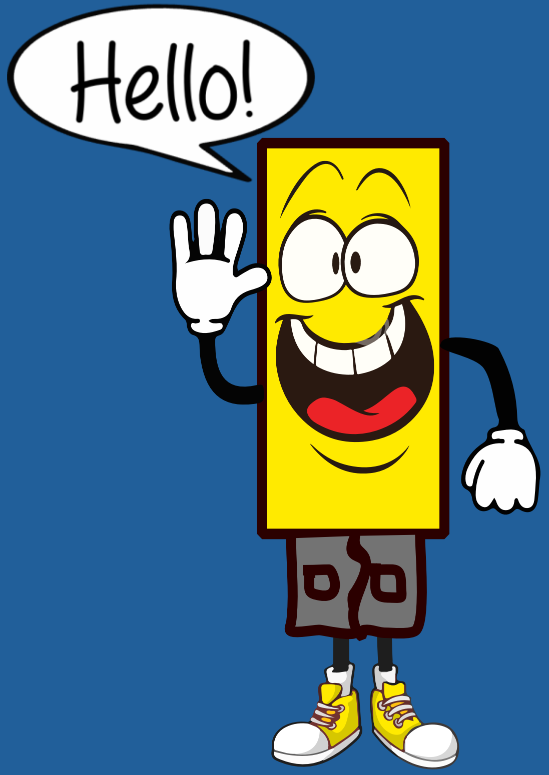
Welcome to flash drive safety

Hello, my name is Link, what is your name?

Please type your full name here and click enter.

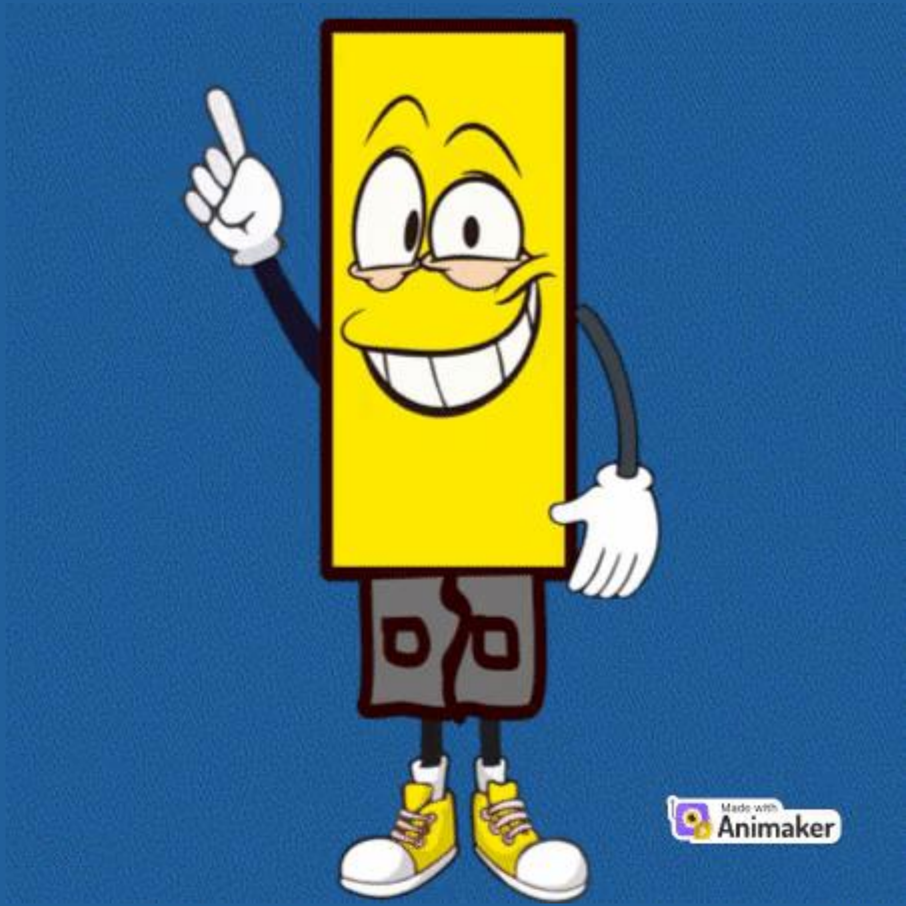


Enter

Welcome Learner,

It is great to meet you. Let's look at what we will be learning in this course.

There are four sections for you to work through.



Continue

Introduction

Lost and found flash drives

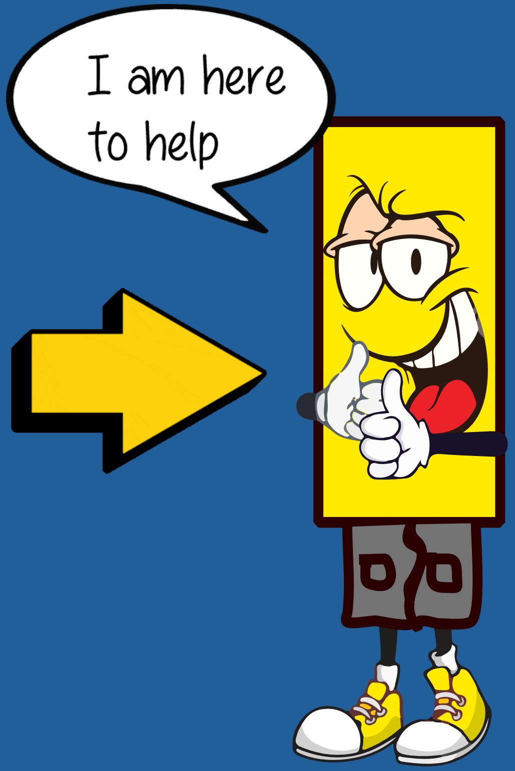
Gifted and personal flash drives

Dealing with malware

Back

Continue

If you are not sure what the correct answer is, I can help you. Whenever you see me, you can just click on me, and I will pop up with some handy hints.



Back Continue

Introduction

Flash drives, and their incorrect use, can pose a risk to our network security.

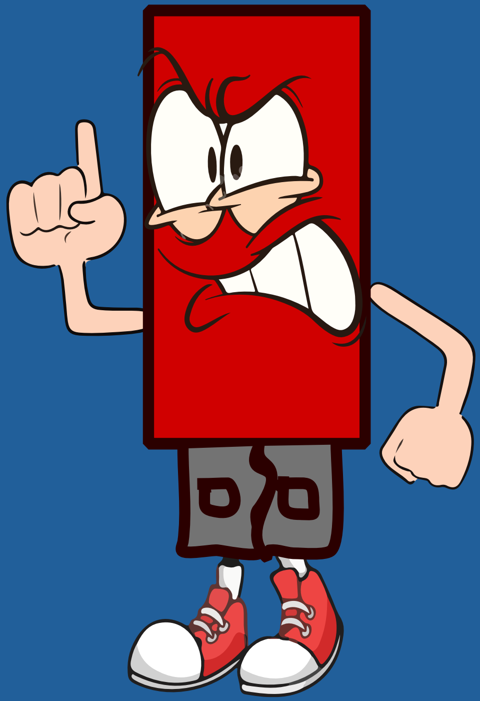
But before we begin to learn about flash drive safety, let’s look at some of the technical terms you may encounter.

Back Continue

Flash drive

A flash drive is a small, portable data storage device that uses flash memory to store and transfer data.

Flash drives are also known as USB drives, thumb drives, or removable storage devices.



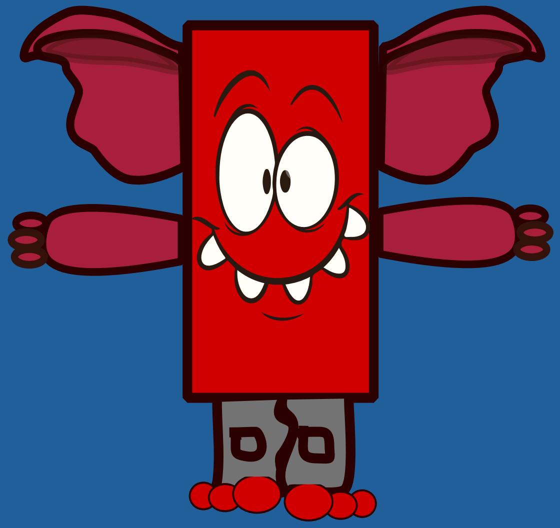
Back

Continue

Malware

Malware is short for malicious software and refers to any program or file that is intentionally harmful to a computer, network, or server.

Malware is like the mischievous gremlin of the computer world and can cause chaos in your system. It includes viruses, spyware, and other destructive programs.



Back Continue

Ransomware

Ransomware is a type of malware that encrypts a victim’s files or locks them out of their system and demands a ransom to restore access. Think of ransomware as the pirates of cyberspace.

Ransomware locks up your files, holds them hostage, and demands a reward to set them free.

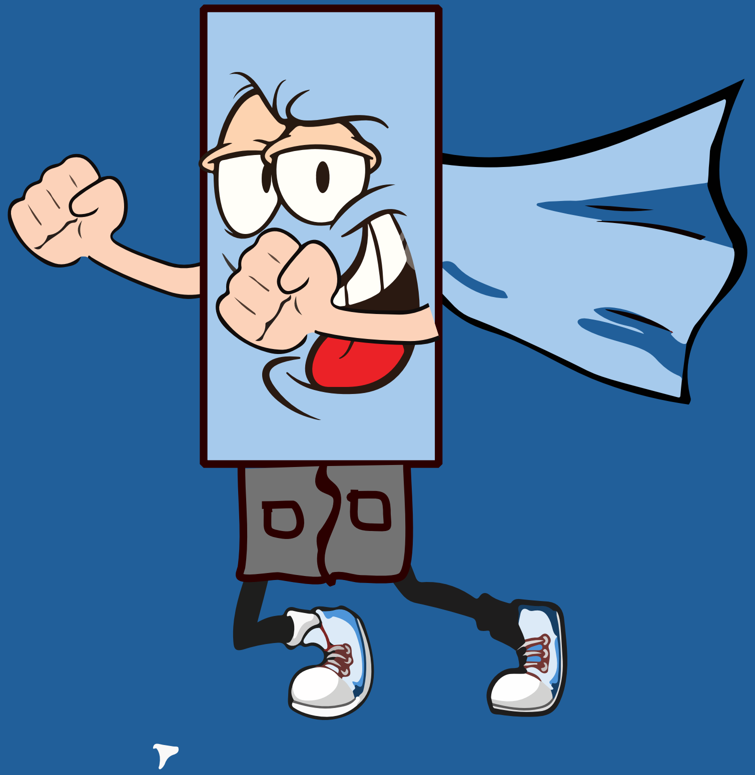
Back

Continue

Cyber security

Cyber security is the process of protecting computer systems, networks, and data from digital threats, such as hacking, malware, and any other unauthorized access.

Think of cyber security as the superhero that protects your computer or network from malicious threats.

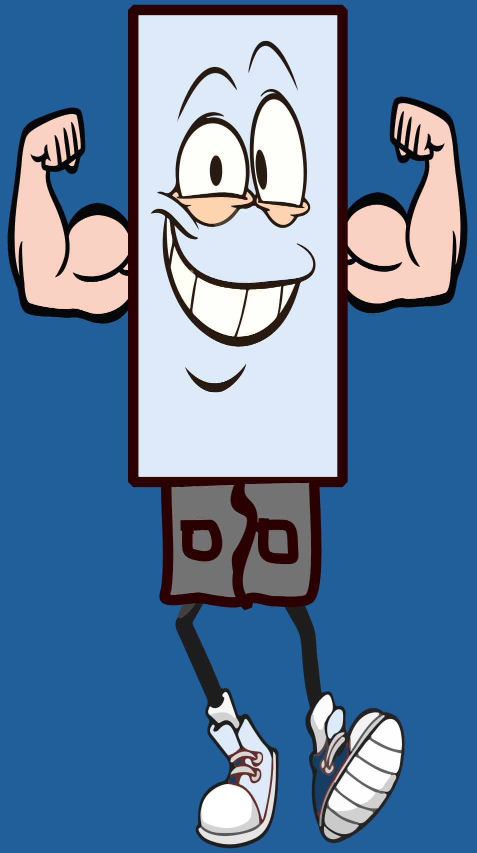


Back

Continue

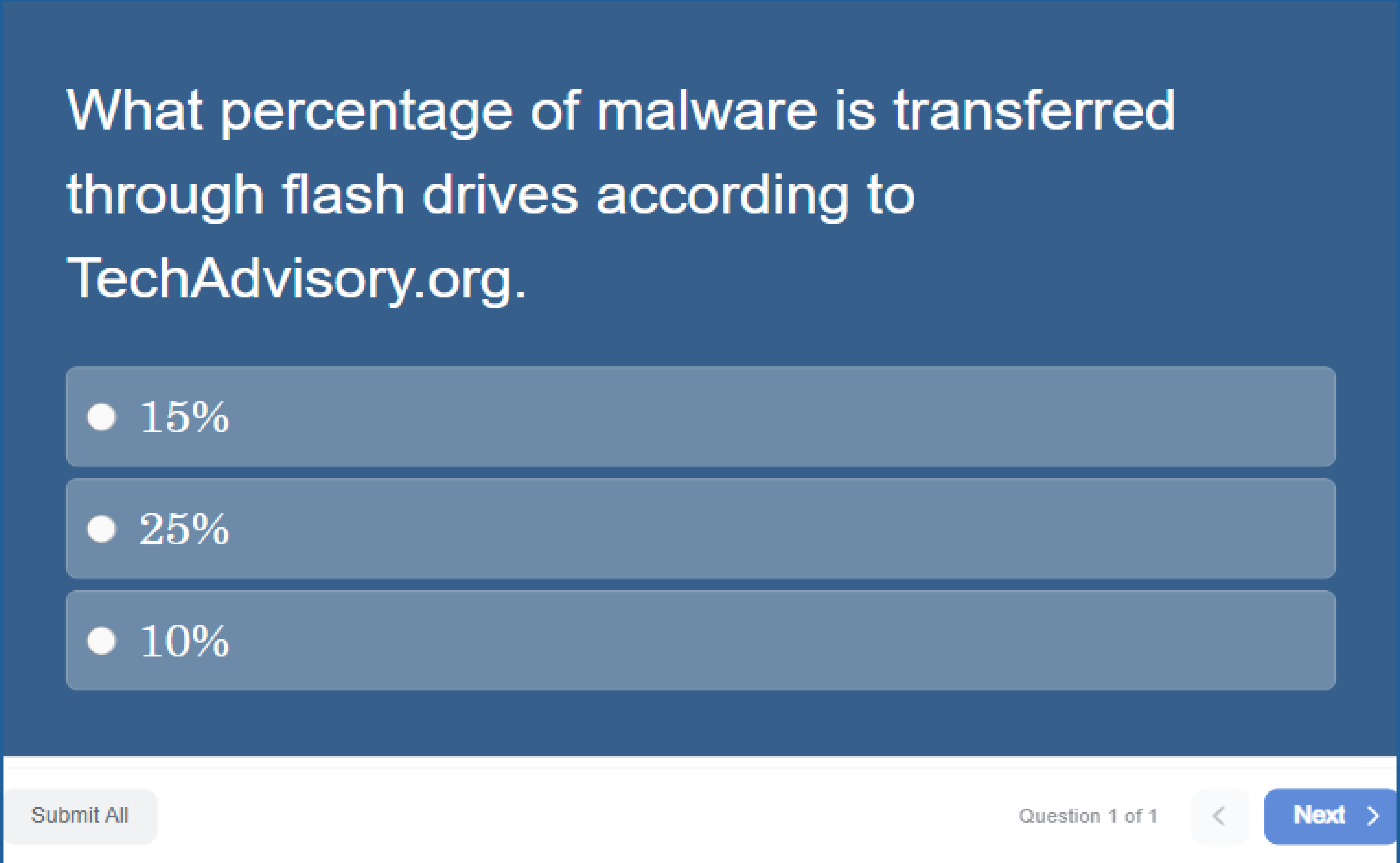
Firewall

A firewall is a security system that acts as a barrier between a private network and external networks, like the internet. It controls incoming and outgoing network traffic based on predetermined security rules to prevent unauthorized access and potential threats.



Imagine your computer or network as an exclusive club and the firewall is the bouncer who decides who gets in and who does not.

Back Continue

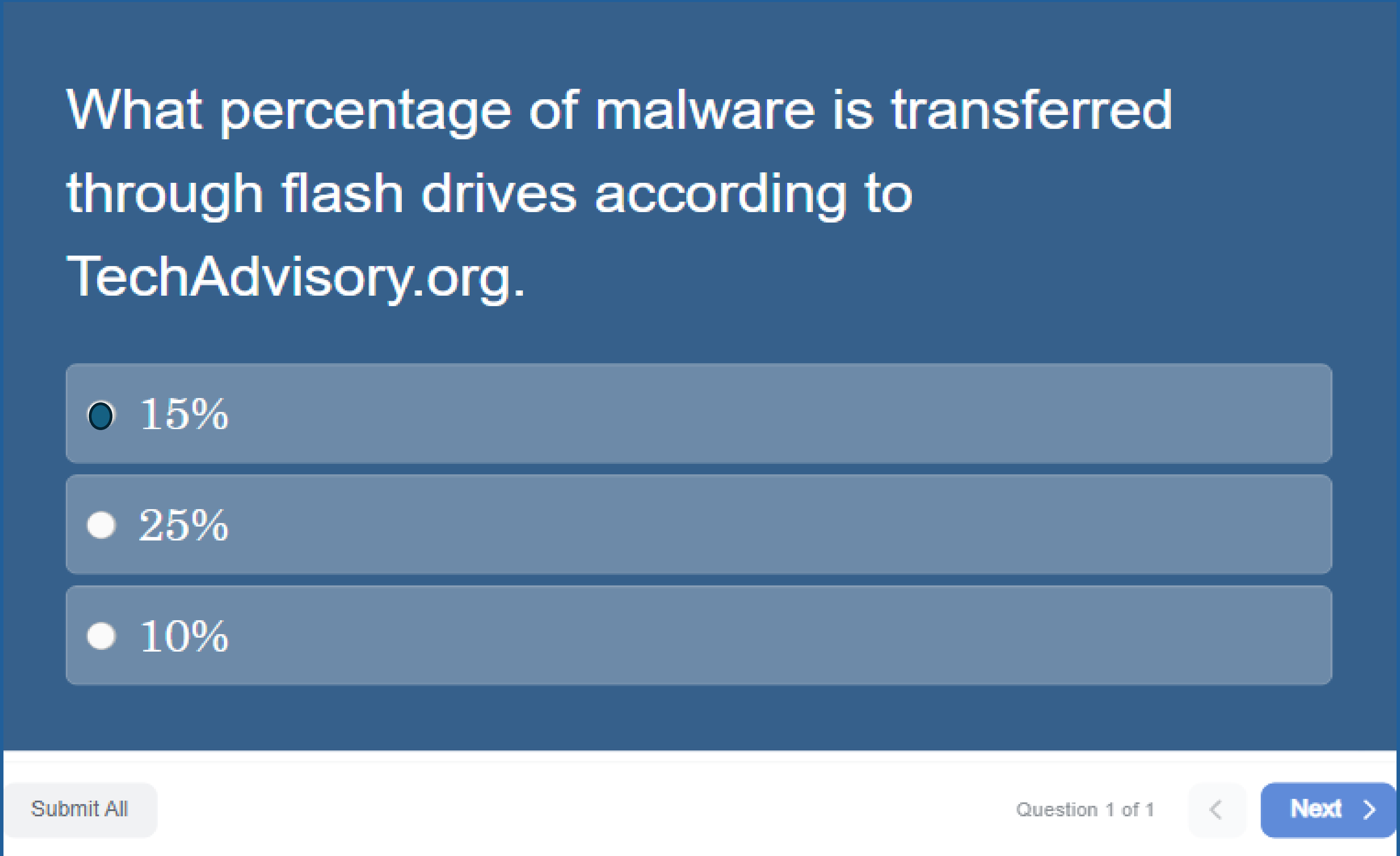


What percentage of malware is transferred through flash drives according to TechAdvisory.org.

