



STAY AWARE CYBERSAFE



The DCP Cybersecurity Awareness Assessment



CITY OF *Los Angeles*
DEFERRED COMPENSATION PLAN

VOYA
FINANCIAL

2025 NAGDCA Leadership Award Submission: Technology & Cybersecurity

PLAN PROFILE

The City of Los Angeles Deferred Compensation Plan (DCP) is one of the largest public sector 457(b) retirement plans in the country, serving over 53,000 participants with nearly \$11 billion in assets. Through its various communications campaigns the DCP leverages its extensive reach and influence to promote financial security and retirement readiness. With a commitment to innovation, the DCP continually seeks new ways to engage its diverse workforce, which includes members of the Los Angeles City Employees' Retirement System (LACERS), Los Angeles Fire and Police Pensions (LAFPP), and the Water & Power Employees' Retirement Plan (WPERP). This breadth of representation makes valuable and strategic communications campaigns vital to promoting retirement savings and productive financial behaviors which is reflected in the DCP's growing participation rate of 73% and average participant deferral rate of 9%.

BACKGROUND AND OBJECTIVES

As technology becomes increasingly more prevalent in everyday life, cybersecurity has emerged as one of the most urgent challenges facing retirement savers. But one group is especially vulnerable: retirees. Retirees are often targeted by cybercriminals because they may not have access to employer-provided cybersecurity training or tools and often have significant assets accumulated in retirement plans, making them high-value targets.

According to the FBI, individuals aged 60 and older reported over \$3.4 billion in losses due to cybercrime in 2023, an 11% increase over the previous year.¹ An AARP survey also found that 42% of Americans age 50+ have had money stolen due to a scam using sensitive information obtained fraudulently.² These alarming findings signal a clear and urgent need for targeted cybersecurity education for retirees. In response, the City of Los Angeles Deferred Compensation Plan launched an innovative new communications campaign and interactive assessment designed specifically to engage its retired participants on the topic of cybersecurity. The goals of the campaign were to:

- Proactively educate retirees on how to protect their retirement accounts and personal information;
- Assess participants' understanding of digital best practices through a short, interactive survey;
- Highlight specific knowledge gaps and identify topics needing further attention;
- Promote ongoing education through follow-up articles, blog content, and statement messages;
- Begin building a cybersecurity-first mindset among DCP participants.



IN THEIR OWN WORDS

"This campaign addressed a real and growing concern for our retiree population. By combining education with a simple and engaging assessment, we empowered participants to better protect themselves online and feel more confident about the security of their retirement accounts."

- Esther Chang | Plan Manager, City of Los Angeles Deferred Compensation



The DCP Cybersecurity Awareness Assessment

PROJECT SUMMARY

Built on SurveyMonkey, the **DCP Cybersecurity Assessment** was comprised of seven yes/no questions directly based on the U.S. Department of Labor's *Online Security Tips for Retirement Plan Participants*³. These questions were carefully selected to reflect the most critical behaviors participants should adopt to protect their accounts and identities, including:

- Creating strong, unique passwords;
- Recognizing phishing attempts;
- Installing anti-virus software; and
- Understanding how and where to report a suspected breach.

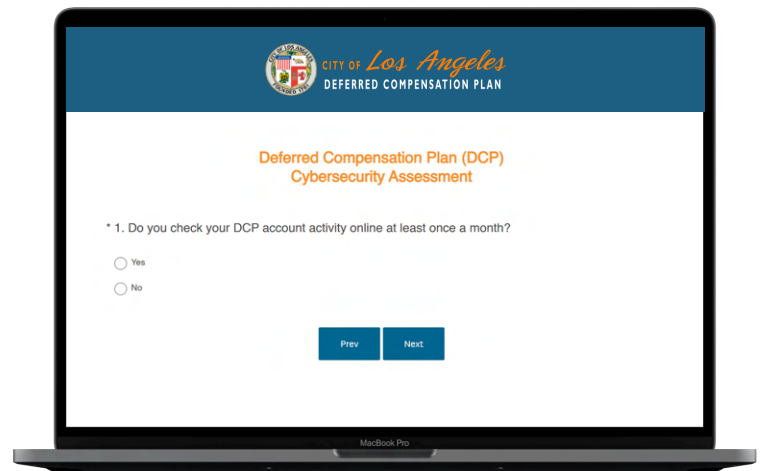
To increase engagement and make learning fun, we gamified the experience with a “Cybersecurity Badge” system based on the participant’s quiz score:

