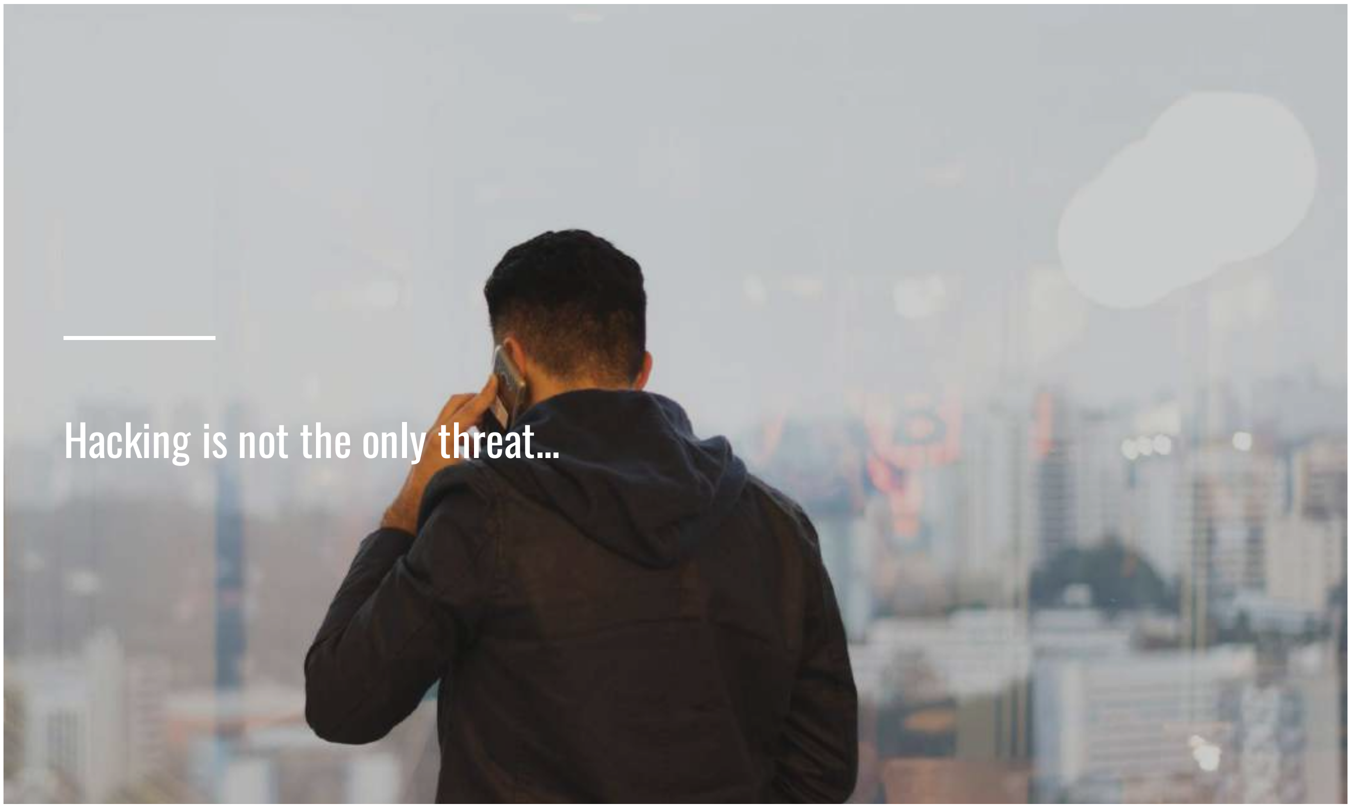
dermot o reilly

Social Engineering

Section 1 of 1

Social Engineering


Hacking is not the only threat...

When you hear the word “Hacker”, you probably think of computer whiz kids who hack into corporate databases to steal confidential information. However, most people don't realize that the most common form of hacking is Social Engineering. Consider this scenario:

You are working as a receptionist at a tech company in Dublin. One day a courier arrives and informs you that he is here to collect your manager's laptop for repair. How should you respond?

○ Present the courier with the laptop, but check his ID first

○ Don't hand over the laptop until you receive confirmation from your manager

SUBMIT

Complete the content above before moving on.

Social engineers are experts in the human condition

What is Social Engineering?

Social Engineering attacks attempt to persuade you to reveal information about yourself, your company, clients, etc. by appearing as legitimate sources of information or authority. They may also introduce computer viruses to your network or steal corporate information, commit fraud, or cause other damage.

How Does Social Engineering Work?