● 15%

● 25%

● 10%

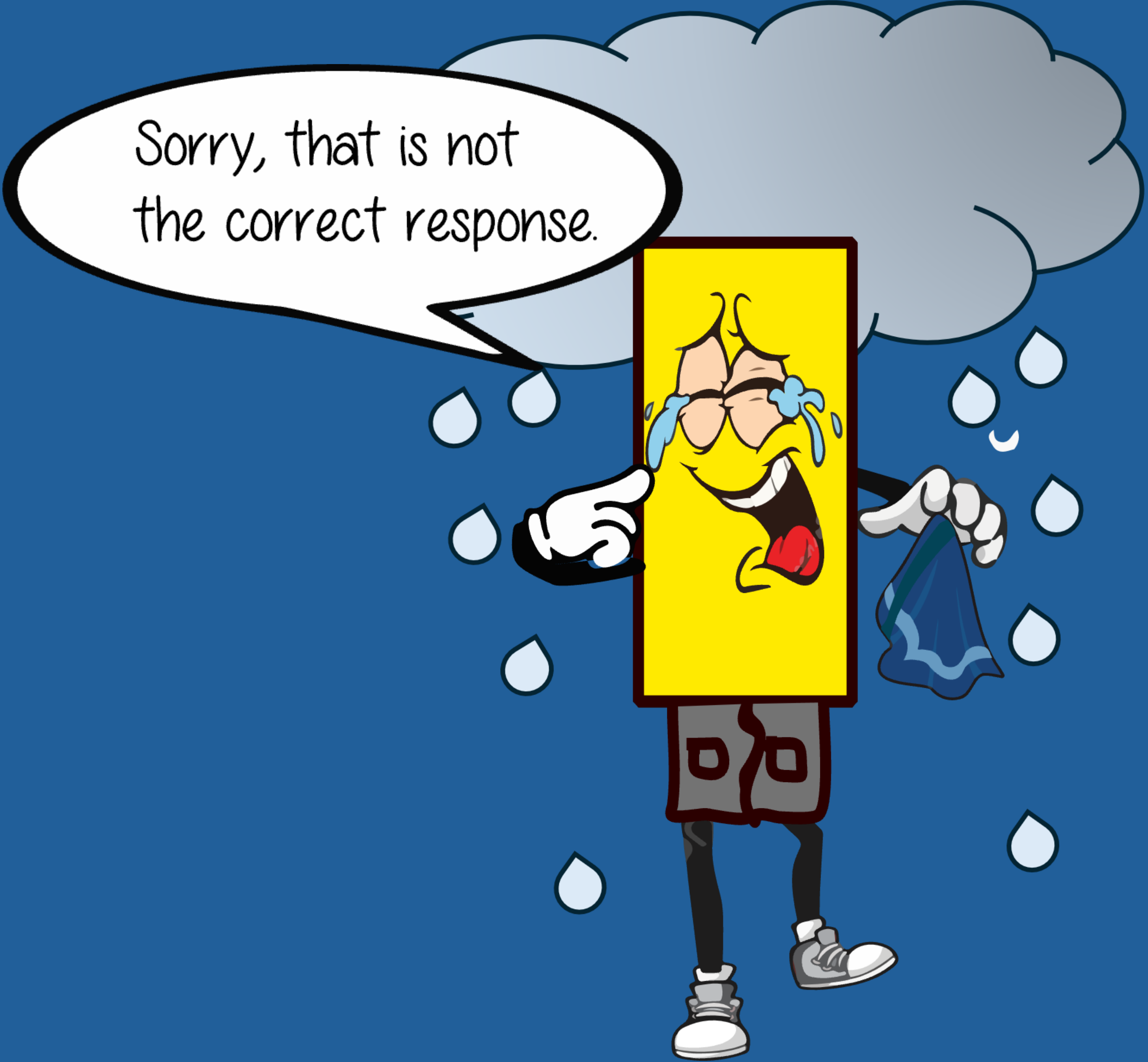


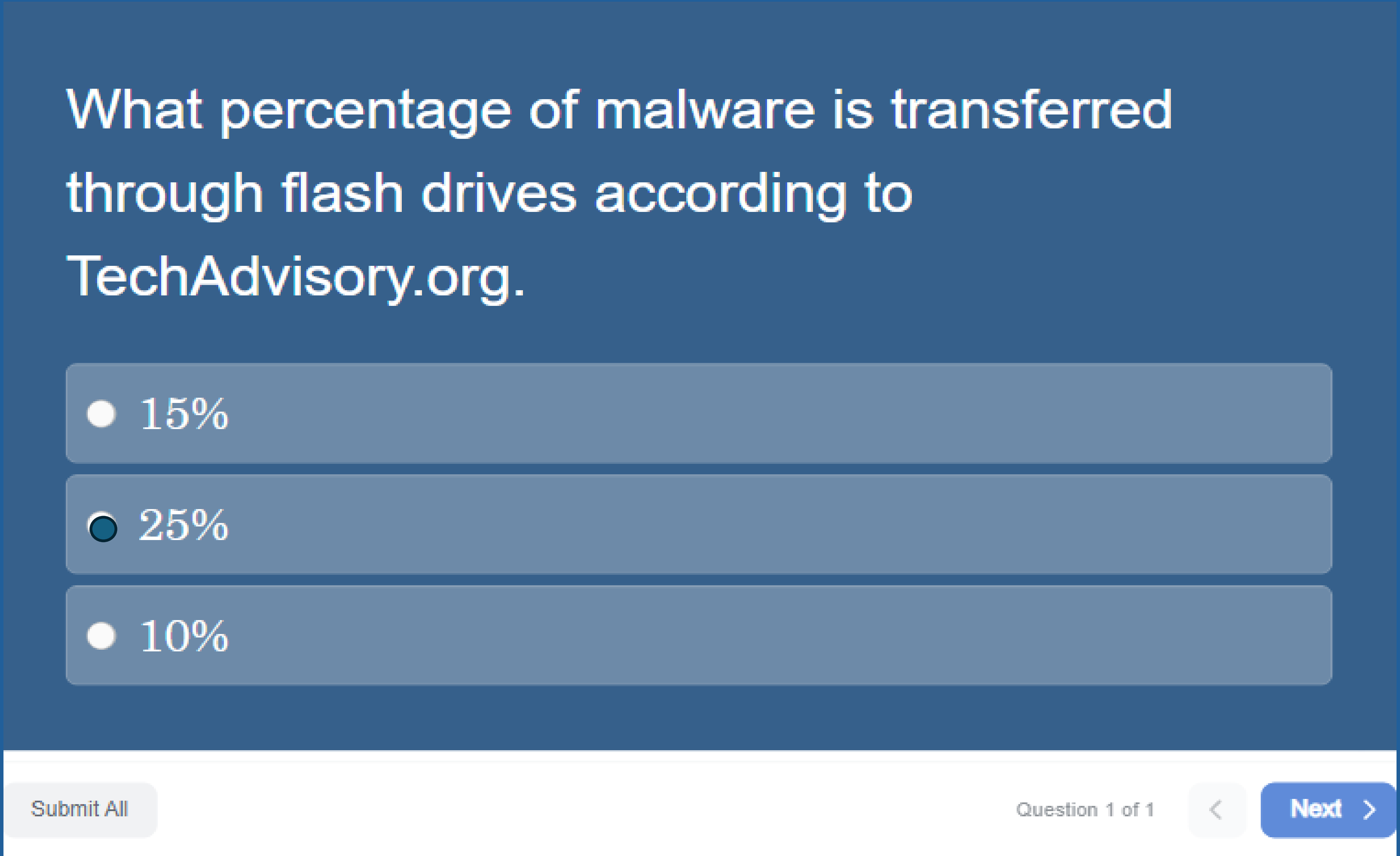
What percentage of malware is transferred through flash drives according to TechAdvisory.org.

● 15%

○ 25%

○ 10%


Sorry, that is not the correct response.

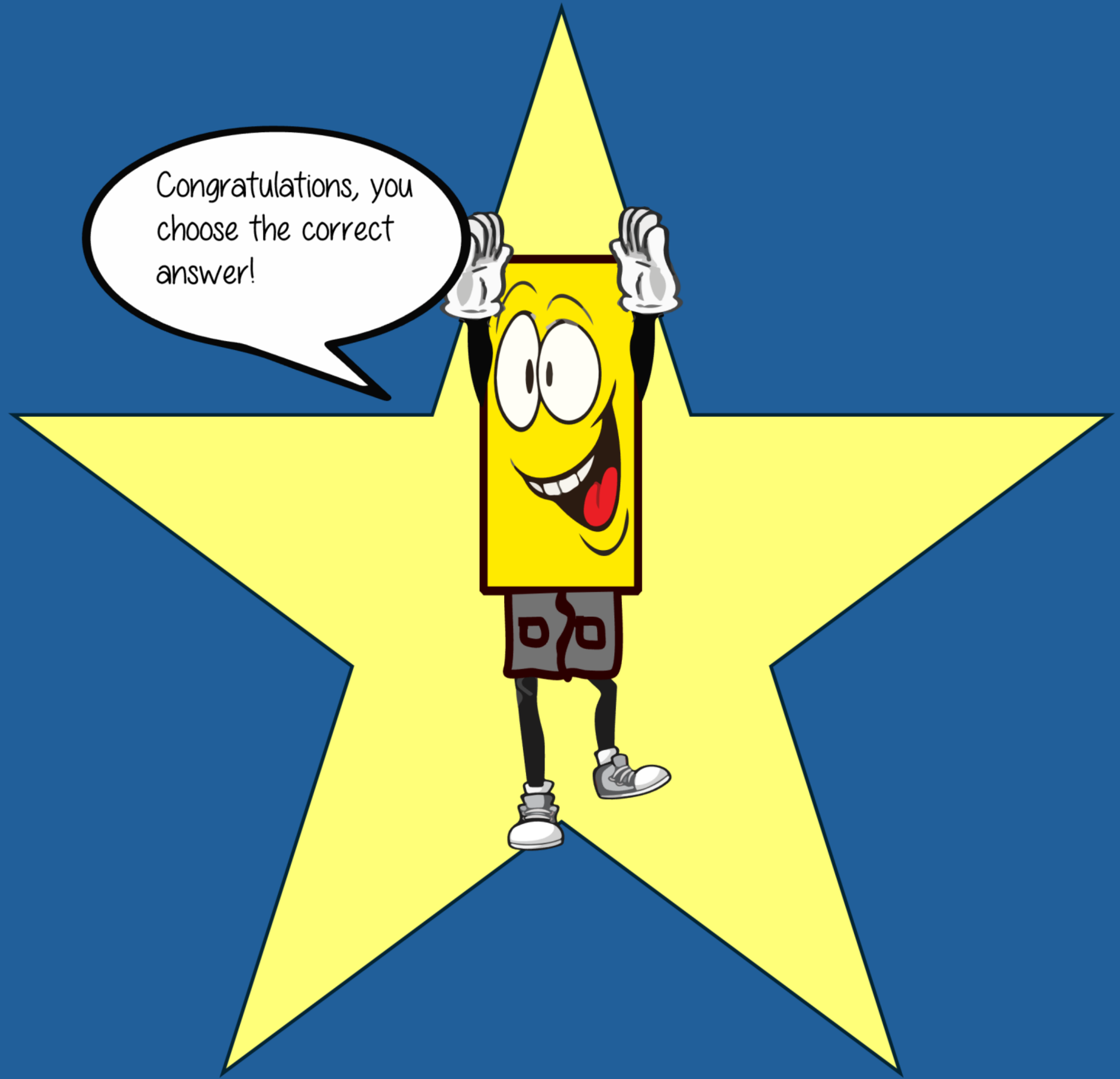


What percentage of malware is transferred through flash drives according to TechAdvisory.org.

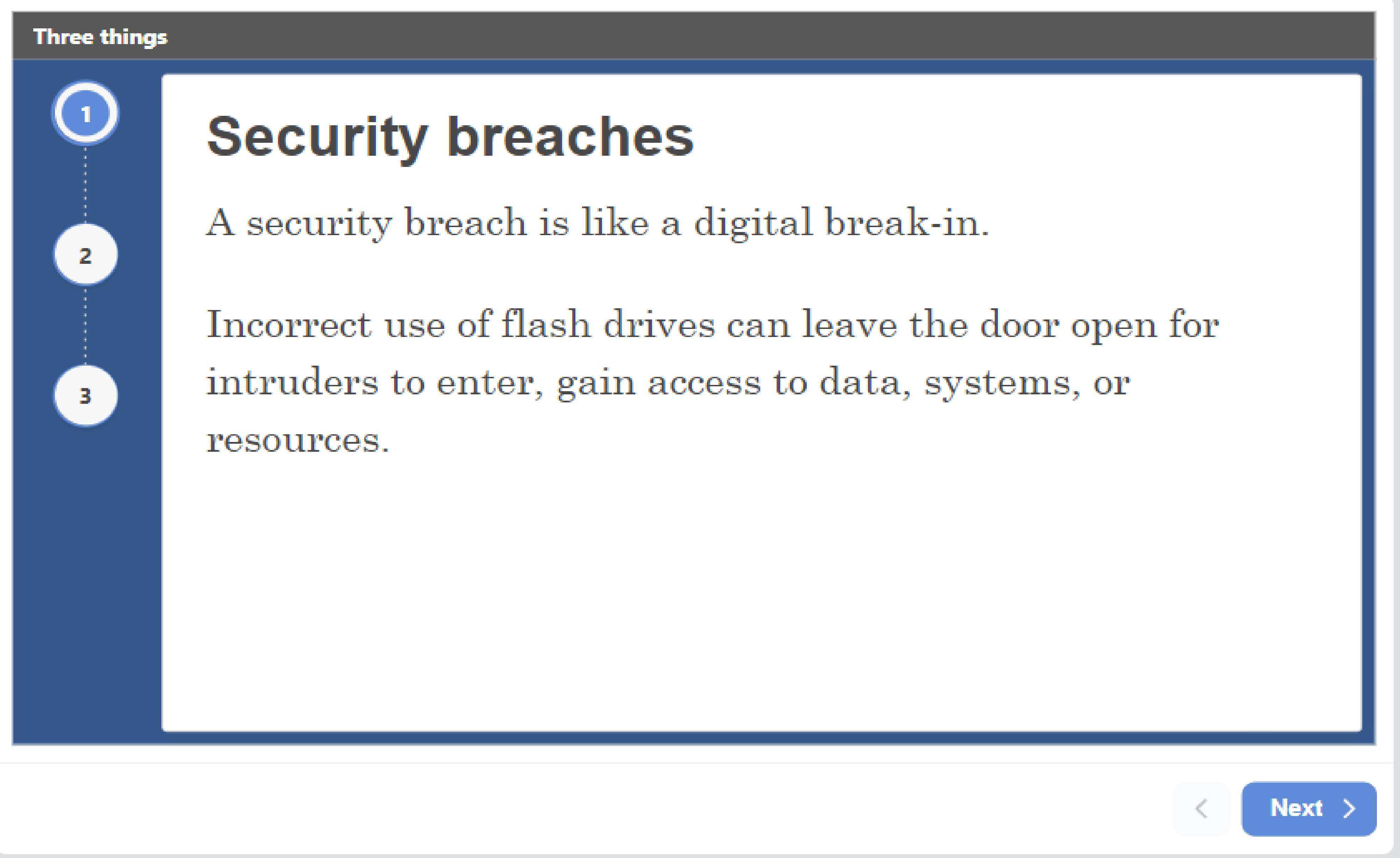
○ 15%

● 25%

○ 10%


Congratulations, you choose the correct answer!

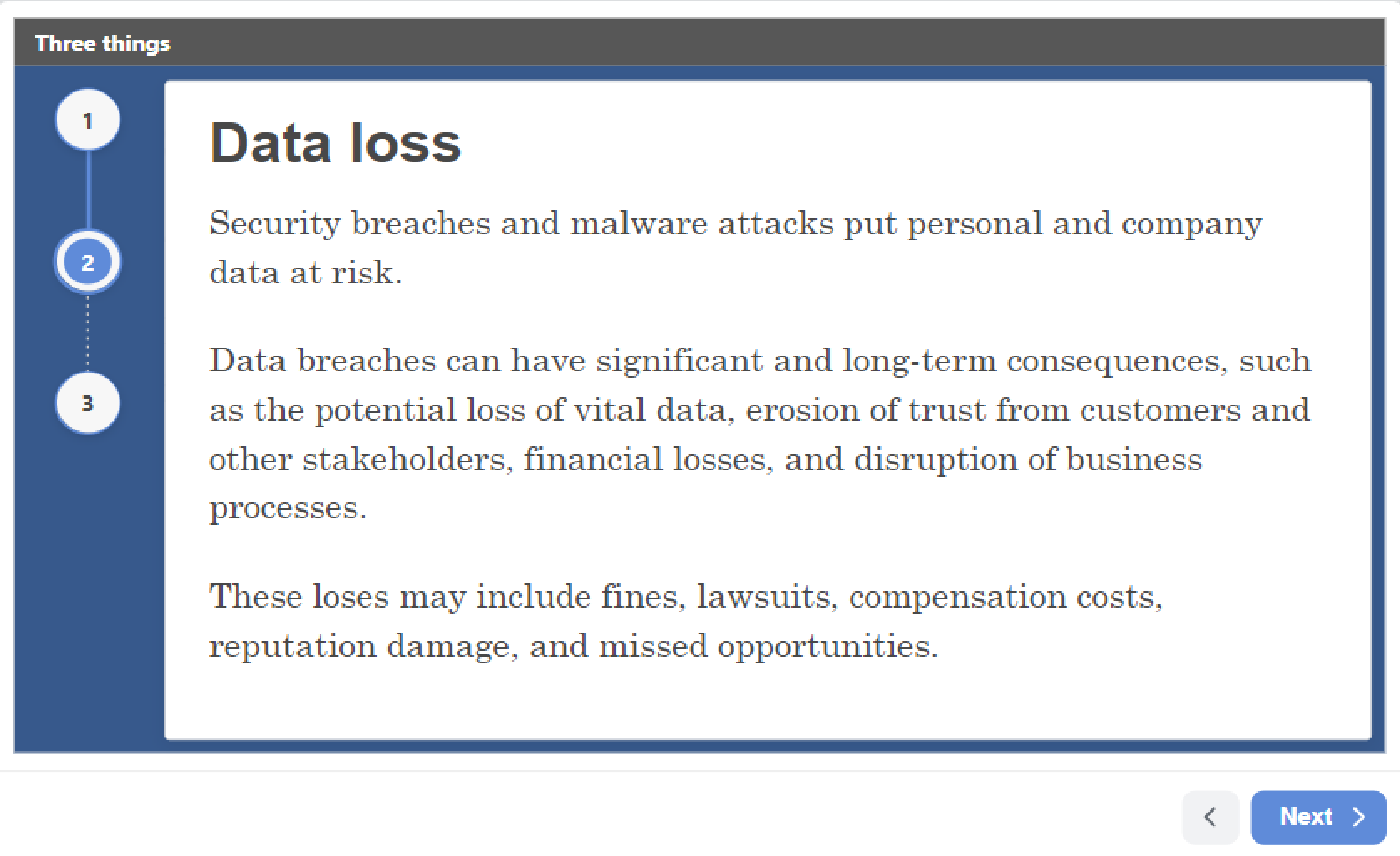
What can improper use of flash drives cause?



Security breaches

A security breach is like a digital break-in.

Incorrect use of flash drives can leave the door open for intruders to enter, gain access to data, systems, or resources.



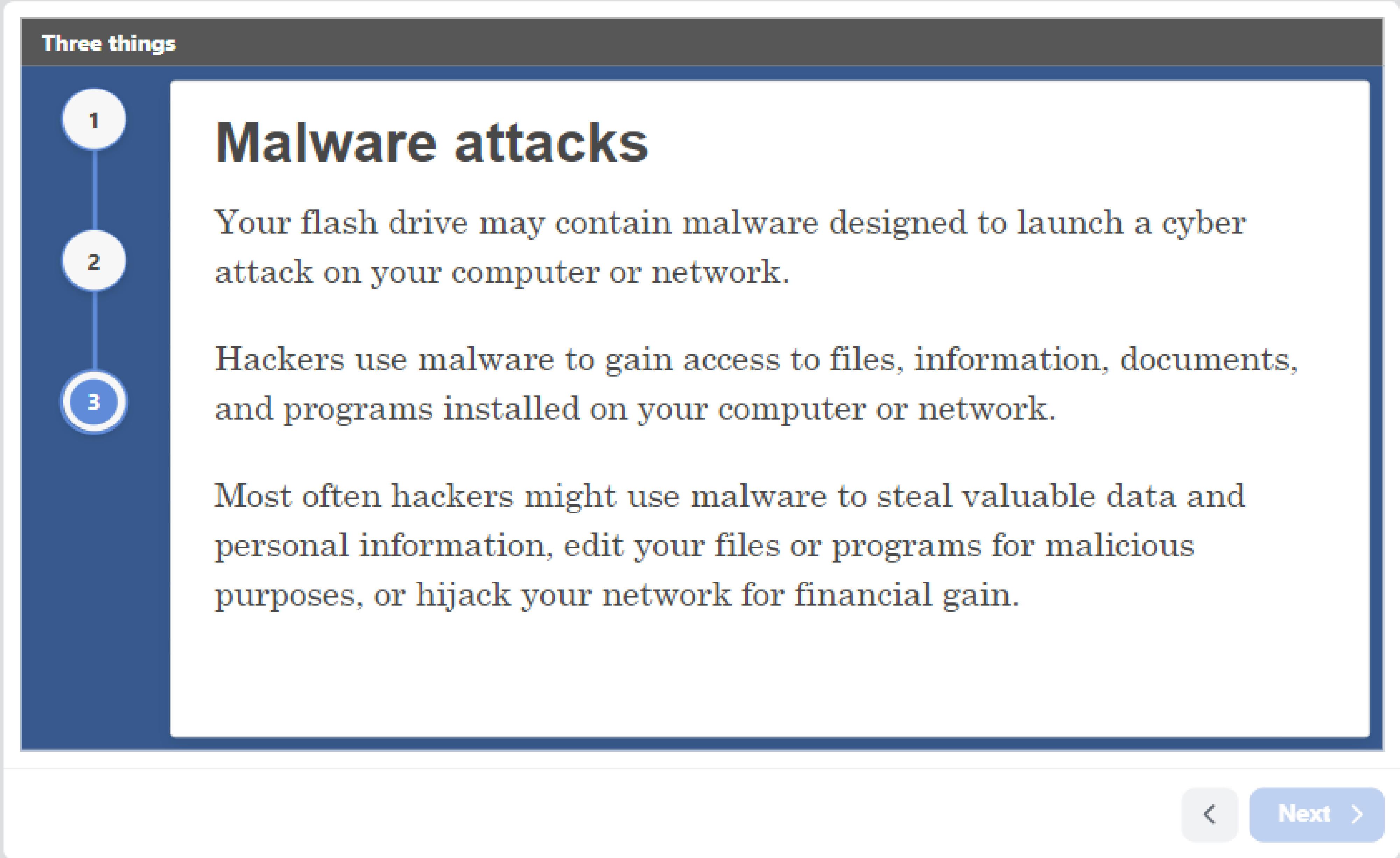
Three things

Data loss

Security breaches and malware attacks put personal and company data at risk.

Data breaches can have significant and long-term consequences, such as the potential loss of vital data, erosion of trust from customers and other stakeholders, financial losses, and disruption of business processes.

These loses may include fines, lawsuits, compensation costs, reputation damage, and missed opportunities.



Malware attacks

Your flash drive may contain malware designed to launch a cyber attack on your computer or network.

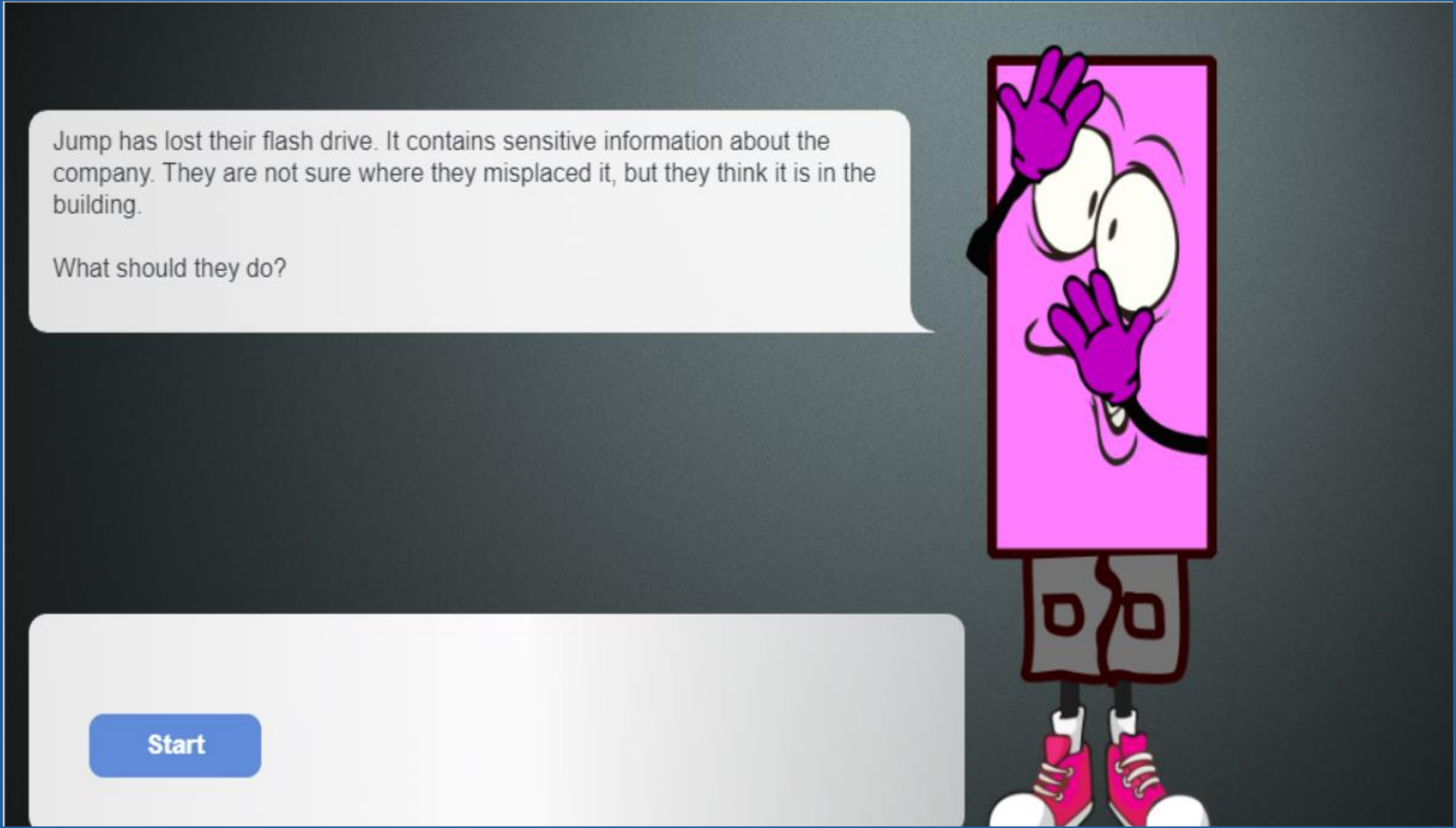
Hackers use malware to gain access to files, information, documents, and programs installed on your computer or network.

Most often hackers might use malware to steal valuable data and personal information, edit your files or programs for malicious purposes, or hijack your network for financial gain.

In this section, we will explore situations when a flash drive is lost.

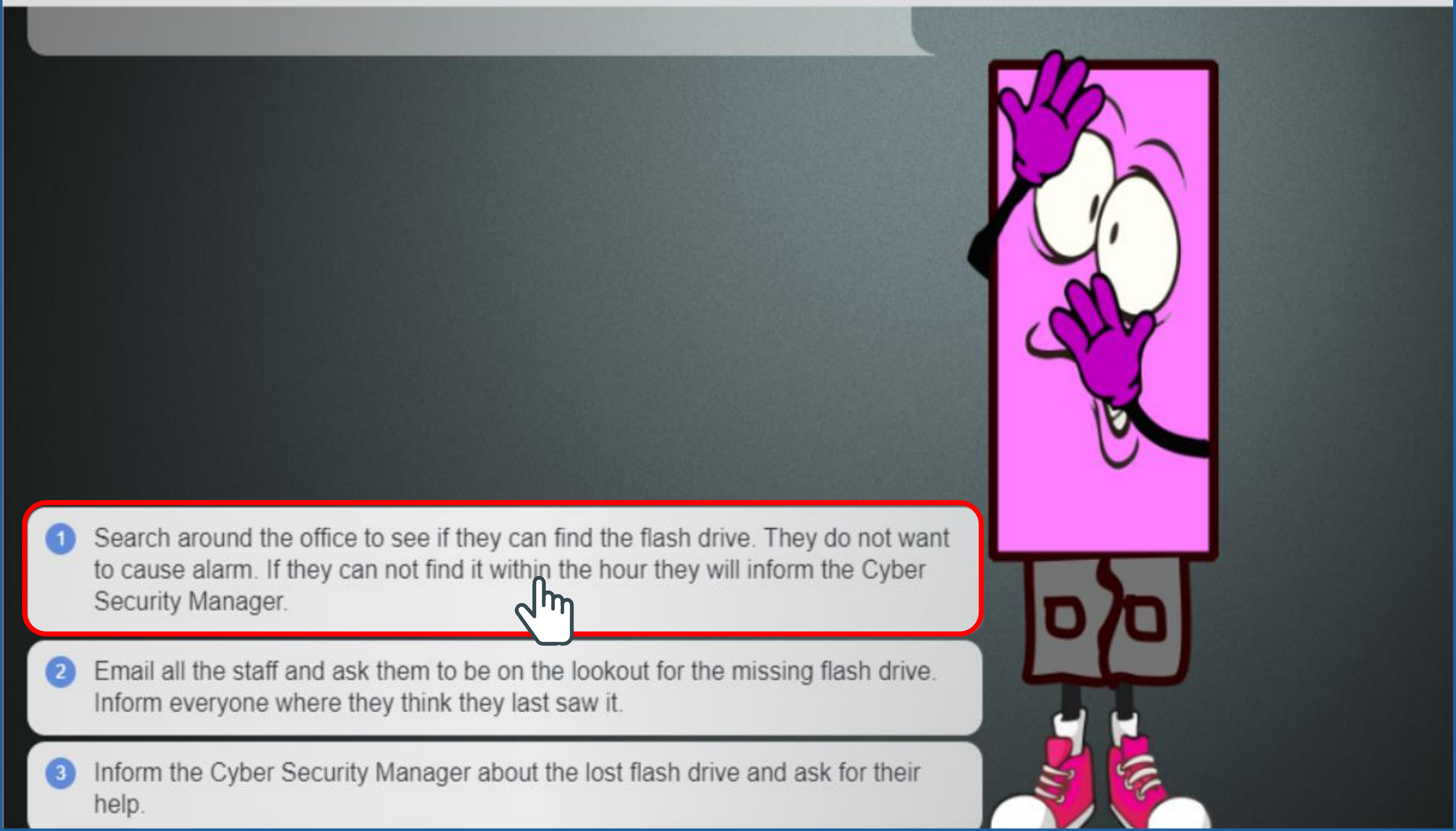
Back Continue

Lost and found flash drives

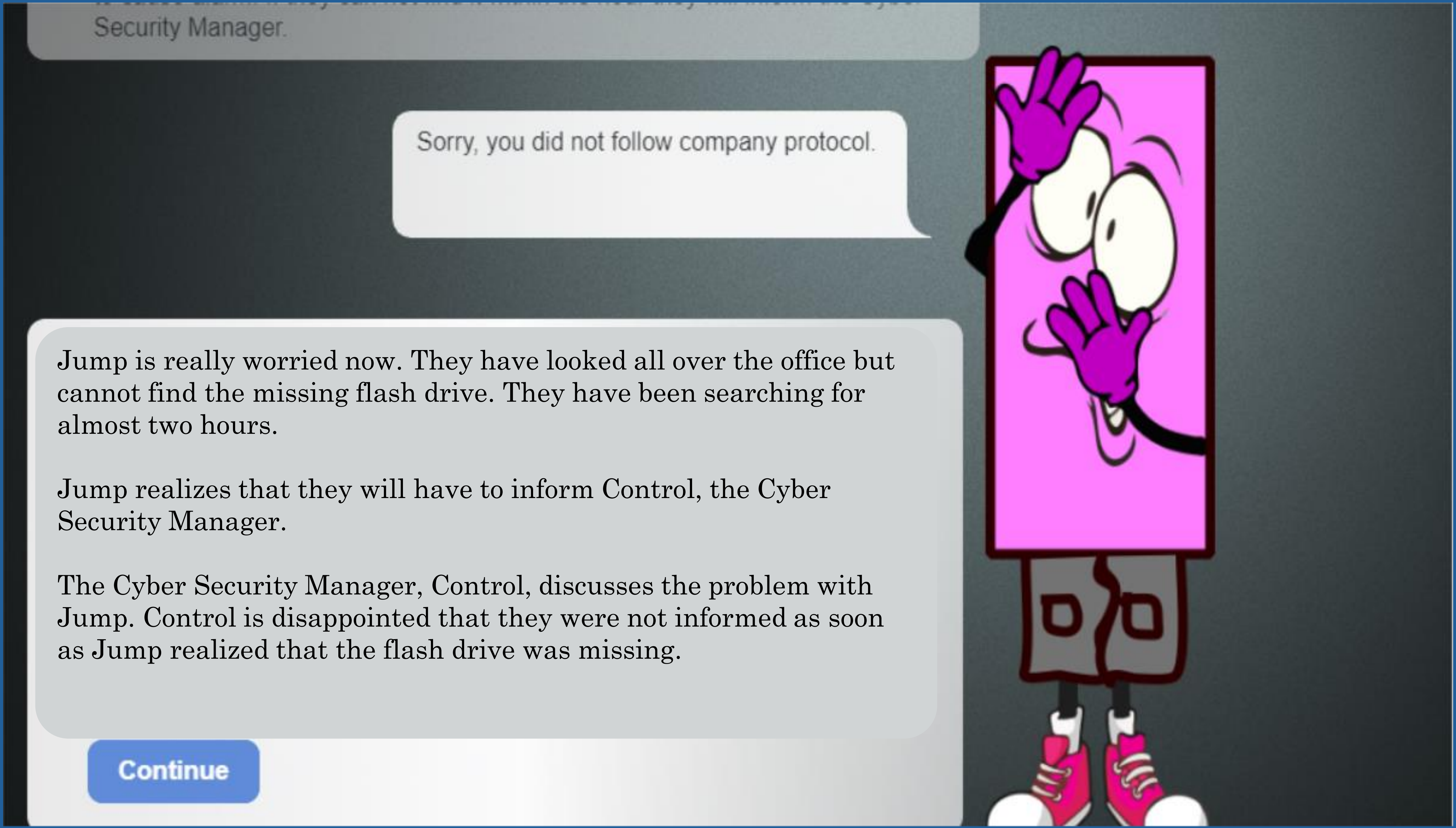


Jump has lost their flash drive. It contains sensitive information about the company. They are not sure where they misplaced it, but they think it is in the building.

What should they do?



1. Search around the office to see if they can find the flash drive. They do not want to cause alarm. If they can not find it within the hour they will inform the Cyber Security Manager.
2. Email all the staff and ask them to be on the lookout for the missing flash drive. Inform everyone where they think they last saw it.
3. Inform the Cyber Security Manager about the lost flash drive and ask for their help.



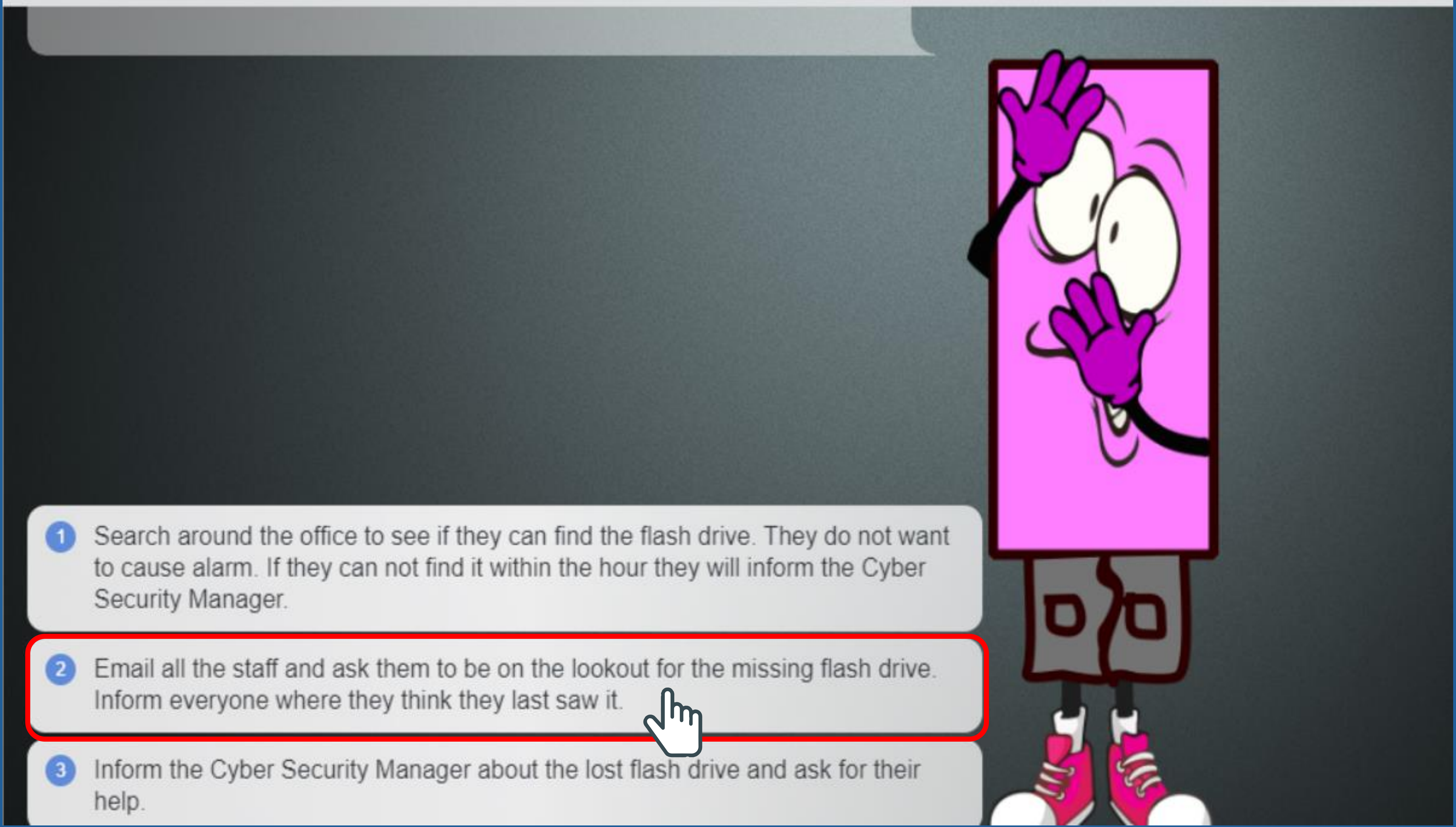
Security Manager.