- Cybersecurity Star (100%)
- Cybersecurity Defender (70–90%)
- Cybersecurity Builder (42–69%)
- Cybersecurity Learner (14–41%)
- Cybersecurity Starter (under 14%)

After completing the survey, users immediately received the “badge” they earned and received correct answers with brief, plain-language explanations drawn from DOL guidance. Participants were also invited to visit a new companion blog post on the **LA457.com/cybersecurity** that offered a deeper dive into the same security topics.

This campaign was designed with simplicity and approachability in mind. Retirees may not regularly engage with digital learning tools, so we ensured the tone was empowering, not intimidating. The language was jargon-free, the experience was mobile-friendly, and the branding mirrored other trusted DCP communications, building participant confidence and trust.

The campaign was promoted through a multichannel outreach strategy, including **5,611 emails** to retired participants, **3,438 postcards** mailed to retirees who prefer physical mail, promotion in the quarterly newsletter, and messages in account statements. Messaging emphasized the short time commitment (just two minutes), the opportunity to test one’s knowledge, and the value of knowing how “cyber-safe” their online account practices are.



Online DCP Cybersecurity Assessment



“Badges” earned based on assessment score



Email and postcards

ENGAGEMENT & RESULTS

A total of 231 retirees completed the survey. While the 4% engagement rate may be a relatively strong return for this demographic given the request to complete an elective assessment on a specialized subject matter (cybersecurity), we also recognize opportunities for improvement that have been outlined in the conclusion of this document. Regardless, the campaign provided key data points that will influence and shape future communications on this topic.

Key Findings


- The average quiz score was 65%, earning most participants the Cybersecurity Builder badge, showing a moderate level of understanding but clear room for growth.
- The most frequently missed question (answered correctly by only 28%) was related to how to report a cybersecurity incident on their DCP account, highlighting a crucial knowledge gap.
- The highest-scoring question asked whether participants avoid sharing sensitive data like Social Security numbers or account details over email (answered this correctly by 97%) demonstrating strong baseline awareness of this core principle.

ONGOING IMPACT

This data gave us valuable insight into the cybersecurity literacy of our retiree population and helped us fine-tune future communication efforts. More importantly, it revealed that retirees were willing to engage with interactive digital content when it was accessible, helpful, and clearly tied to protecting their savings.

As a direct result of the campaign:

- We introduced a new recurring “Cybersecurity Corner” article in the quarterly DCP newsletter, covering topics like multifactor authentication, mobile security, and phishing scams.
- We embedded targeted cybersecurity messages into quarterly participant statements to increase visibility.
- We built cybersecurity education into our 2025 strategy and are expanding the assessment to all Plan participants (not just retirees) because we recognize that cybersecurity is a shared responsibility that benefits everyone. To that end, our 2025 communications strategy includes two distinct campaigns (in May and September) that will introduce additional cybersecurity education and insights.



Support for DCP participants affected by the recent wildfires and fires

As our community faces the ongoing impact of the recent wildfires and fires, we want to extend our support to our City of Los Angeles colleagues and Deferred Compensation Plan (DCP) participants. Your safety and well-being are our top priority.

If you've been affected by the fires and need financial relief, the DCP offers several options to help you access your funds.

FOR ACTIVE EMPLOYEES

- **Leave** - Receive from your DCP account, including a new Qualified Disaster Loan up to \$100,000, subject to requirements. Requests are made via payroll deduction (you may also request a delay in beginning payments for up to one year).
- **Emergency Withdrawals** - Request funds for immediate needs.
 - **Qualified Disaster Distribution** - Up to \$22,000 per disaster.
 - **Emergency Expense Withdrawal** - Up to \$2,000 per year subject to requirements.
 - **In-Service Withdrawal** - Available if you are over age 59½.
 - **Unfathomable Emergency Withdrawal** - Based on demonstrated financial hardship.

Log into your account at [LA457.com](#) or call 844-523-2457 to initiate your request.

FOR RETIRED OR TERMINATED EMPLOYEES

- **Withdrawals** - Choose from expense distribution, lump sum distribution, or lump sum withdrawal from your DCP account.
- **Leave** - Available, including the new Qualified Disaster Loan up to \$100,000, subject to requirements. Requests are made monthly from your bank account.