“Social Engineers” use well-honed people skills to extract information from unsuspecting users. For example, a member of the accounts team might receive a call from a "manager" requesting payment of an invoice, or a staff member might receive a request to provide sensitive information to someone claiming to be from the accounts department.

CONTINUE

The tools of the social engineer include telephone, email, and personal charm

Social Engineering by Telephone

Social engineers commonly use the telephone as an attack method, the reason being that it allows them to remain anonymous. They often target help-desk staff, given that they are trained to be helpful and friendly and more likely to provide the information that the fraudster is looking for. The fraudster will often claim to be a senior staff member and may request seemingly innocuous information such as the contact details for a manager or other key staff member. Often the fraudster might be more blatant and request sensitive information from an unsuspecting employee such as a username or password.

Here are some common characteristics of social engineering by telephone:

- Claiming a position of authority
- Creating a sense of urgency
- Impersonating someone else
- Requesting sensitive information

Social Engineering In Person

"In-person" social engineering is all about using social skills to engage people to obtain information.

- Social engineers use extremely well-honed people skills to extract information from targets.
- They engage people in social situations, including at bars or restaurants
- They may develop a relationship with the target over weeks or months.
- Once a trusting relationship has been developed, the social engineer will exploit that relationship to obtain work-related information from the target.

CONTINUE

Combat Social Engineering

□ Be wary of unsolicited phone calls, text messages, instant messages, or emails.

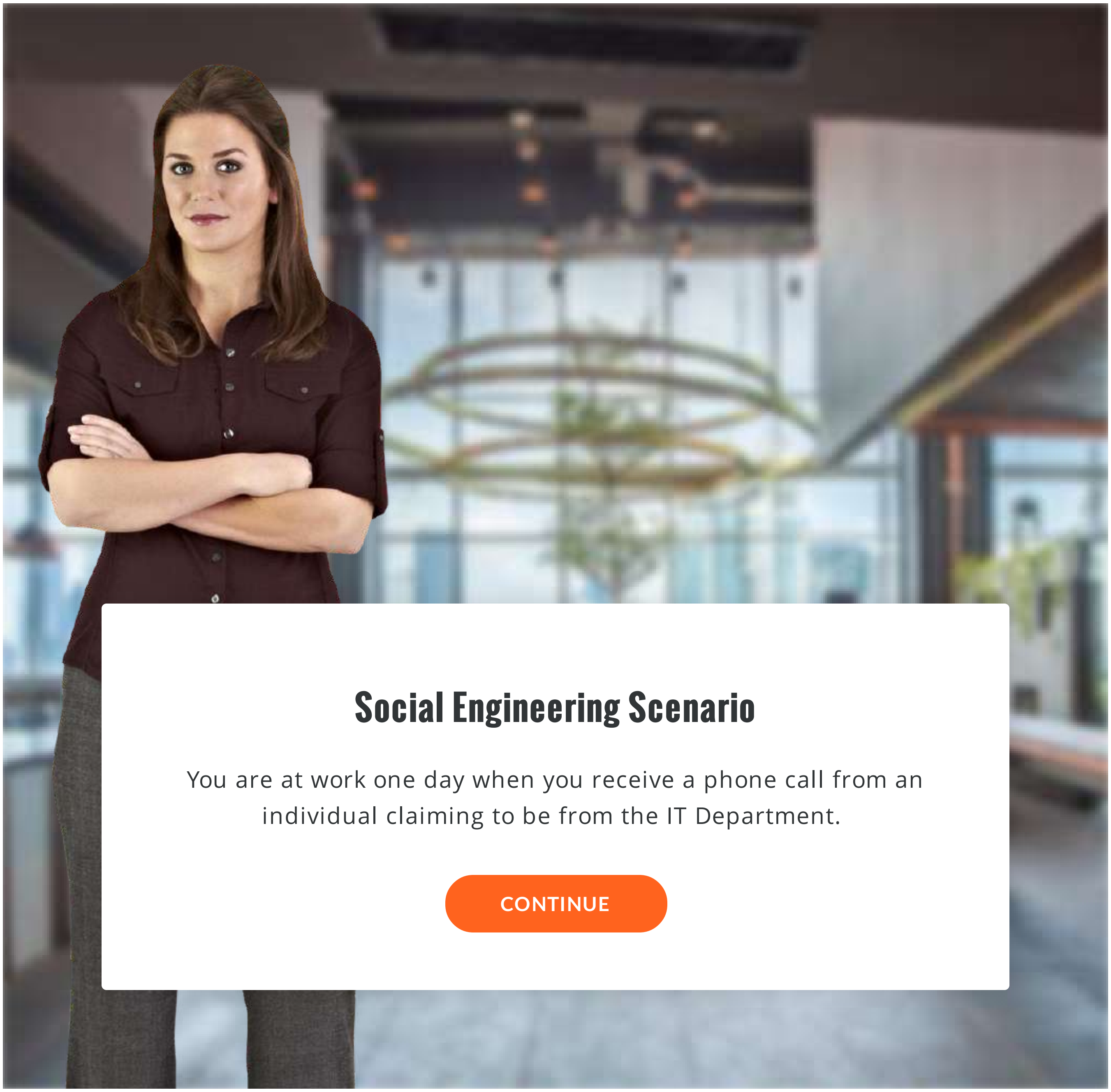
□ Be cautious of individuals being overly friendly or inquisitive about you or your job in public places.