Sorry, you did not follow company protocol.

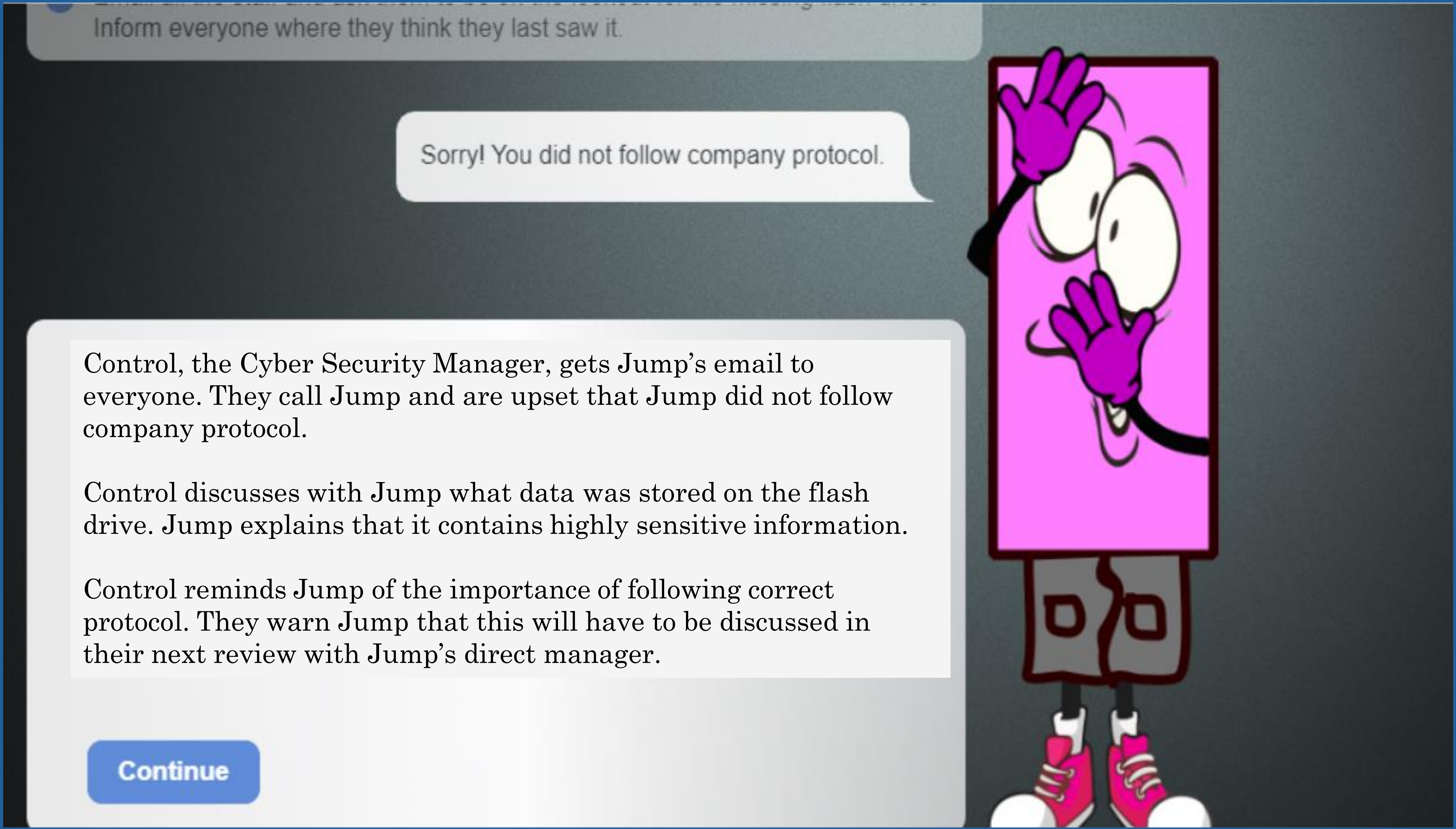
Jump is really worried now. They have looked all over the office but cannot find the missing flash drive. They have been searching for almost two hours.

Jump realizes that they will have to inform Control, the Cyber Security Manager.

The Cyber Security Manager, Control, discusses the problem with Jump. Control is disappointed that they were not informed as soon as Jump realized that the flash drive was missing.



1. Search around the office to see if they can find the flash drive. They do not want to cause alarm. If they can not find it within the hour they will inform the Cyber Security Manager.
2. Email all the staff and ask them to be on the lookout for the missing flash drive. Inform everyone where they think they last saw it.
3. Inform the Cyber Security Manager about the lost flash drive and ask for their help.



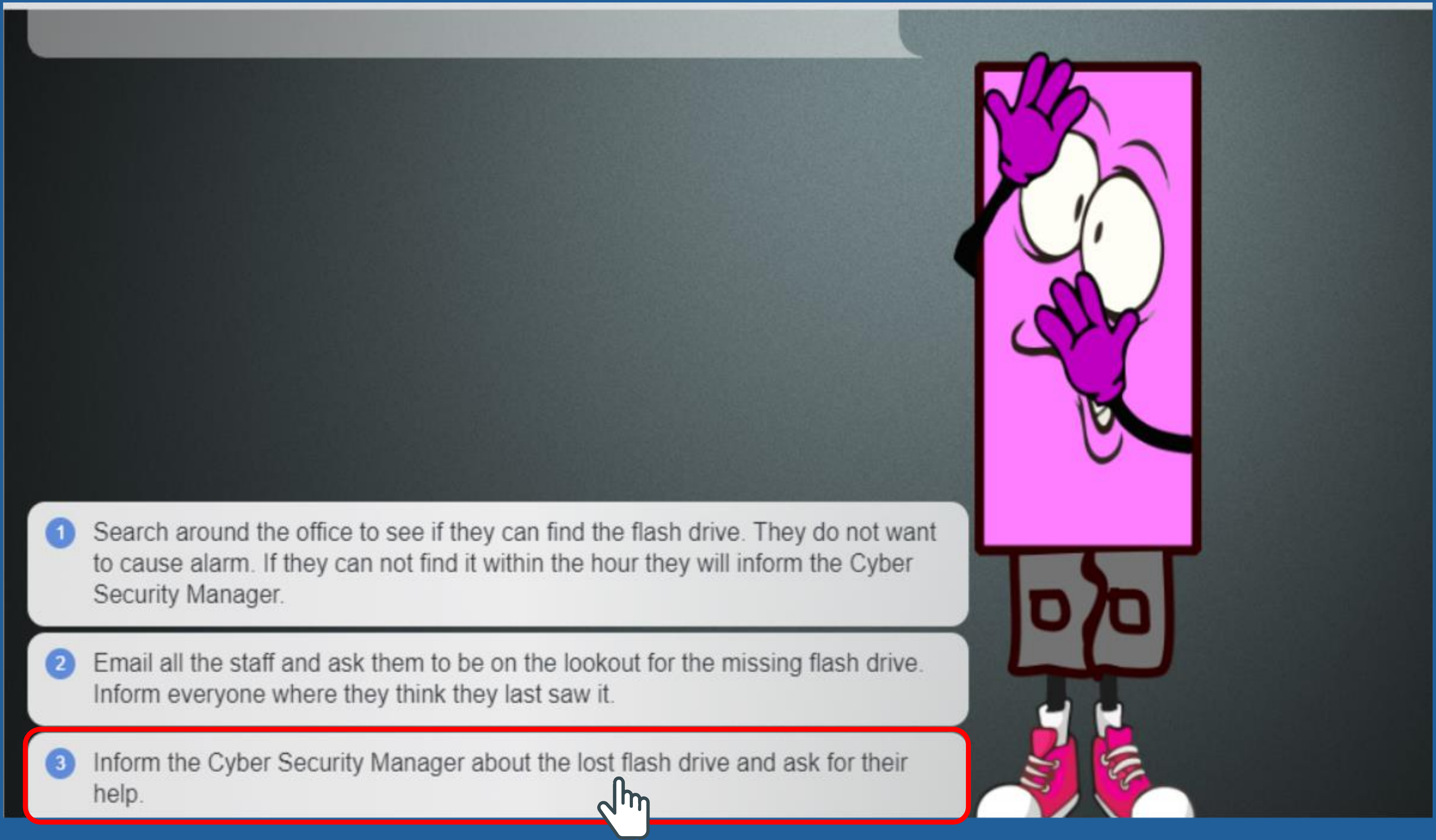
Inform everyone where they think they last saw it.

Sorry! You did not follow company protocol.

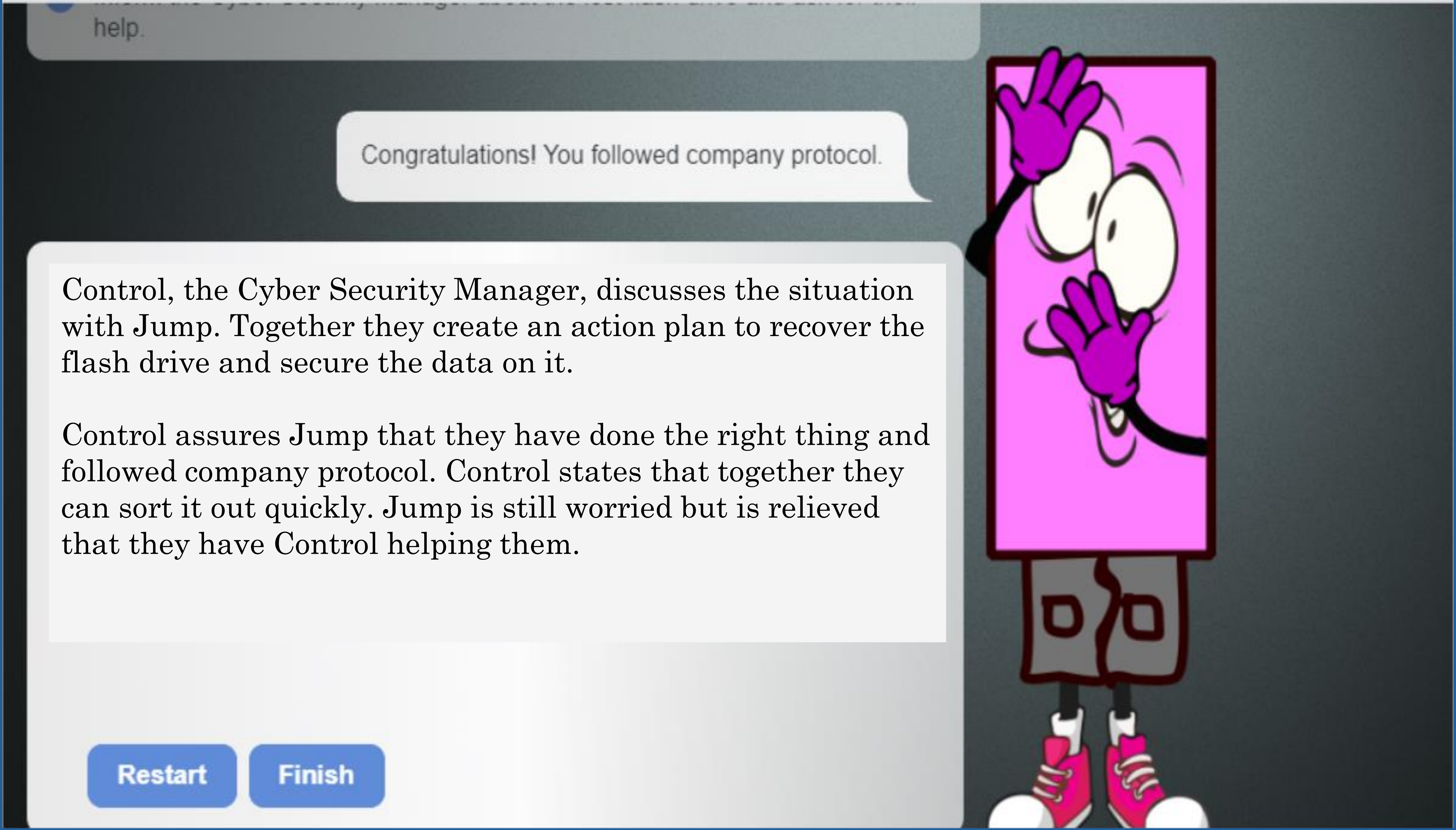
Control, the Cyber Security Manager, gets Jump’s email to everyone. They call Jump and are upset that Jump did not follow company protocol.

Control discusses with Jump what data was stored on the flash drive. Jump explains that it contains highly sensitive information.

Control reminds Jump of the importance of following correct protocol. They warn Jump that this will have to be discussed in their next review with Jump’s direct manager.



1. Search around the office to see if they can find the flash drive. They do not want to cause alarm. If they can not find it within the hour they will inform the Cyber Security Manager.
2. Email all the staff and ask them to be on the lookout for the missing flash drive. Inform everyone where they think they last saw it.
3. Inform the Cyber Security Manager about the lost flash drive and ask for their help.

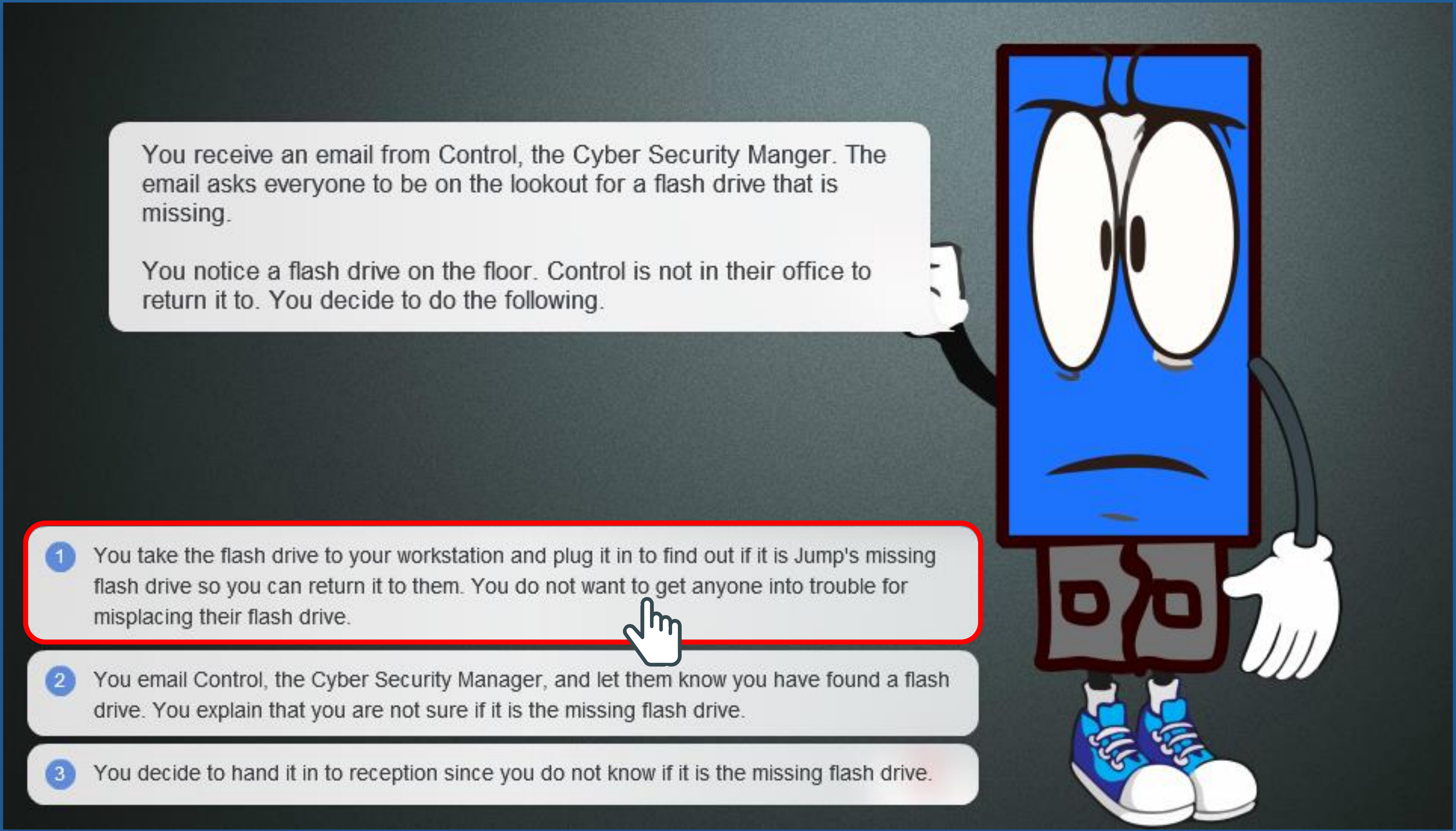


help.

Congratulations! You followed company protocol.

Control, the Cyber Security Manager, discusses the situation with Jump. Together they create an action plan to recover the flash drive and secure the data on it.

Control assures Jump that they have done the right thing and followed company protocol. Control states that together they can sort it out quickly. Jump is still worried but is relieved that they have Control helping them.



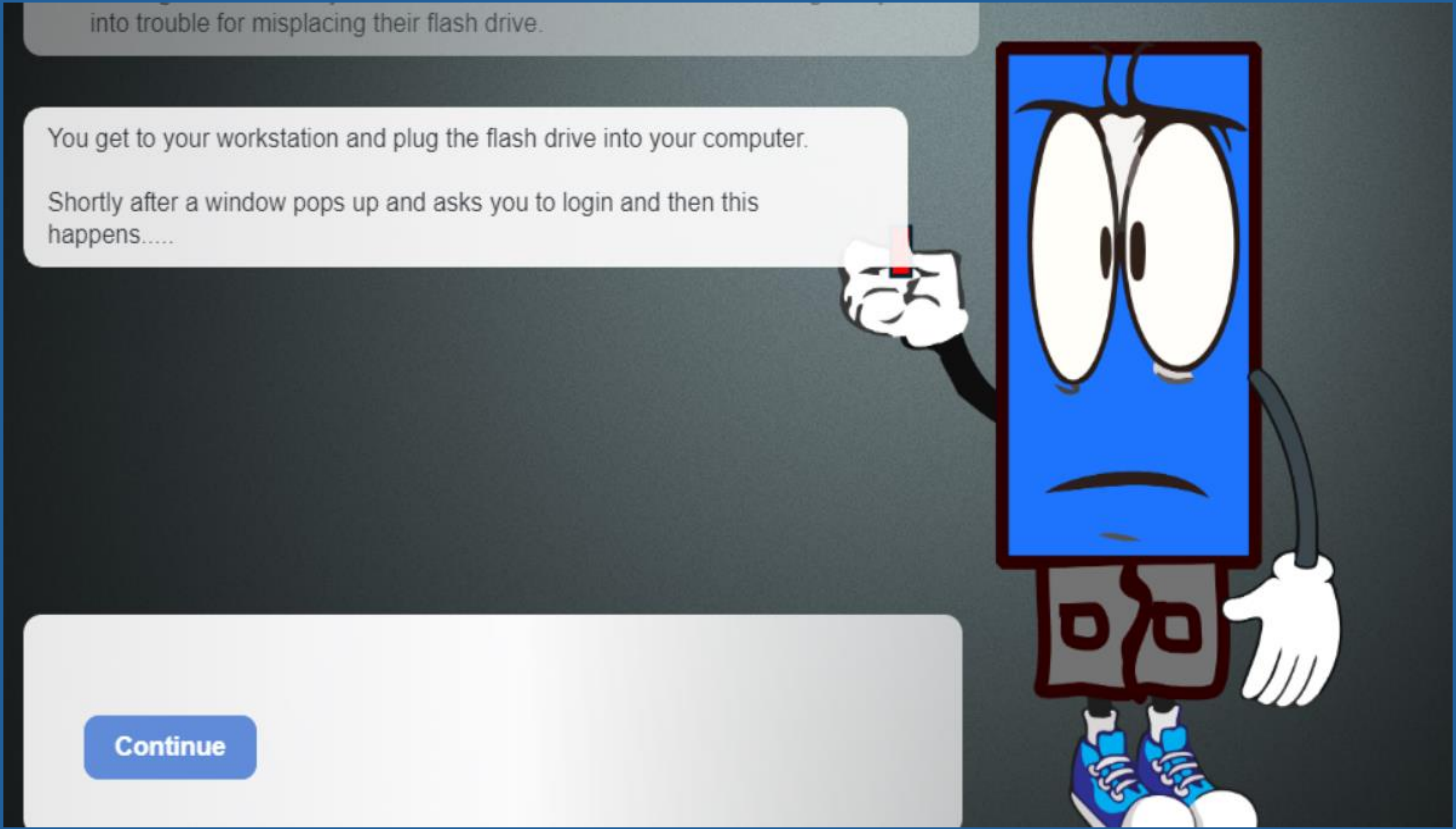
You receive an email from Control, the Cyber Security Manger. The email asks everyone to be on the lookout for a flash drive that is missing.

