitive information such as usernames, passwords, or credit card information by posing as a trustworthy organization. Phishing is typically carried out by email and often directs users to enter details at a fake website.

Audit Methodology

As part of our audit, we sent phishing emails to all city employees with city email addresses. We embedded a link to a fake website in our phishing email enticing employees to click on the link to the website and provide their network login information.

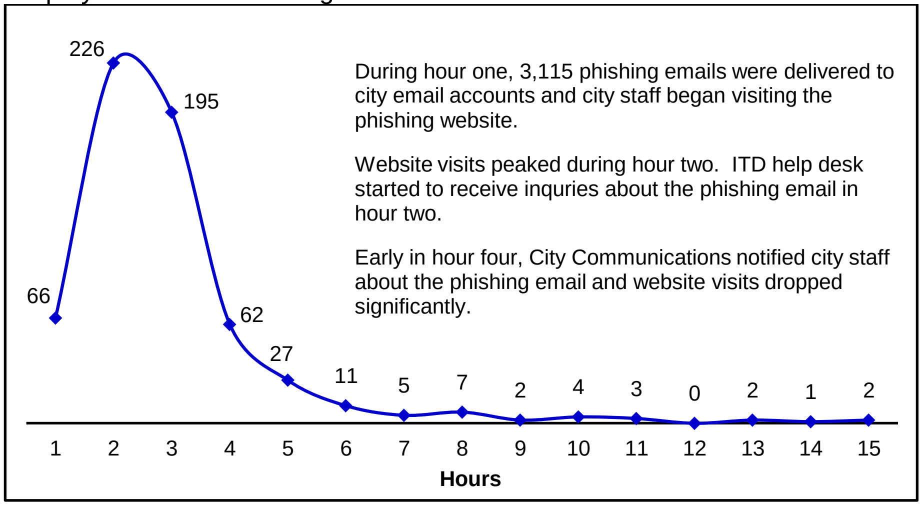
For more information, contact the City Auditor's Office at 816-513-3300 or auditor@kcmo.org.

To view the complete report, go to http://kcmo.gov/cityauditor and click on Search Audit Reports

What We Found

During our phishing email test, employees visited our fake website over 600 times within the first 24 hours after the emails were sent. About 280 employees provided valid login credentials that could be used to hack the city's systems. In addition, 28 employees had not changed their passwords two months after being told to do so. Had this been a real phishing email, hackers could have used the information employees provided to harm the integrity, confidentiality, and availability of the city's information systems. Information technology security is as much a human issue as it is a technology issue. Employees need to be aware of cyber security and learn to recognize and protect the city from phishing and other social engineering attacks.

Employee Visits to Phishing Website



During hour one, 3,115 phishing emails were delivered to city email accounts and city staff began visiting the phishing website.

Website visits peaked during hour two. ITD help desk started to receive inquries about the phishing email in hour two.

Early in hour four, City Communications notified city staff about the phishing email and website visits dropped significantly.

Information Technology Division (ITD) staff took appropriate steps to respond to our phishing email by alerting staff the email was fraudulent, deleting the email, and advising employees to change their passwords. Although ITD has practices in place to respond to phishing emails, ITD does not have a comprehensive cyber security incident response plan to ensure staff responds to attacks quickly, consistently, and effectively.

What We Recommend

Our recommendations are directed towards ensuring that:

- Employees respond to phishing emails and other social engineering attacks appropriately, and
- Cyber incidents are promptly identified, exploited weaknesses are mitigated, loss and destruction are minimized, and IT services are restored.

Management agreed with the recommendations.