Call the Service Center at 844-523-2457 to initiate your request.

Cybersecurity Corner

Could you spot a "phishing attack"? Phishing attacks are emails designed to trick you into revealing passwords, account numbers, and other sensitive information. These scams often appear as emails or texts from trusted organizations, urging you to click on dangerous links or share personal details. Watch out for these warning signs:

- Unexpected messages from unknown contacts or services you don't use.
- Spelling errors or poor grammar.
- Mismatched or odd links - hover over them (without clicking) to check the actual destination.
- Requests for personal information. Remember, legitimate organizations will never ask for passwords or account details via email or text.
- Urgent, too-good-to-be-true, or fear-based messages.
- Strange sender addresses that don't match the organization.

If something feels suspicious, trust your instincts - don't click or share! If you suspect you have been targeted with a phishing email or text message claiming to be from the Deferred Compensation Plan or Voya Financial, report it right away by calling 844-523-2457 or emailing LA457@cityofla.org.

April 2025 Newsletter "Cybersecurity Corner"

Cybersecurity Corner

Could you spot a "phishing attack"? Phishing attacks are emails designed to trick you into revealing passwords, account numbers, and other sensitive information. These scams often appear as emails or texts from trusted organizations, urging you to click on dangerous links or share personal details. Watch out for these warning signs:

- Unexpected messages from unknown contacts or services you don't use.
- Spelling errors or poor grammar.
- Mismatched or odd links - hover over them (without clicking) to check the actual destination.
- Requests for personal information. Remember, legitimate organizations will never ask for passwords or account details via email or text.
- Urgent, too-good-to-be-true, or fear-based messages.
- Strange sender addresses that don't match the organization.

If something feels suspicious, trust your instincts - don't click or share! If you suspect you have been targeted with a phishing email or text message claiming to be from the Deferred Compensation Plan or Voya Financial, report it right away by calling 844-523-2457 or emailing LA457@cityofla.org.



The DCP Cybersecurity Awareness Assessment

CONCLUSION & FEASIBILITY

The DCP's Cybersecurity Assessment campaign was a timely, relevant, and creative response to one of the fastest-growing threats to retirement security. By targeting a high-risk yet often underserved retiree segment we delivered a solution that was as educational as it was empowering. This campaign proves that cybersecurity education doesn't have to be complicated, lengthy, or fear-based to be effective. With thoughtful design, a bit of gamification, and a message of empowerment, retirement plans can foster real behavior change. While recognizing the successes of the campaign, we also reflected on what we learned and what we can do to improve engagement on future initiatives of a similar initiatives. A few of those include:

- Rather than a single assessment, develop micro-assessments delivered over a series of months that help train participants to expect cybersecurity educational content on a regular basis.
- Put the potential awards and badges-earned in the more prominent position in our campaign communications.
- Rethink the question structure by integrating more real-world scenarios that participants may find relatable.
- Explore partnerships with the City of Los Angeles IT department or related division to help drive promotion through alternative channels.

While there is plenty of room for improvement, we would assert that the existing campaign approach is effective and easily adaptable for other public sector retirement plans. The entire survey was built using SurveyMonkey - an affordable, user-friendly tool accessible to any organization. The questions were based on freely available DOL guidance, making content development simple and authoritative. The badge system added a layer of engagement that motivated participation without requiring sophisticated gamification technology.

Most importantly, the campaign demonstrated that cybersecurity education can be effective even among audiences who may be less digitally fluent, as long as the delivery is empathetic and approachable. We hope this initiative can inspire and serve as a model for other public sector plans committed to protecting the digital safety of their participants.

SOURCES

1. FBI Internet Crime Complaint Center. 2023 Elder Fraud Report. https://www.ic3.gov/annualreport/reports/2023_ic3elderfraudreport.pdf
2. AARP 2024: The Fraud Crisis in America: How Adult Consumers Feel, What They Know, And Their Actions That Pose Risk. <https://www.aarp.org/content/dam/aarp/research/topics/work-finances-retirement/fraud-consumer-protection/fraud-awareness-americans.doi.10.26419-2fres.00788.001.pdf>
3. US Department of Labor. Online Security Tips. <https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf>