

# 2023 NASPEs AWARD

## *Eva N. Santos Communication Awards*

Nominations from dues-paying states are considered for eligibility. Nominated leaders and programs should have a positive effect on the administration of state human resource programs. A state's central human resource department or line agency human resource operations may administer nominated programs.

Programs and projects must have been operational for at least six months and must be transferable to other states. Selection criteria are based on the questions asked on the award application. Included in this packet are the specific criteria for each award and their categories. Nominations are encouraged in all areas of human resource management administration.

---

### **NOMINATION INFORMATION**

Title of Nomination: State Civil Service Cybersecurity Course

State: LA

Contact Person: Lindsay Ruiz de Chavez

Contact's Title: Public Information Director

Agency: Louisiana State Civil Service

Mailing Address: P.O. Box 94111, Baton Rouge, LA 70804-9111

Telephone: 225.342.8274

E-mail: Lindsay.ruiz@la.gov

---

### **NOMINATOR INFORMATION**

Nominator: Byron P. Decoteau, Jr. Title: Director

State: LA

Agency: Louisiana State Civil Service

Telephone: 225.342.8274

E-mail: Byron.Decoteau@la.gov

---

#### **ALL SUBMISSIONS MUST:**

- Meet all eligibility requirements
- Meet deadline requirements
- Include a complete nomination packet
- Conform to all copyright laws

# 2023 NASPEs AWARD

## *Eva N. Santos Communication Awards*

### DETAILS

Feel free to include links to websites and snapshots as part of your nomination.

1. Please provide a brief description of the submission.

The submission is an e-Learning course covering the topic of cybersecurity. The course is set up as a first-person game in which the learner encounters a variety of situations that are commonly used by hackers to gain access to systems. The learner must not only navigate these situations appropriately but also identify the suspicious elements that they should be on the lookout for in real-world situations. Throughout the course, learners are also given background information on the different methods used by hackers.

2. How long has the submission been in existence?

The course was released in August of 2020.

3. Why was this submission created?

The course was created to support Act 155 which was passed by the Louisiana State Legislature in 2020. The legislation required all state and local agencies to identify employees or elected officials who have access to the agency's IT assets. These individuals are required to complete the cybersecurity training. To ensure compliance with Act 155, state agency heads are required to annually verify that Cybersecurity Awareness training has been done and report to State Civil Service on the completion of the training by employees and contractors. Course completion reports are due to the State Civil Service Director by March 31st of each year for the previous year.

4. How does this submission support the goals and objectives of your agenda/department?

In recent years there have been multiple instances of hackers, both foreign and domestic, gaining access to the networks of organizations in both private and public sectors. Once they gain access, these hackers hold the networks for ransom and as a result the organizations are unable to operate and meet the needs of their customers and risk losing critical information should they not pay the ransom. This is specifically dangerous for those governmental entities. Government at every level exists to provide essential services to its citizens. Were a hacker to gain access to these systems, the ability of the governmental entity to provide these services would be compromised. This literally could result in a life-or-death situation in some instances. This course ensures that agency employees as well as all government employees statewide, are informed about the dangers that hackers pose and the techniques hackers use to gain access to networks. Learners not only learn about these techniques; they are able to practice identifying suspicious emails and other threats and effectively handling them once they are identified. By dispersing this information, this training assists in keeping state and local networks safe.

#### **ALL SUBMISSIONS MUST:**

- Meet all eligibility requirements • Meet deadline requirements
- Include a complete nomination packet • Conform to all copyright laws

# 2023 NASPEs AWARD

## *Eva N. Santos Communication Awards*

5. Have you been able to measure the effectiveness of this submission? If so, how?

The effectiveness of this course is best measured by the number of learners that it has reached. The course is made available to all state employees through our Learning Management System. This course has been taken by 57,620 state employees since its release. This number is most likely an underrepresentation though, as there are instances when multiple employees have taken the training in a workshop-style set-up. In addition to state employees, the Louisiana Legislature has mandated that the course be made available to all governmental entities throughout the state. In 2022 alone, the course has been distributed to 233 different government organizations within Louisiana to train 82,620 people. Incredibly, since its inception, the course has reached almost 240,000 people.

In addition to the numbers of learners who have been impacted by this training, we also collect feedback from our learners after they have completed the course. This feedback, which is obtained through Survey Monkey, has been overwhelmingly positive. Many have stated how they have enjoyed how interactive the course is and that they enjoy the game-like feel it has to it. Others have gone as far as to say that it is the best e-learning course they have ever taken.

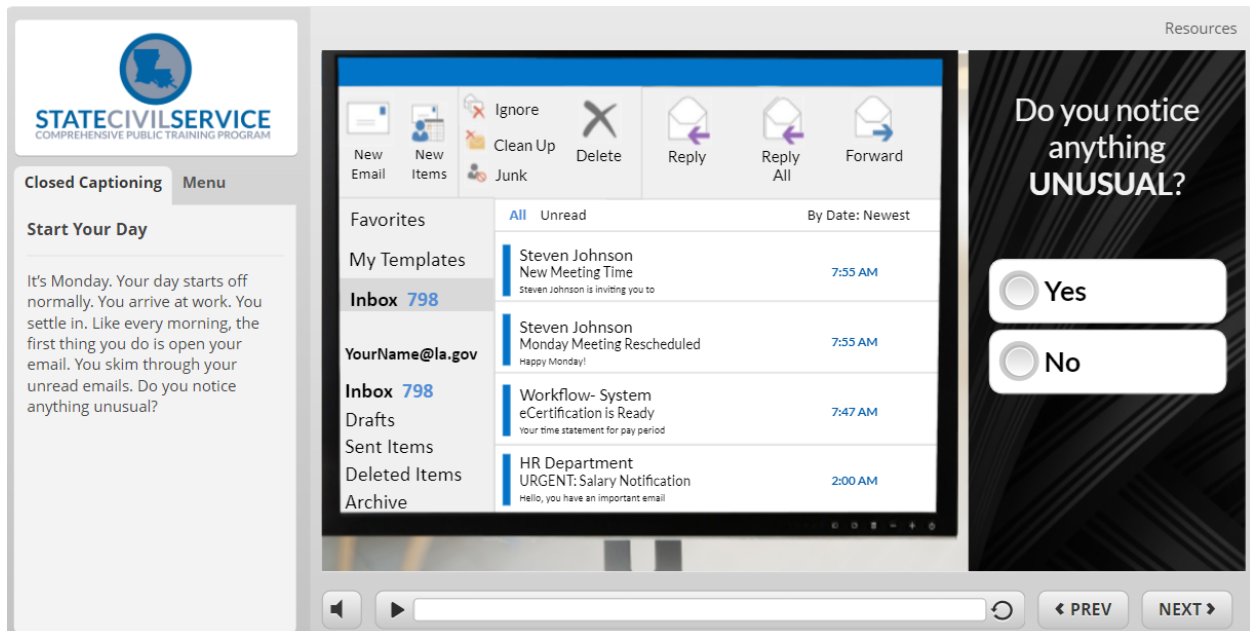
A few screenshots and promotional videos can be found below:

### Course Promos:

<https://youtu.be/t3CPC15ihBA>

<https://youtu.be/WG0CijJufGk>

### Screenshots:



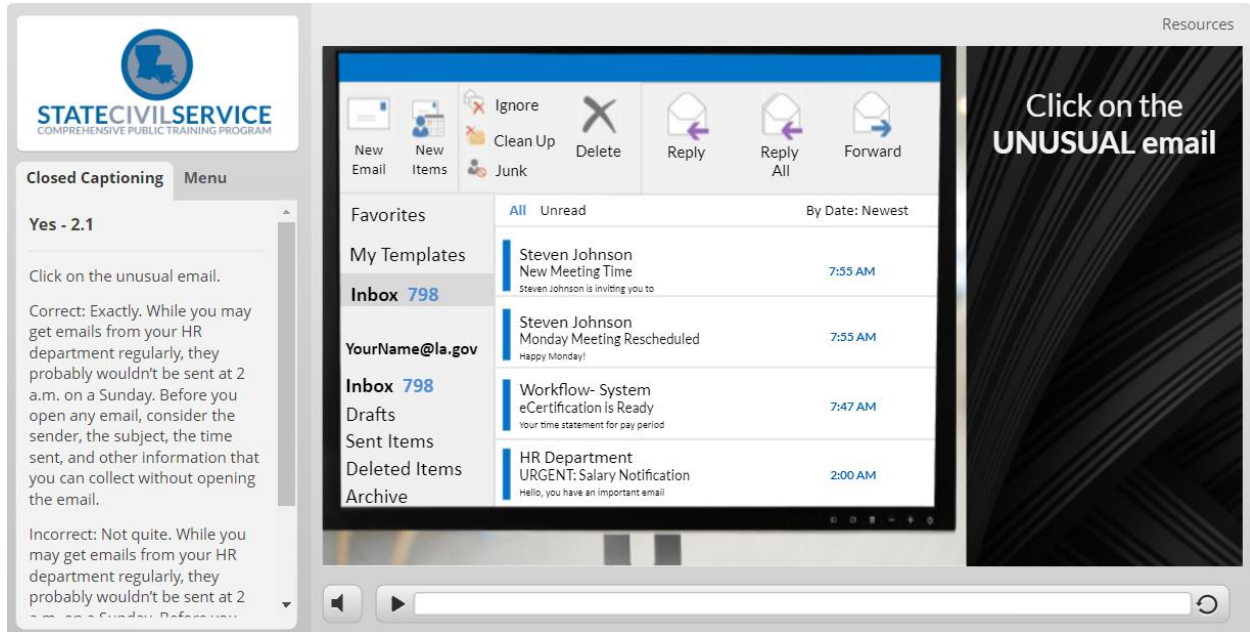
### ALL SUBMISSIONS MUST:

- Meet all eligibility requirements
- Meet deadline requirements
- Include a complete nomination packet
- Conform to all copyright laws

# 2023 NASPEs AWARD

## Eva N. Santos Communication Awards

Resources



The screenshot shows an email client interface. On the left, there is a sidebar with the State Civil Service logo and a 'Closed Captioning' menu. The main area displays an email inbox with several messages. A video player is overlaid on the right side of the inbox, showing a dark background with the text 'Click on the UNUSUAL email'.

**STATE CIVIL SERVICE**  
COMPREHENSIVE PUBLIC TRAINING PROGRAM

**Closed Captioning** Menu

**Yes - 2.1**

Click on the unusual email.

Correct: Exactly. While you may get emails from your HR department regularly, they probably wouldn't be sent at 2 a.m. on a Sunday. Before you open any email, consider the sender, the subject, the time sent, and other information that you can collect without opening the email.

Incorrect: Not quite. While you may get emails from your HR department regularly, they probably wouldn't be sent at 2 a.m. on a Sunday. Before you open any email, consider the sender, the subject, the time sent, and other information that you can collect without opening the email.

**Click on the UNUSUAL email**

**Ignore** **Delete** **Reply** **Reply All** **Forward**

**New Email** **New Items** **Clean Up** **Junk**

**Favorites** **All** **Unread** **By Date: Newest**

**My Templates**

**Inbox 798**

**YourName@la.gov**

**Inbox 798**

**Drafts**

**Sent Items**

**Deleted Items**

**Archive**

Steven Johnson  
New Meeting Time  
Steven Johnson is inviting you to

7:55 AM

Steven Johnson  
Monday Meeting Rescheduled  
Happy Monday!

7:55 AM

Workflow-System  
eCertification is Ready  
Your time statement for pay period

7:47 AM

HR Department  
URGENT: Salary Notification  
Hello, you have an important email

2:00 AM

Resources



The screenshot shows a video player interface. On the left, there is a sidebar with the State Civil Service logo and a 'Closed Captioning' menu. The main area displays a video player with a dark background and a hooded figure. The text 'Phishing' is prominently displayed at the top, followed by 'Tries to trick you into giving information:' and a list of items: Passwords, Social Security numbers, and Banking information.

**STATE CIVIL SERVICE**  
COMPREHENSIVE PUBLIC TRAINING PROGRAM

**Closed Captioning** Menu

**Phishing Defined**

Phishing is simple. I use email to trick you into giving me information or access to your system. There's different types of phishing - spear fishing, where I target you or someone specific and pretend to be from a specific organization, like your work or your bank. There's vishing where I call you on an internet telephone service. There's smishing - that's where I text you. There's even pharming - that's phishing + farming - that's where I redirect web traffic to a fake site.

**Phishing**

**Tries to trick you into giving information:**

- Passwords
- Social Security numbers
- Banking information

**PREV** **NEXT**

### ALL SUBMISSIONS MUST:

- Meet all eligibility requirements
- Meet deadline requirements
- Include a complete nomination packet
- Conform to all copyright laws

# 2023 NASPEs AWARD

## *Eva N. Santos Communication Awards*

Resources

**Look at the email more closely**

**Click on everything that indicates this email is fake**

**Click SUBMIT**

**Review the Email**

Look at the email more closely. Click on everything that indicates this email is fake. When you are finished, click submit.

◀ ▶ 🔍 ↻ ◀ PREV SUBMIT

### ALL SUBMISSIONS MUST:

- Meet all eligibility requirements • Meet deadline requirements
- Include a complete nomination packet • Conform to all copyright laws