□ Understand that social engineers are experts in the art of persuasion.

□ Be aware of physical security requirements. If you observe someone unknown to you that seems suspicious, inform your manager.

□ Be suspicious of emails with no contact information at the end of the message.

CONTINUE

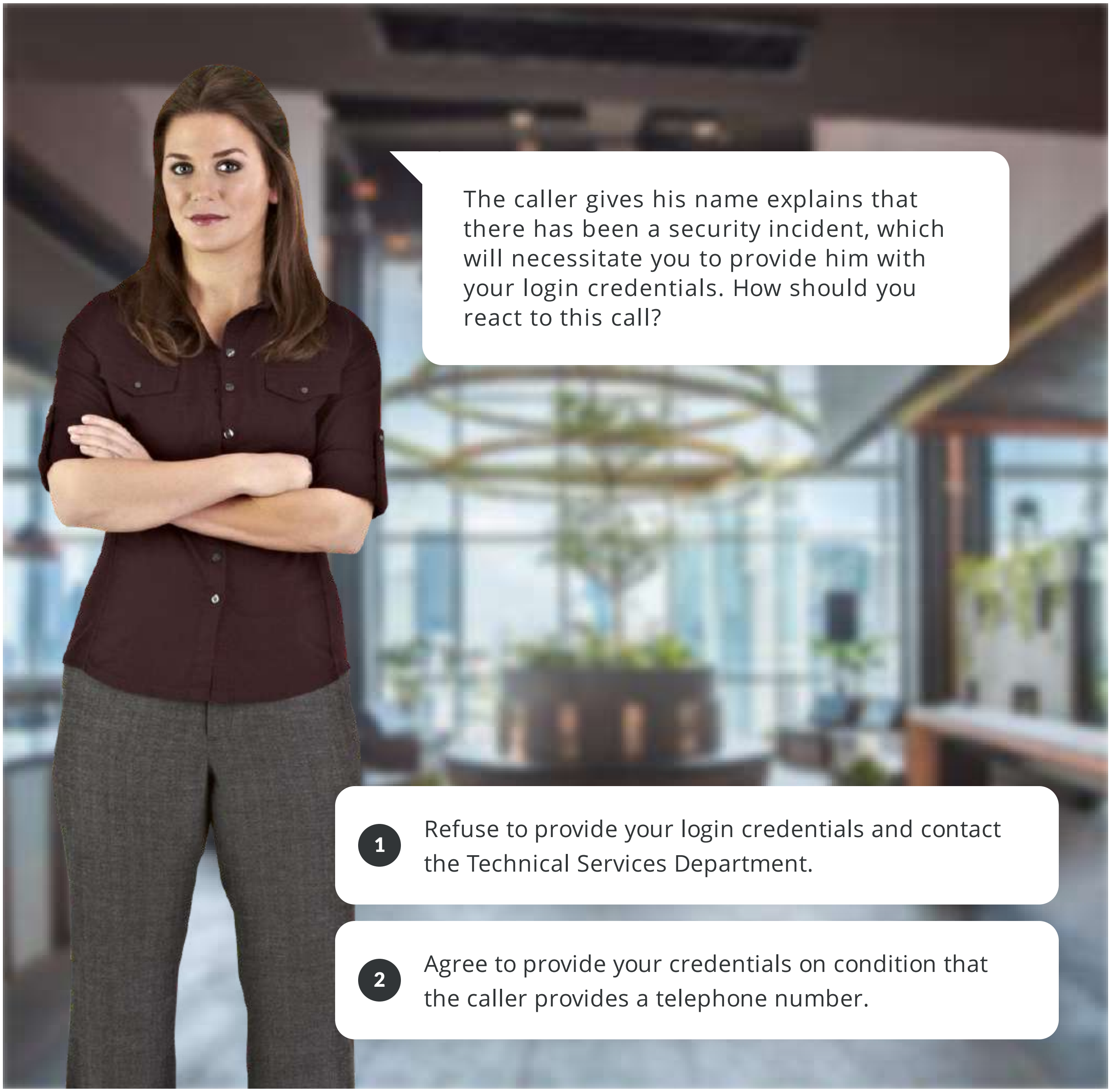


Social Engineering Scenario

You are at work one day when you receive a phone call from an individual claiming to be from the IT Department.