You notice a flash drive on the floor. Control is not in their office to return it to. You decide to do the following.

[✓ 1 You take the flash drive to your workstation and plug it in to find out if it is Jump's missing flash drive so you can return it to them. You do not want to get anyone into trouble for misplacing their flash drive.]

2 You email Control, the Cyber Security Manager, and let them know you have found a flash drive. You explain that you are not sure if it is the missing flash drive.

3 You decide to hand it in to reception since you do not know if it is the missing flash drive.



into trouble for misplacing their flash drive.

You get to your workstation and plug the flash drive into your computer.

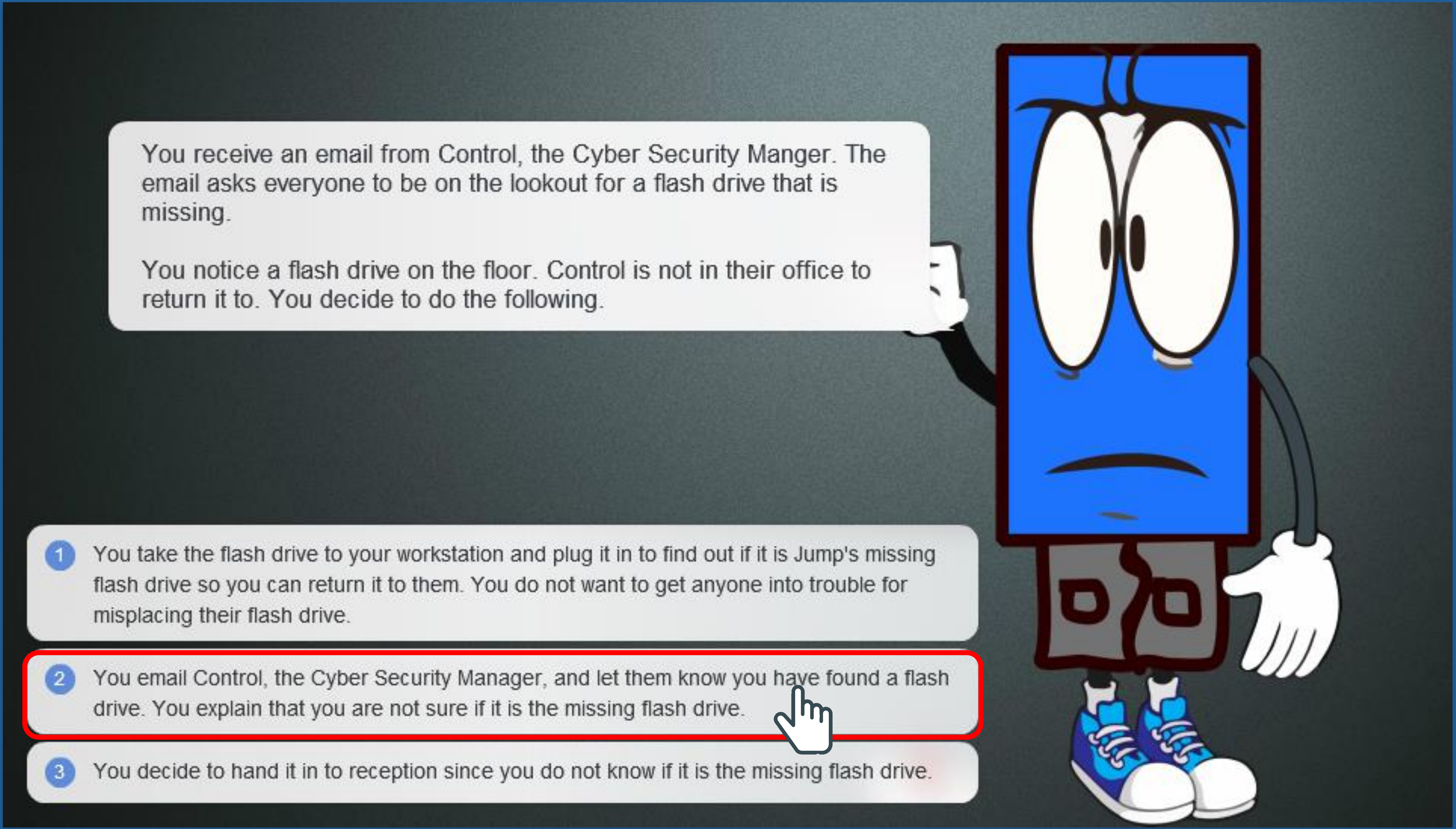
Shortly after a window pops up and asks you to login and then this happens.....

You have 10:00 minutes left

Pay $$$ or we will infect your system.

(This is a simulation and will not infect your system.)

Back Continue



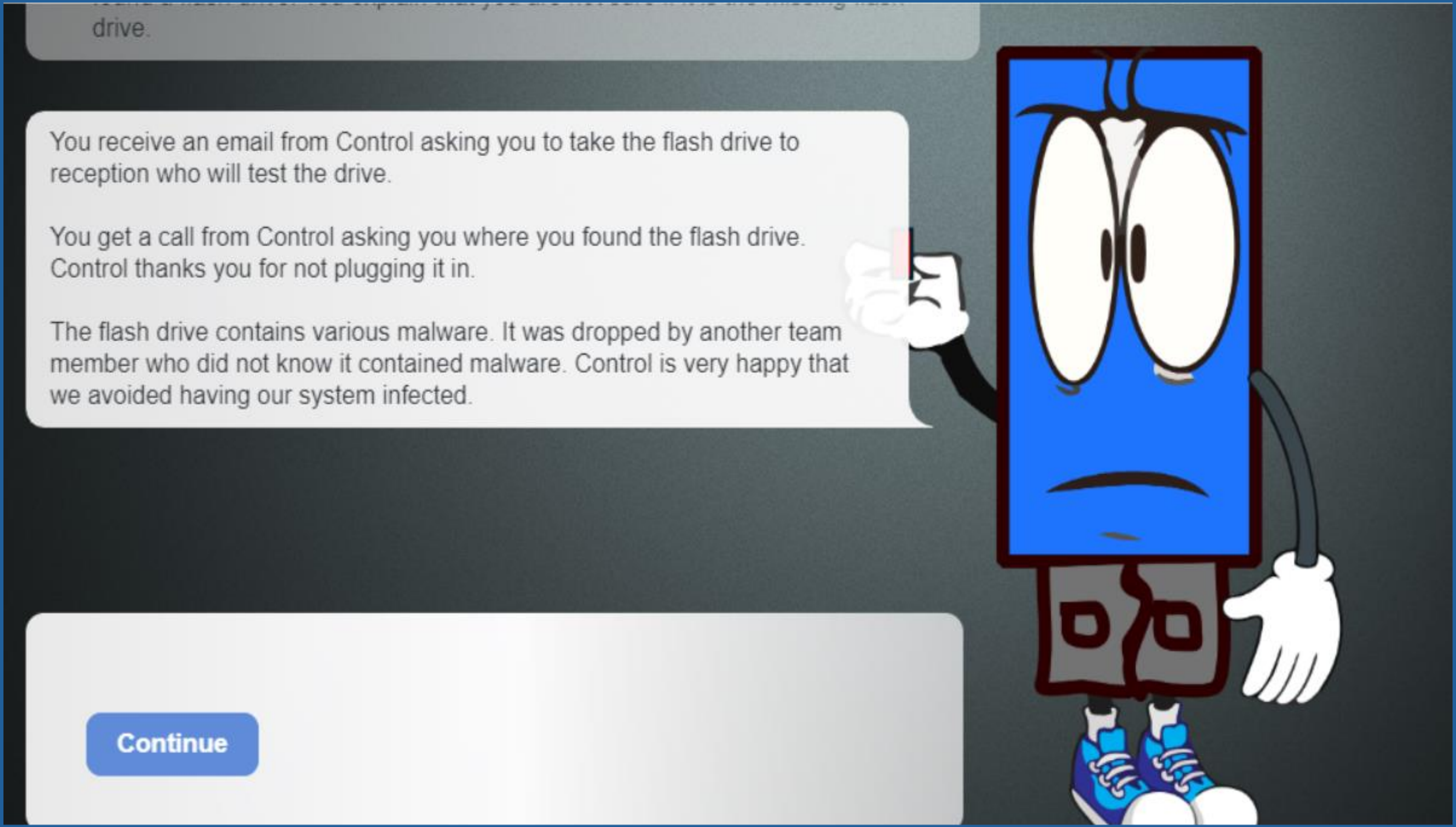
You receive an email from Control, the Cyber Security Manger. The email asks everyone to be on the lookout for a flash drive that is missing.

You notice a flash drive on the floor. Control is not in their office to return it to. You decide to do the following.

1 You take the flash drive to your workstation and plug it in to find out if it is Jump's missing flash drive so you can return it to them. You do not want to get anyone into trouble for misplacing their flash drive.

[✓ 2 You email Control, the Cyber Security Manager, and let them know you have found a flash drive. You explain that you are not sure if it is the missing flash drive.]

3 You decide to hand it in to reception since you do not know if it is the missing flash drive.

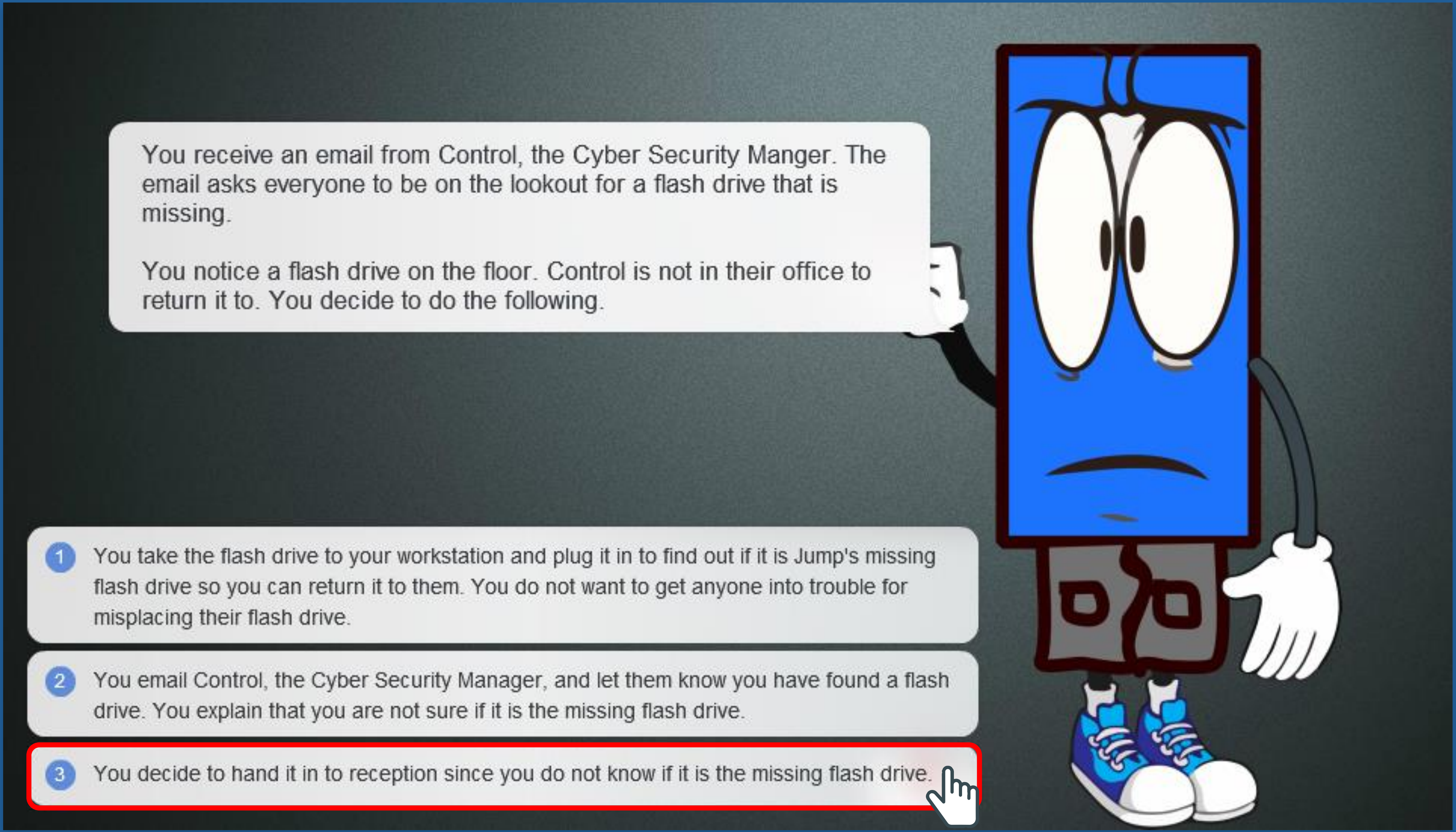


drive.

You receive an email from Control asking you to take the flash drive to reception who will test the drive.

You get a call from Control asking you where you found the flash drive. Control thanks you for not plugging it in.

The flash drive contains various malware. It was dropped by another team member who did not know it contained malware. Control is very happy that we avoided having our system infected.



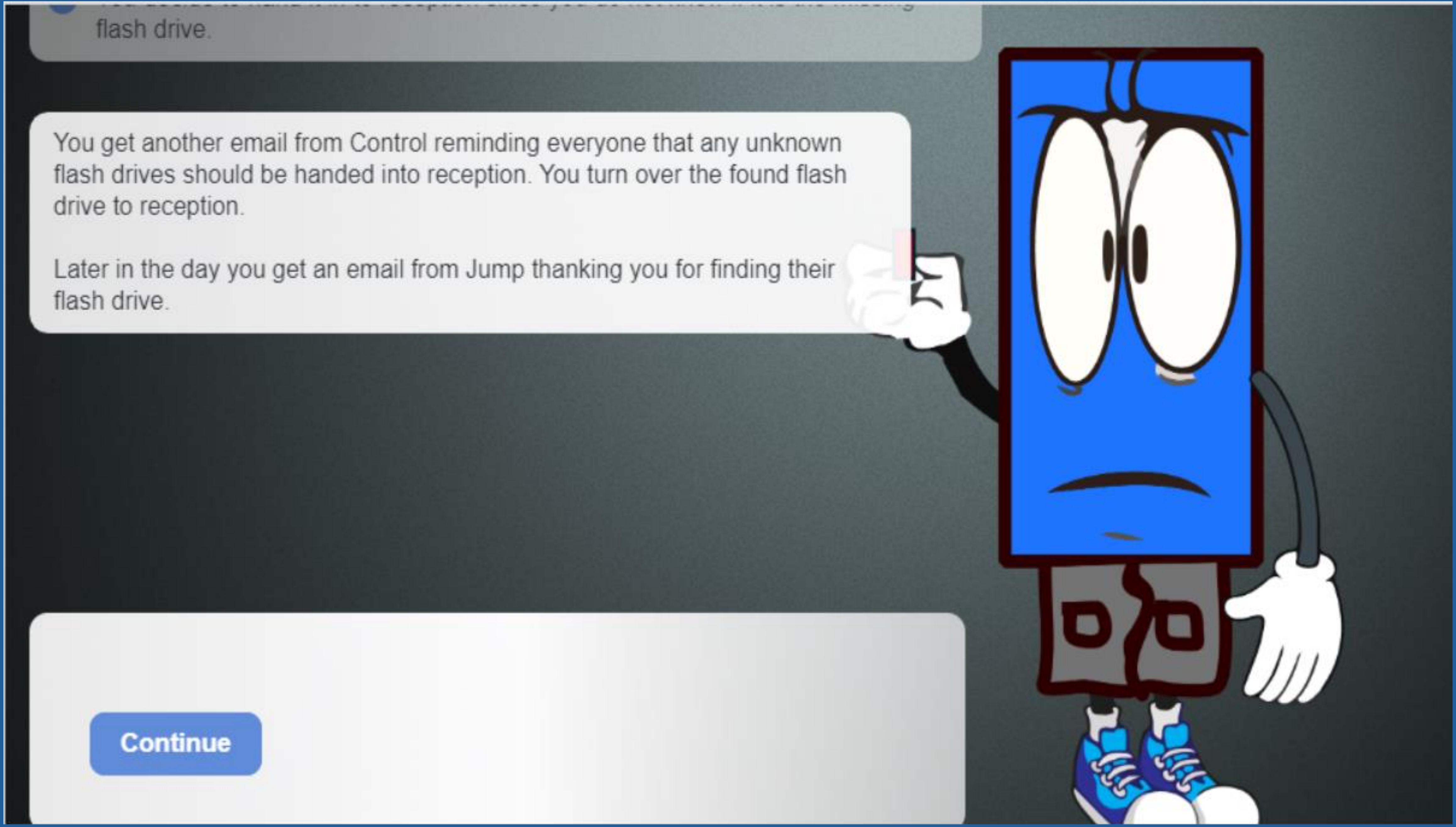
You receive an email from Control, the Cyber Security Manger. The email asks everyone to be on the lookout for a flash drive that is missing.

You notice a flash drive on the floor. Control is not in their office to return it to. You decide to do the following.

1 You take the flash drive to your workstation and plug it in to find out if it is Jump's missing flash drive so you can return it to them. You do not want to get anyone into trouble for misplacing their flash drive.

2 You email Control, the Cyber Security Manager, and let them know you have found a flash drive. You explain that you are not sure if it is the missing flash drive.

[✓ 3 You decide to hand it in to reception since you do not know if it is the missing flash drive.]



flash drive.

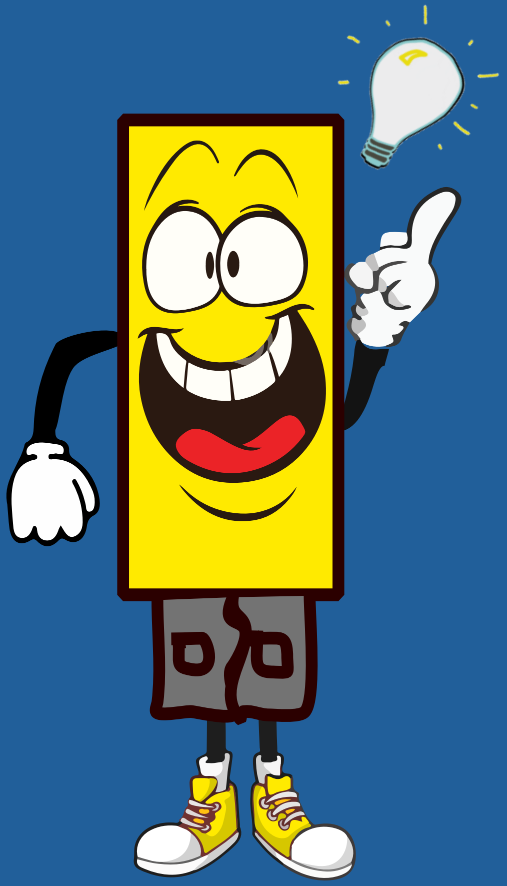
You get another email from Control reminding everyone that any unknown flash drives should be handed into reception. You turn over the found flash drive to reception.

Later in the day you get an email from Jump thanking you for finding their flash drive.

Remember

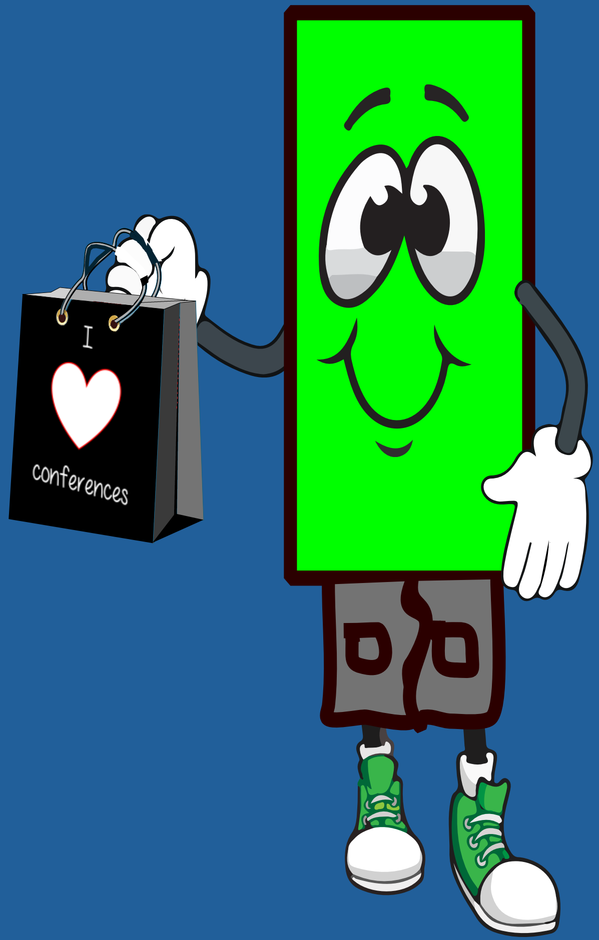
If you lose a flash drive, you must immediately report it to the Cyber Security Manager. They will try to help you recover the flash drive and assess if there has been a data breach.

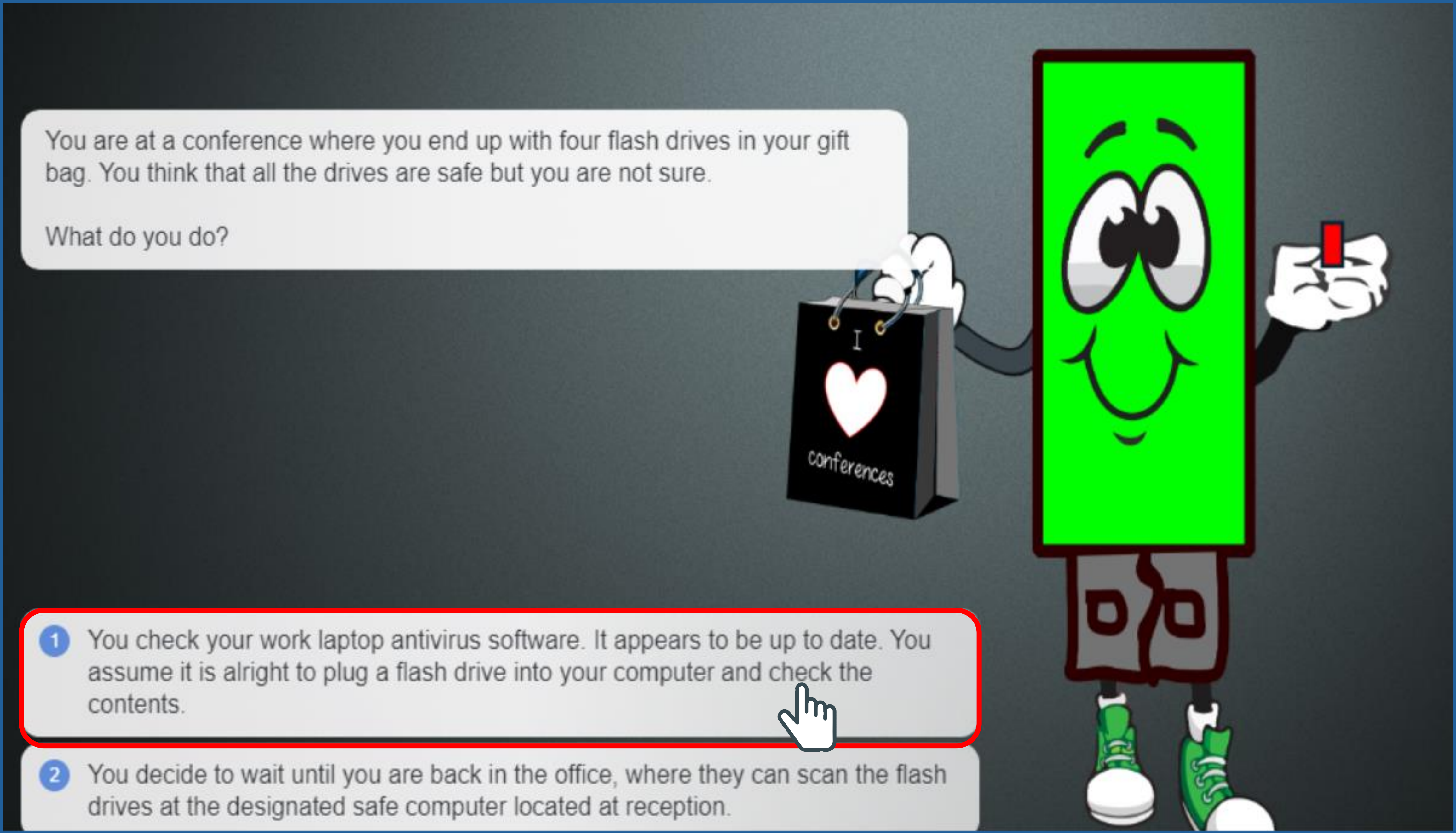
If you find a flash drive, you must hand it in to reception. Reception has a special computer that can safely check flash drives.



Gifted and personal flash drives

In this section, we will explore situations where you are given a flash drive from an outside source or if you use a personal flash drive on a network computer.



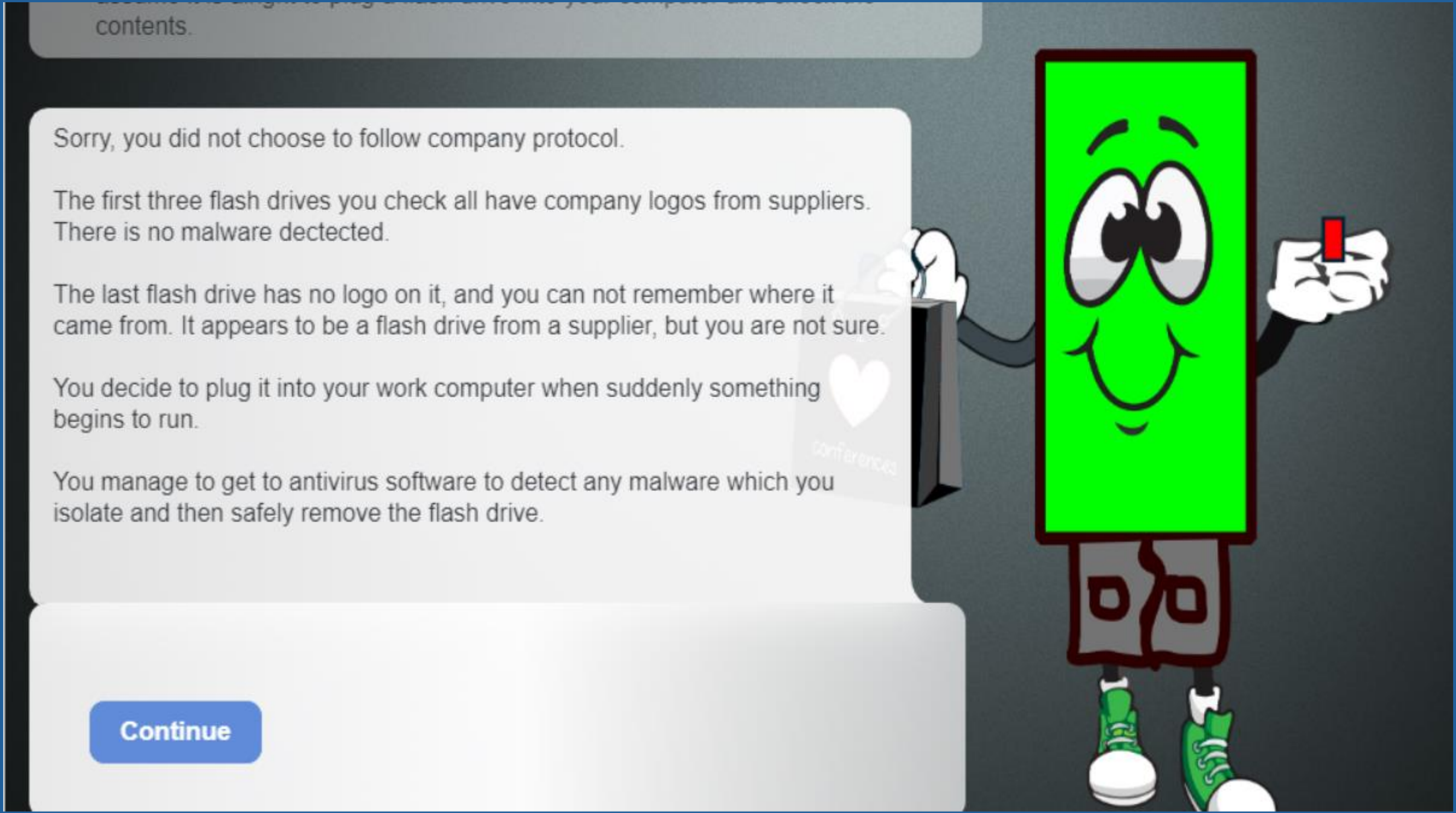


You are at a conference where you end up with four flash drives in your gift bag. You think that all the drives are safe but you are not sure.

What do you do?

[✓ 1 You check your work laptop antivirus software. It appears to be up to date. You assume it is alright to plug a flash drive into your computer and check the contents.]

2 You decide to wait until you are back in the office, where they can scan the flash drives at the designated safe computer located at reception.



contents.

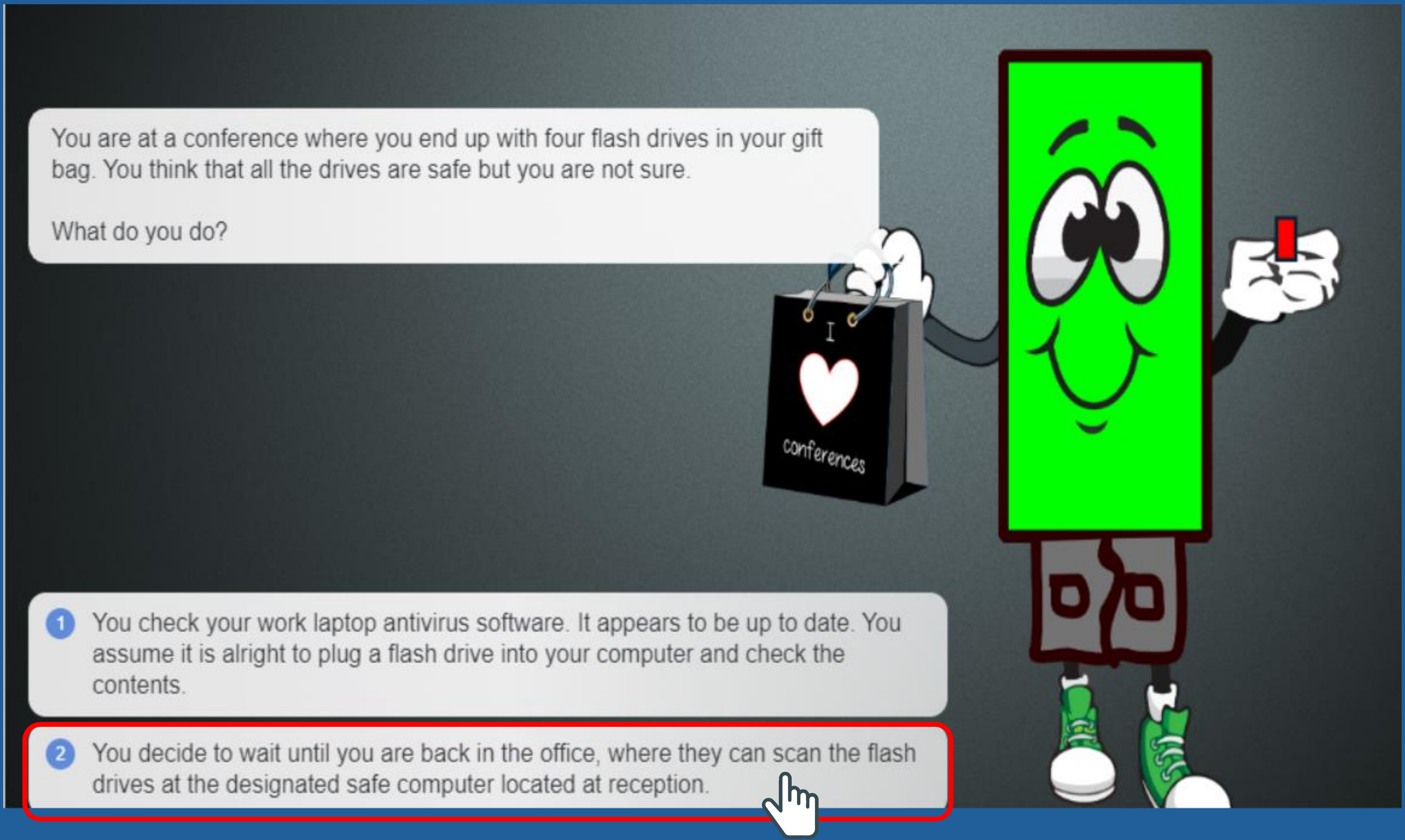
Sorry, you did not choose to follow company protocol.

The first three flash drives you check all have company logos from suppliers. There is no malware dectected.

The last flash drive has no logo on it, and you can not remember where it came from. It appears to be a flash drive from a supplier, but you are not sure.

You decide to plug it into your work computer when suddenly something begins to run.

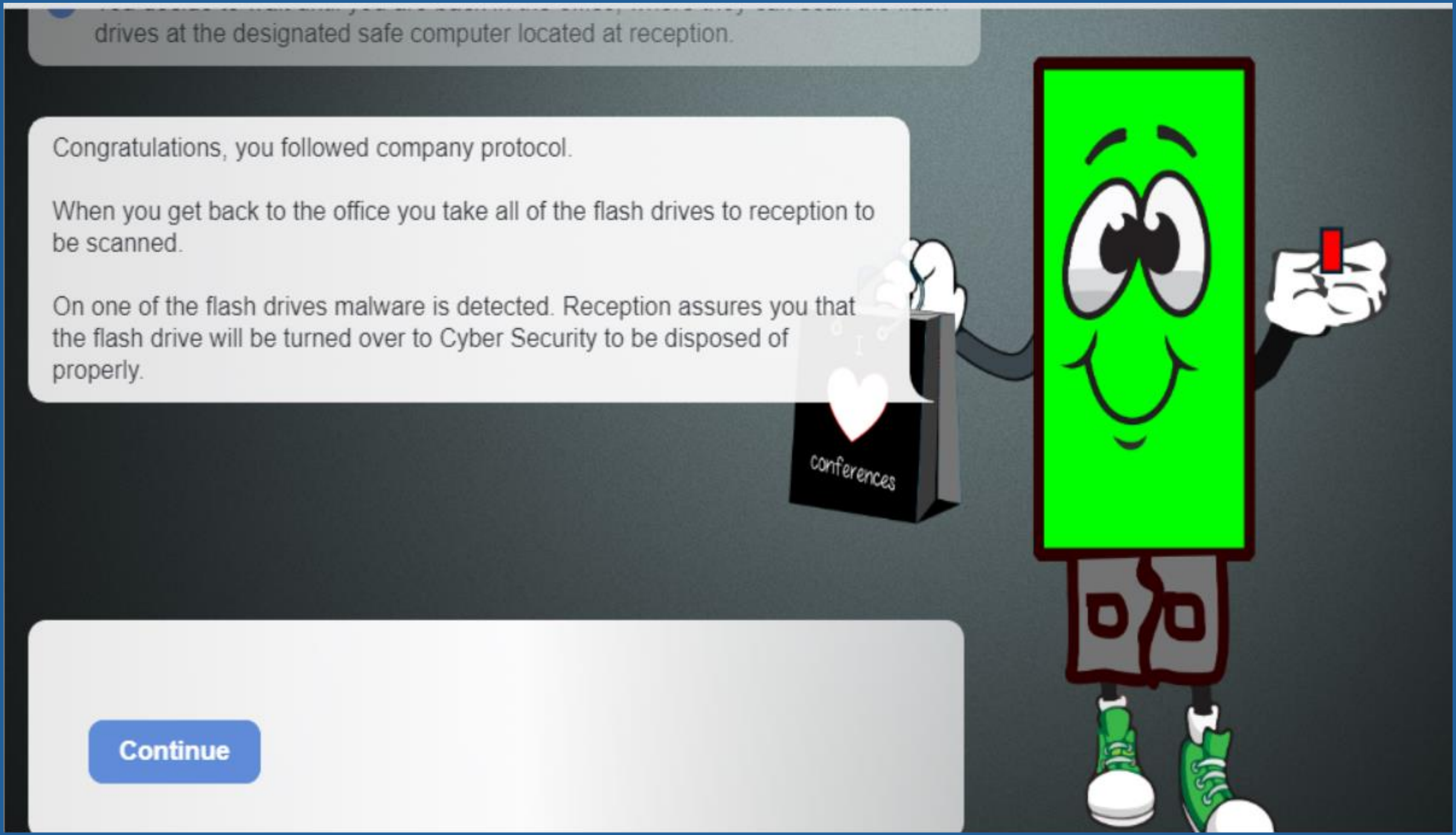
You manage to get to antivirus software to detect any malware which you isolate and then safely remove the flash drive.



You are at a conference where you end up with four flash drives in your gift bag. You think that all the drives are safe but you are not sure.

What do you do?

1. You check your work laptop antivirus software. It appears to be up to date. You assume it is alright to plug a flash drive into your computer and check the contents.
2. You decide to wait until you are back in the office, where they can scan the flash drives at the designated safe computer located at reception.

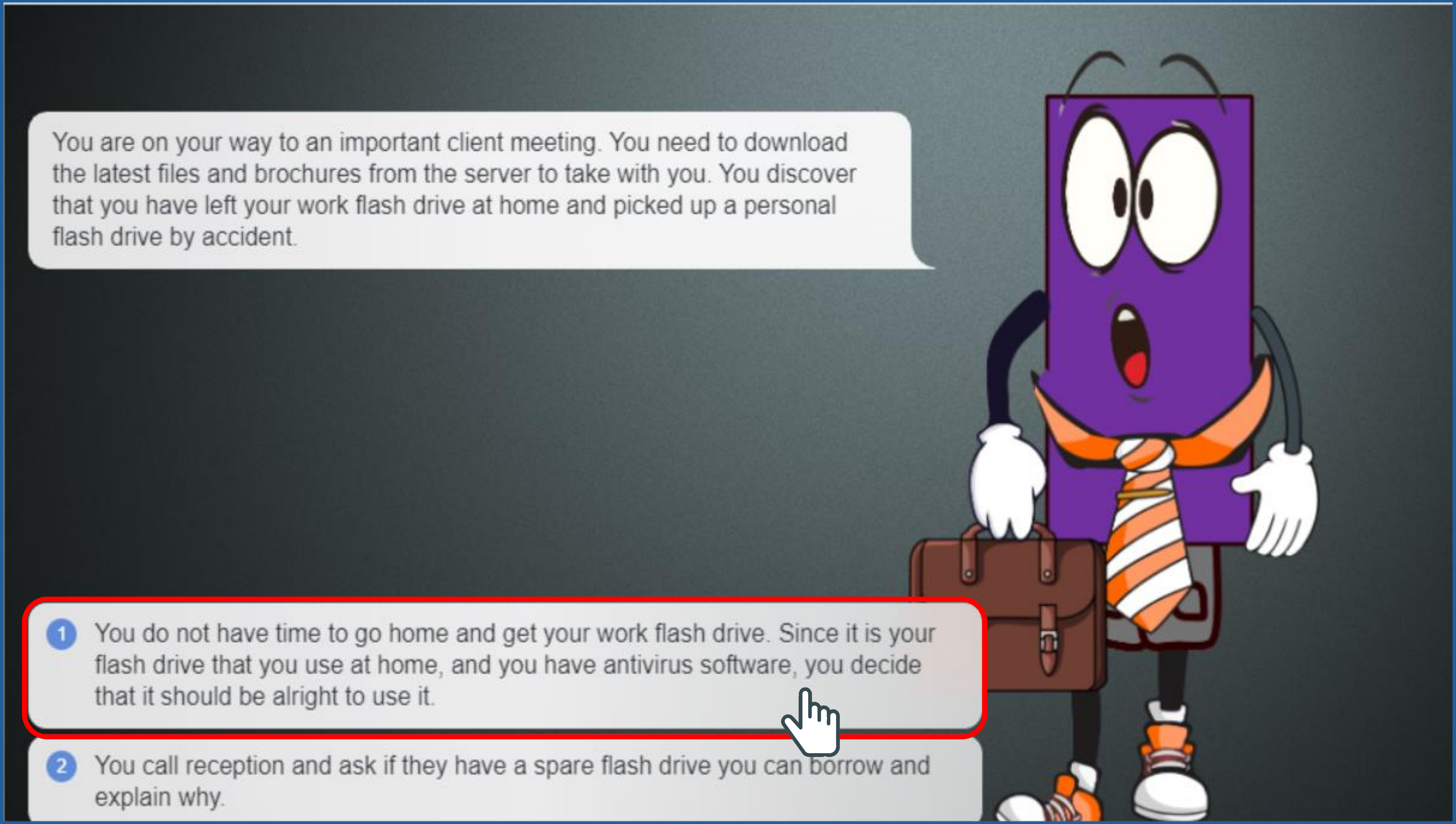


drives at the designated safe computer located at reception.

Congratulations, you followed company protocol.

When you get back to the office you take all of the flash drives to reception to be scanned.

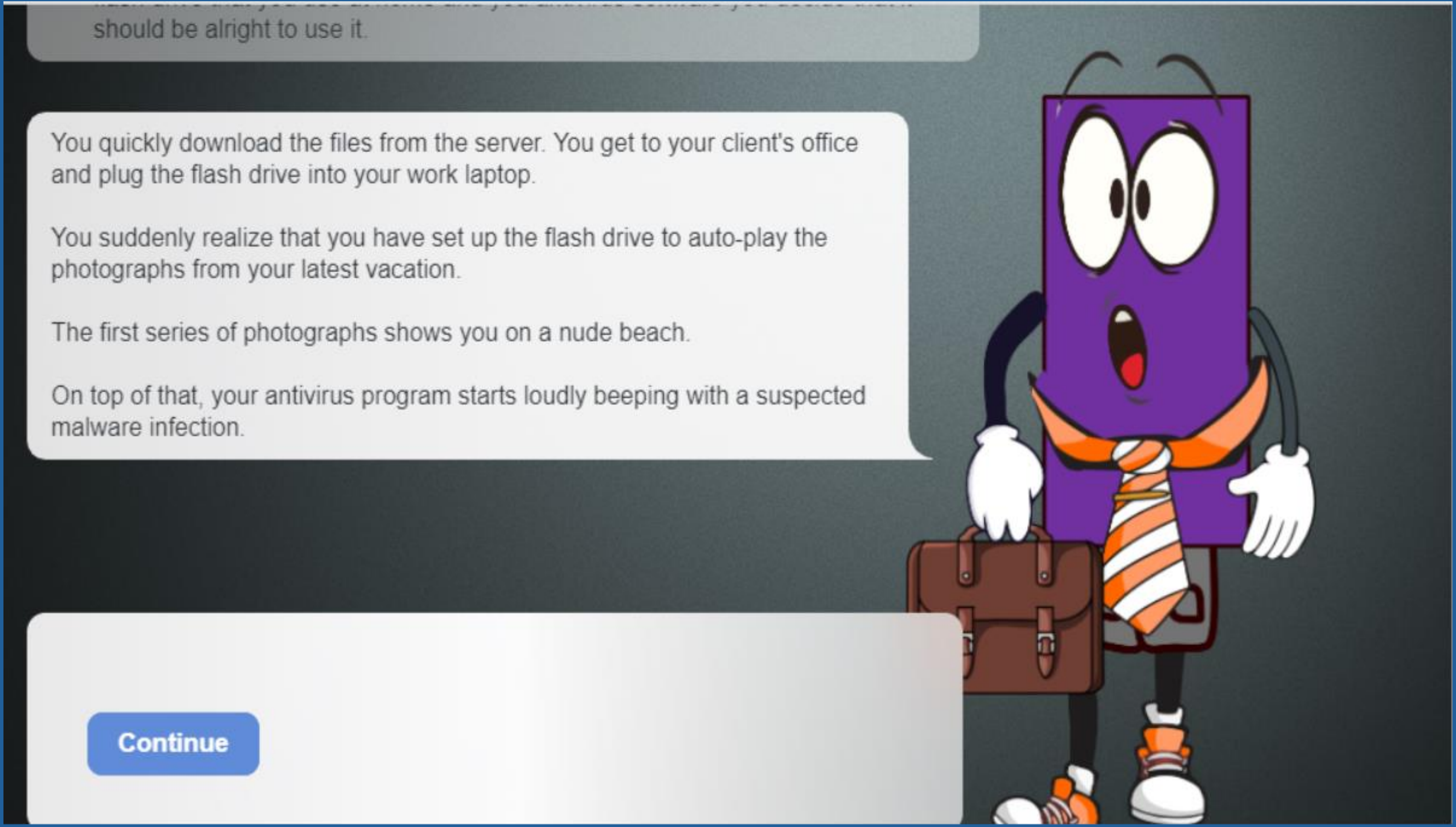
On one of the flash drives malware is detected. Reception assures you that the flash drive will be turned over to Cyber Security to be disposed of properly.



You are on your way to an important client meeting. You need to download the latest files and brochures from the server to take with you. You discover that you have left your work flash drive at home and picked up a personal flash drive by accident.

[✓ 1 You do not have time to go home and get your work flash drive. Since it is your flash drive that you use at home, and you have antivirus software, you decide that it should be alright to use it.]

2 You call reception and ask if they have a spare flash drive you can borrow and explain why.



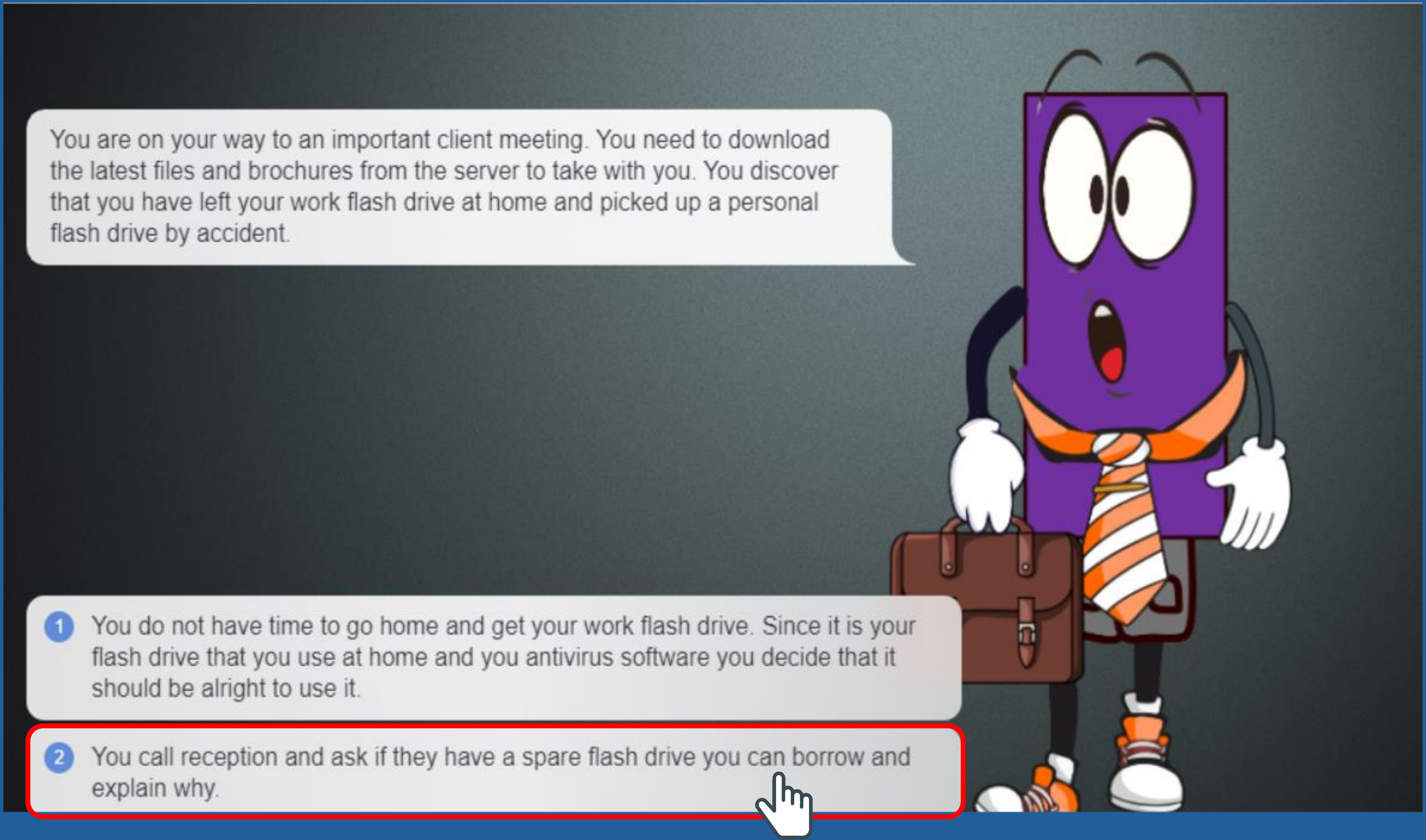
should be alright to use it.

You quickly download the files from the server. You get to your client's office and plug the flash drive into your work laptop.

You suddenly realize that you have set up the flash drive to auto-play the photographs from your latest vacation.

The first series of photographs shows you on a nude beach.

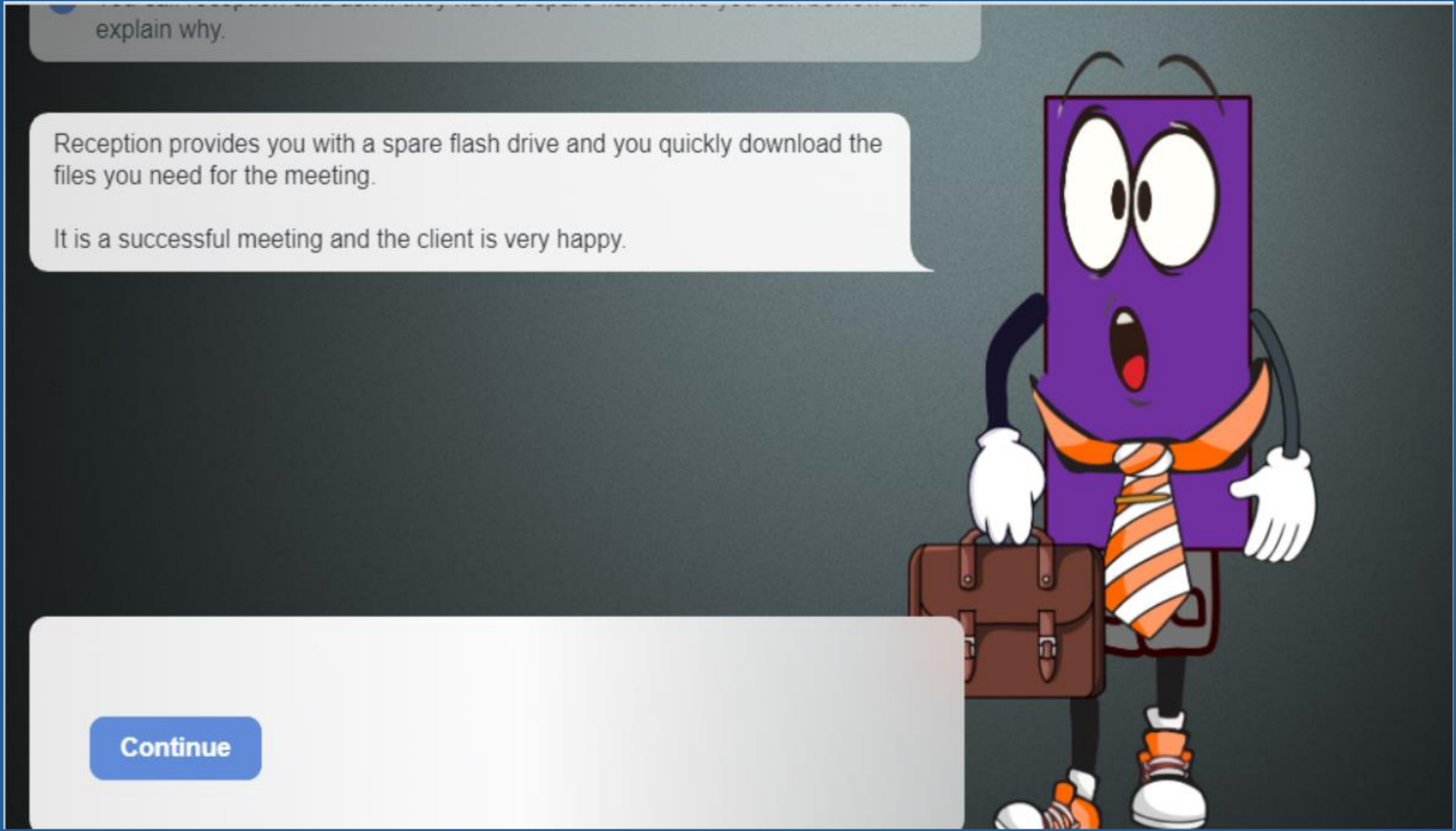
On top of that, your antivirus program starts loudly beeping with a suspected malware infection.



You are on your way to an important client meeting. You need to download the latest files and brochures from the server to take with you. You discover that you have left your work flash drive at home and picked up a personal flash drive by accident.

1. You do not have time to go home and get your work flash drive. Since it is your flash drive that you use at home and you antivirus software you decide that it should be alright to use it.

2. You call reception and ask if they have a spare flash drive you can borrow and explain why.

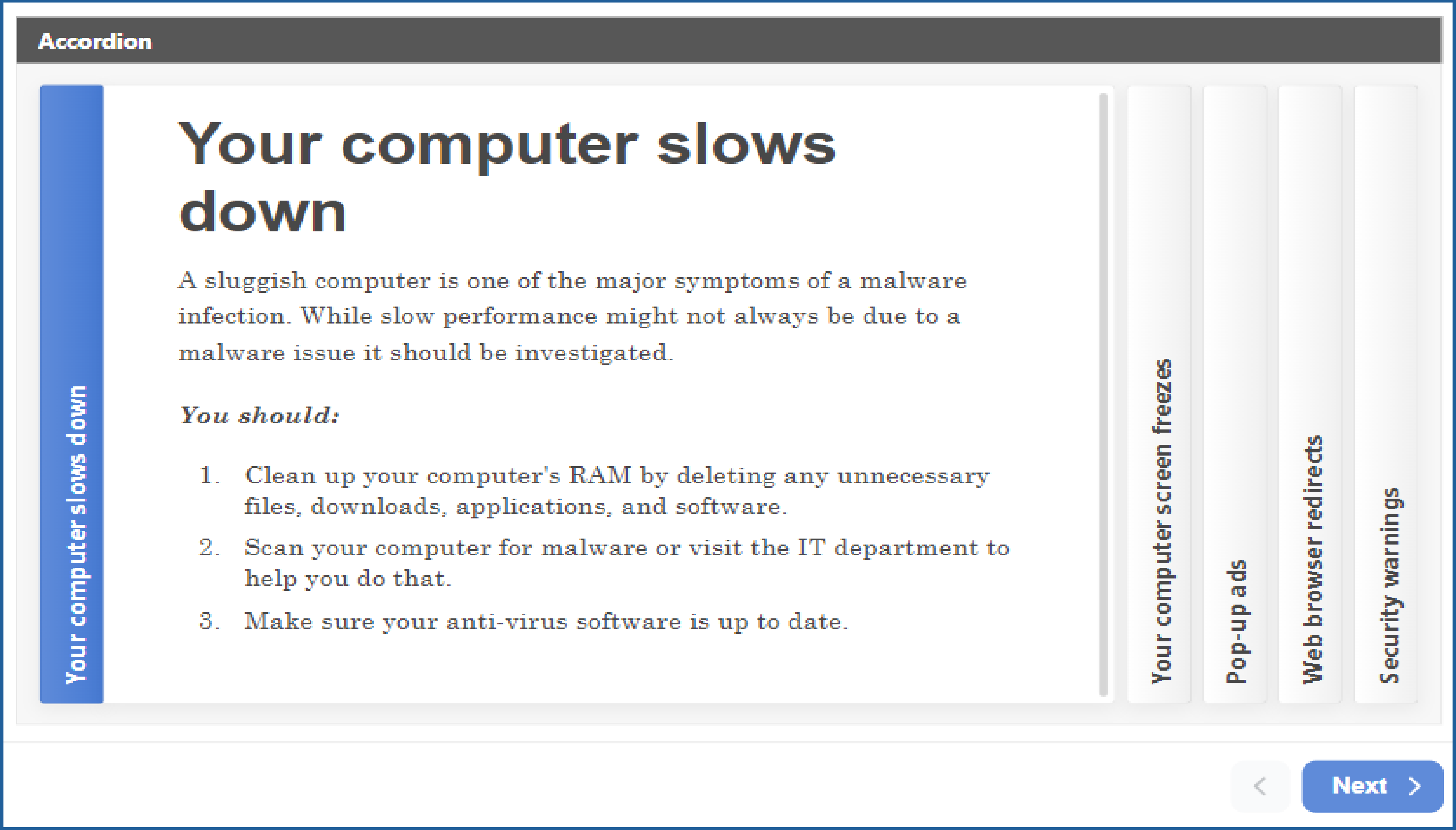


explain why.