Scene 1 Slide 1

Continue → Next Slide



The caller gives his name explains that there has been a security incident, which will necessitate you to provide him with your login credentials. How should you react to this call?

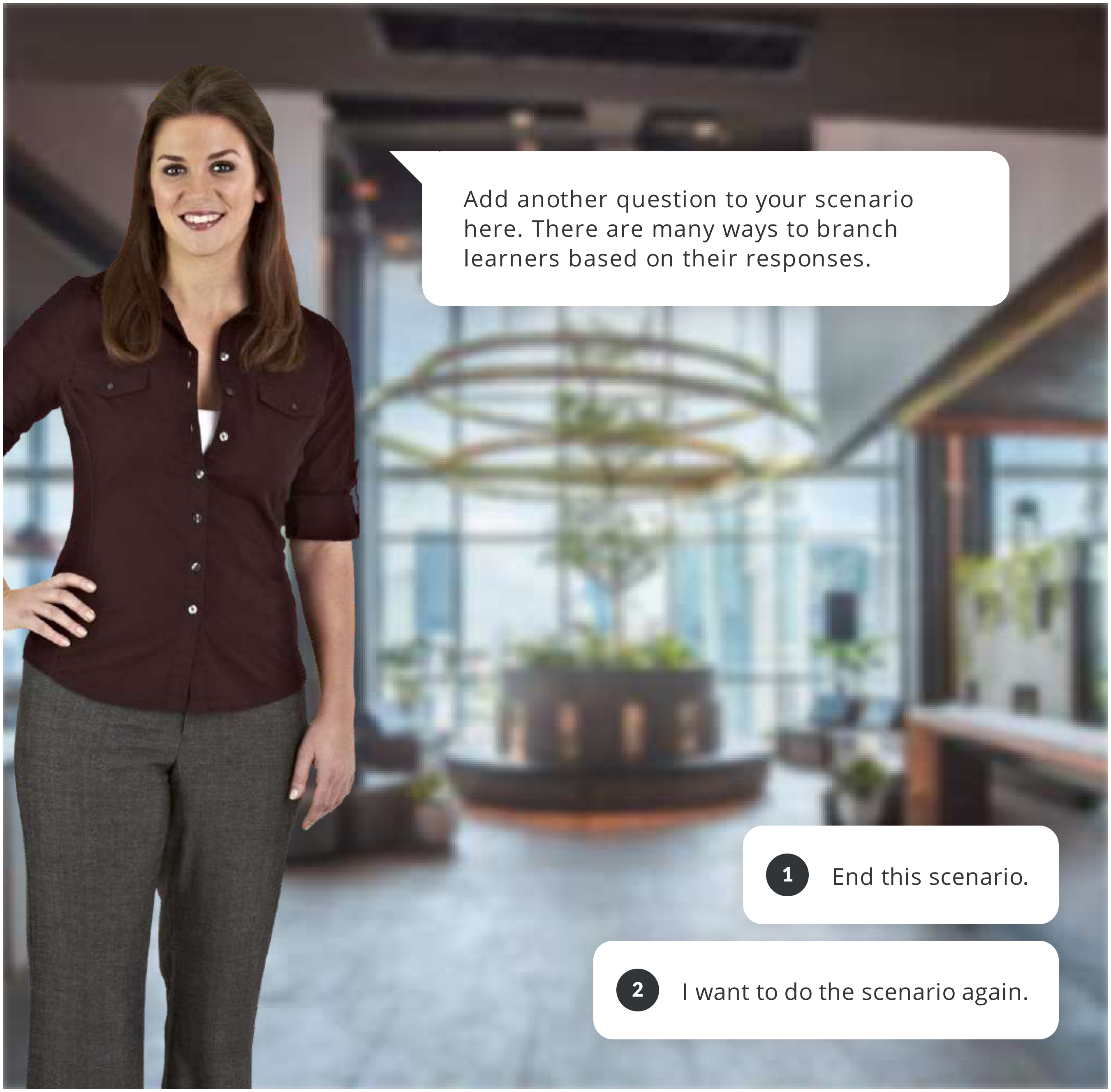
1 Refuse to provide your login credentials and contact the Technical Services Department.

2 Agree to provide your credentials on condition that the caller provides a telephone number.

Scene 1 Slide 2

0 → End of Scenario

1 → Next Slide



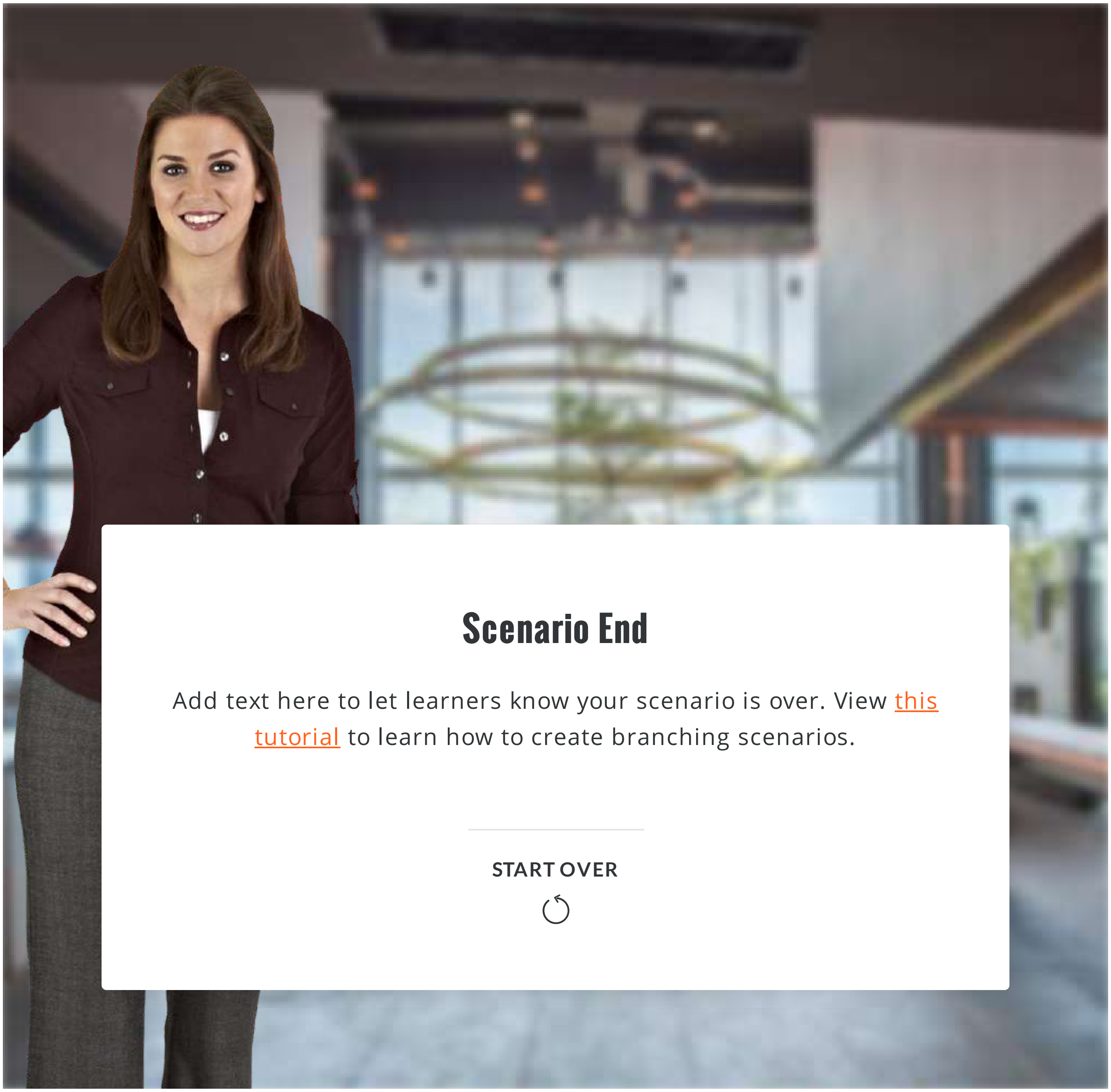
Add another question to your scenario here. There are many ways to branch learners based on their responses.

1 End this scenario.

2 I want to do the scenario again.

Scene 1 Slide 3

0 →	Next Slide
1 →	Scene 1 Slide 1



Scenario End

Add text here to let learners know your scenario is over. View this tutorial to learn how to create branching scenarios.

Scene 1 Slide 4

Continue → End of Scenario

Complete the content above before moving on.

Reporting a Security Incident

If you suspect there has been suspicious activity, please inform Technical Services immediately.

Further Reading