Reception provides you with a spare flash drive and you quickly download the files you need for the meeting.

It is a successful meeting and the client is very happy.

How to recognize the signs that you might be infected.

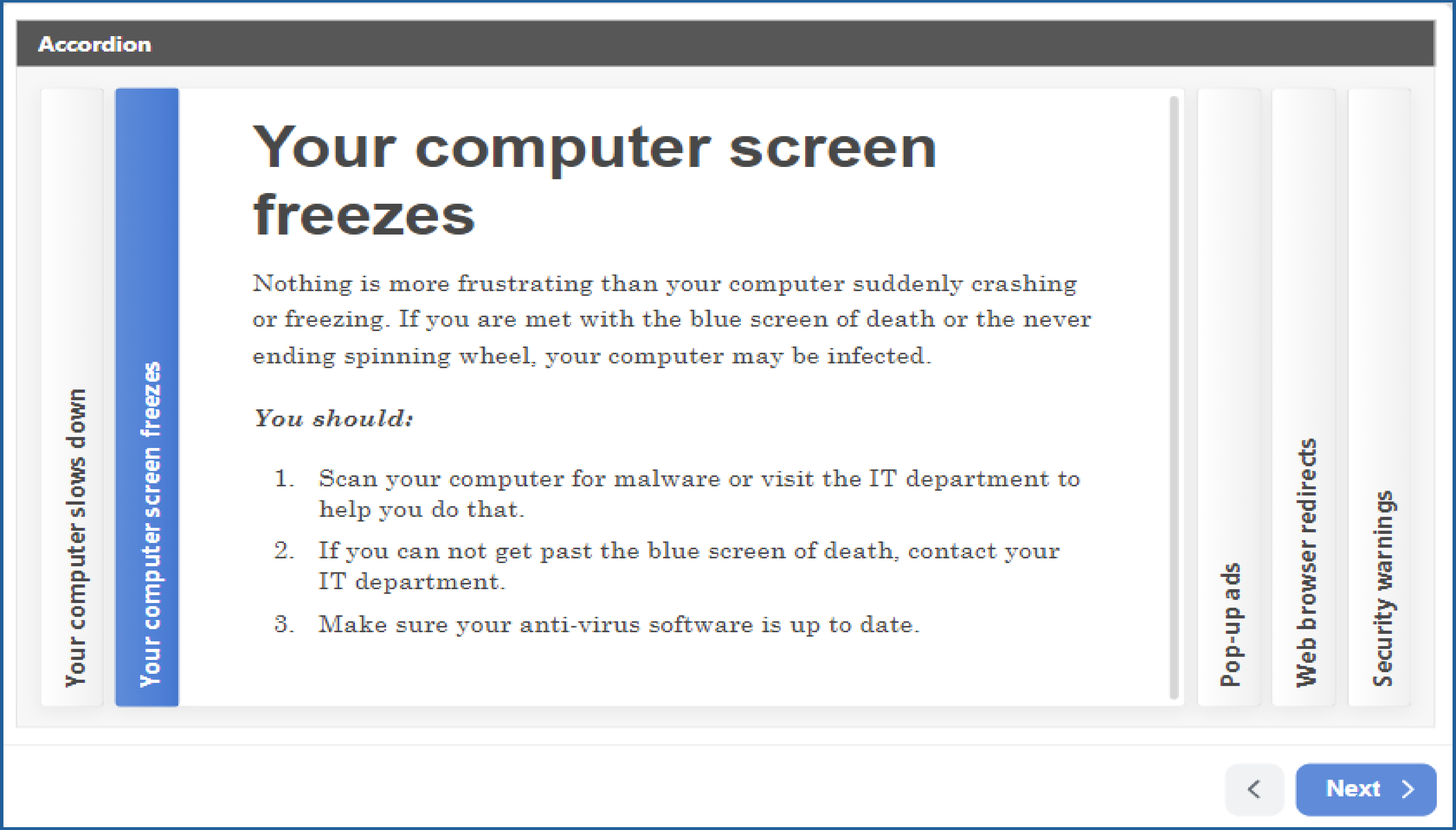


Your computer slows down

A sluggish computer is one of the major symptoms of a malware infection. While slow performance might not always be due to a malware issue it should be investigated.

You should:

1. Clean up your computer's RAM by deleting any unnecessary files, downloads, applications, and software.
2. Scan your computer for malware or visit the IT department to help you do that.
3. Make sure your anti-virus software is up to date.

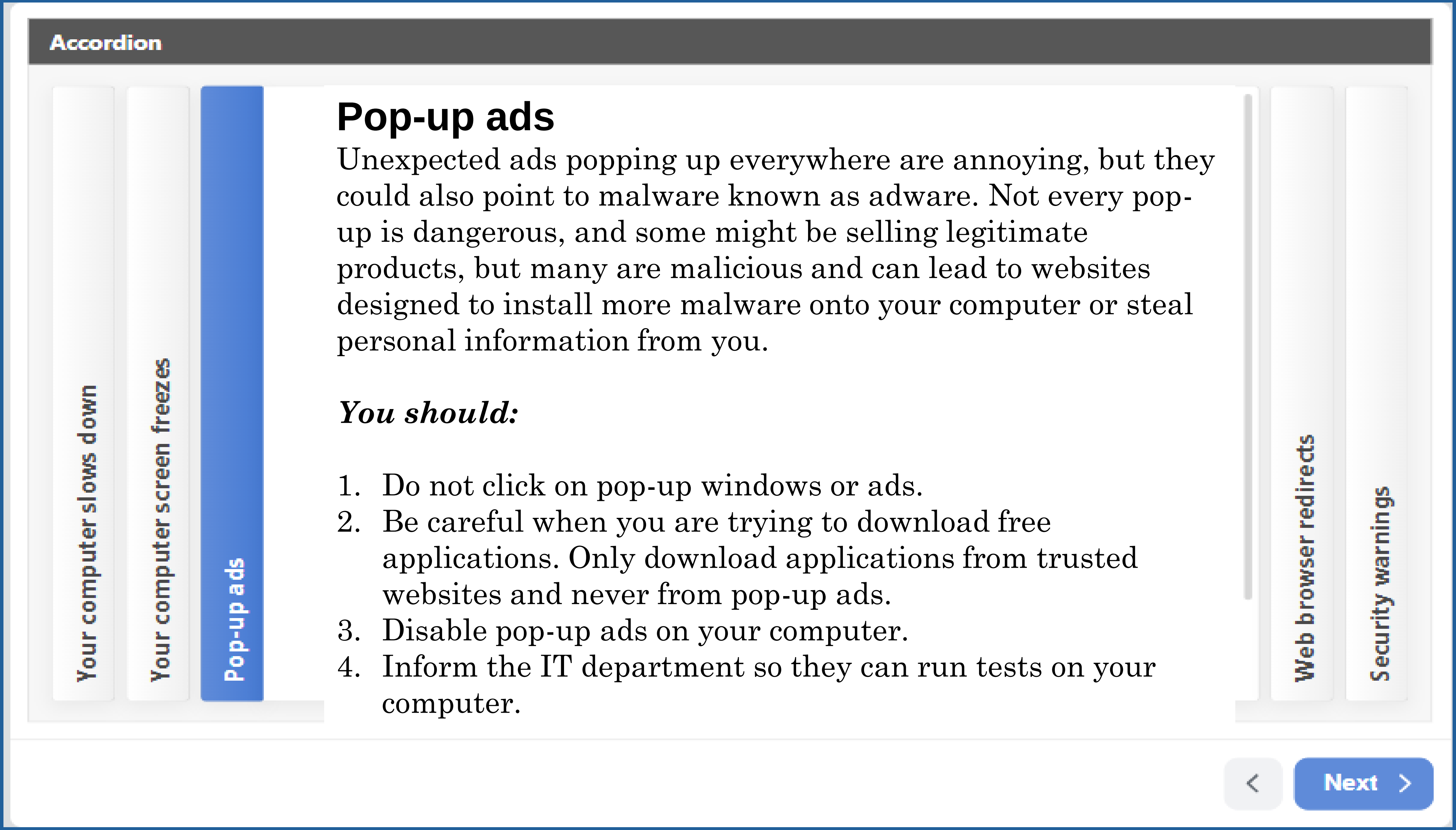


Your computer screen freezes

Nothing is more frustrating than your computer suddenly crashing or freezing. If you are met with the blue screen of death or the never ending spinning wheel, your computer may be infected.

You should:

1. Scan your computer for malware or visit the IT department to help you do that.
2. If you can not get past the blue screen of death, contact your IT department.
3. Make sure your anti-virus software is up to date.

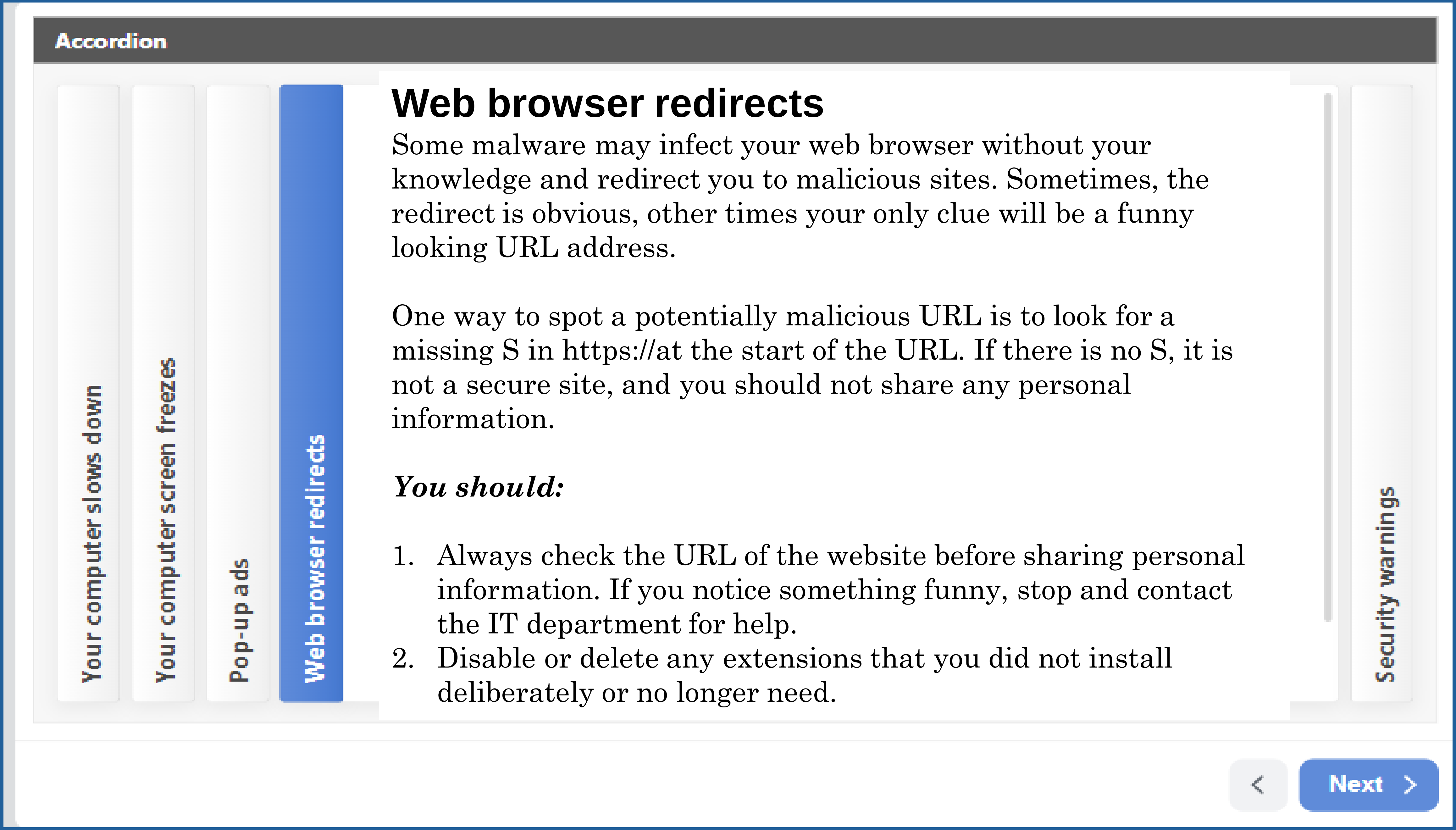


Pop-up ads

Unexpected ads popping up everywhere are annoying, but they could also point to malware known as adware. Not every pop-up is dangerous, and some might be selling legitimate products, but many are malicious and can lead to websites designed to install more malware onto your computer or steal personal information from you.

You should:

1. Do not click on pop-up windows or ads.
2. Be careful when you are trying to download free applications. Only download applications from trusted websites and never from pop-up ads.
3. Disable pop-up ads on your computer.
4. Inform the IT department so they can run tests on your computer.



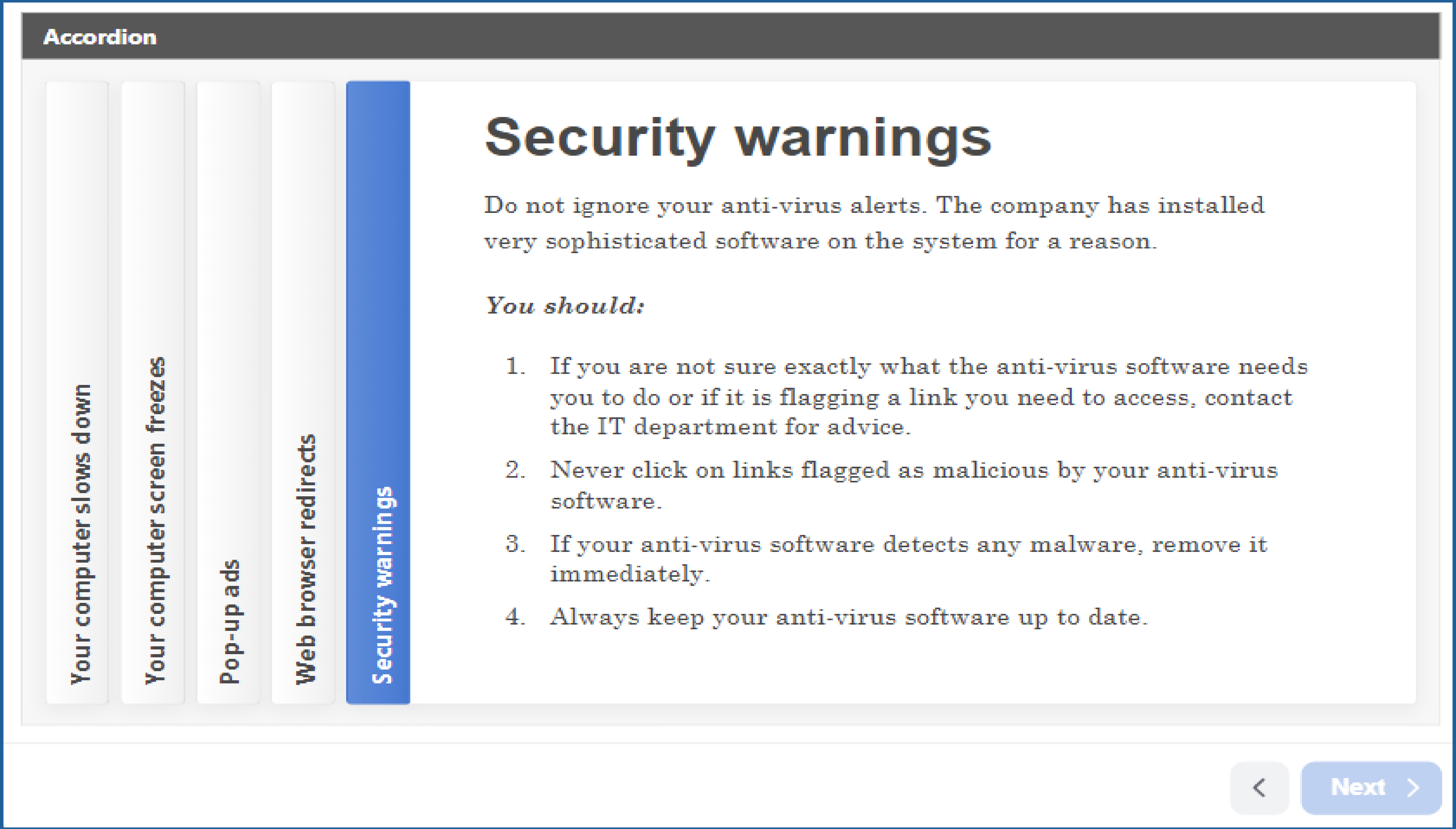
Web browser redirects

Some malware may infect your web browser without your knowledge and redirect you to malicious sites. Sometimes, the redirect is obvious, other times your only clue will be a funny looking URL address.

One way to spot a potentially malicious URL is to look for a missing S in https://at the start of the URL. If there is no S, it is not a secure site, and you should not share any personal information.

You should:

1. Always check the URL of the website before sharing personal information. If you notice something funny, stop and contact the IT department for help.
2. Disable or delete any extensions that you did not install deliberately or no longer need.



Security warnings

Do not ignore your anti-virus alerts. The company has installed very sophisticated software on the system for a reason.

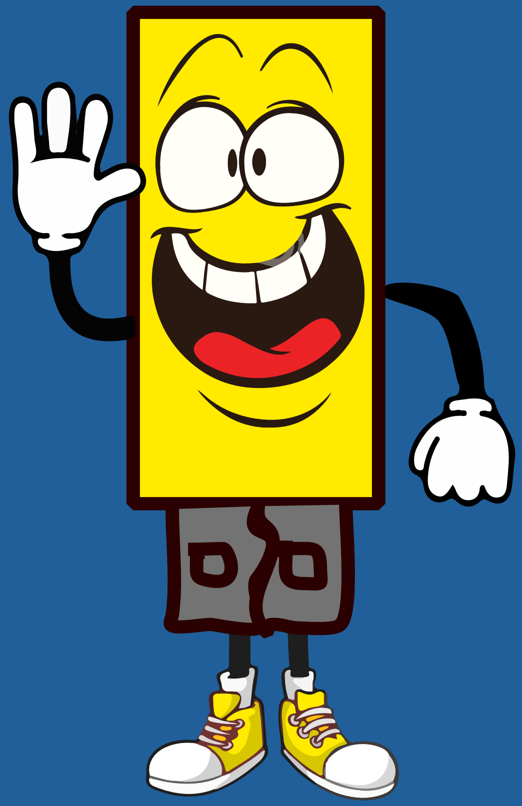
You should:

1. If you are not sure exactly what the anti-virus software needs you to do or if it is flagging a link you need to access, contact the IT department for advice.
2. Never click on links flagged as malicious by your anti-virus software.
3. If your anti-virus software detects any malware, remove it immediately.
4. Always keep your anti-virus software up to date.

Additional safe practices

- Only use company issued flash drives.
- Never lend your flash drive to anyone.
- Always encrypt sensitive data to keep it safe.
- Keep your anti-virus software up to date. If you are unsure about updates check with the cyber security department.

Thank you for joining me today. I hope your enjoyed learning about flash drive safety. If you have any additional questions, please contact your IT department. They are always ready to help.



Back Exit