🟦 #004883

🟦 #2FB5E8

⬜ #FFFFFF

🟦 #ABD8F3

🟥 #C00000

DKA Corporation

DKA Corporation

Let’s Get Started

Next

Submit

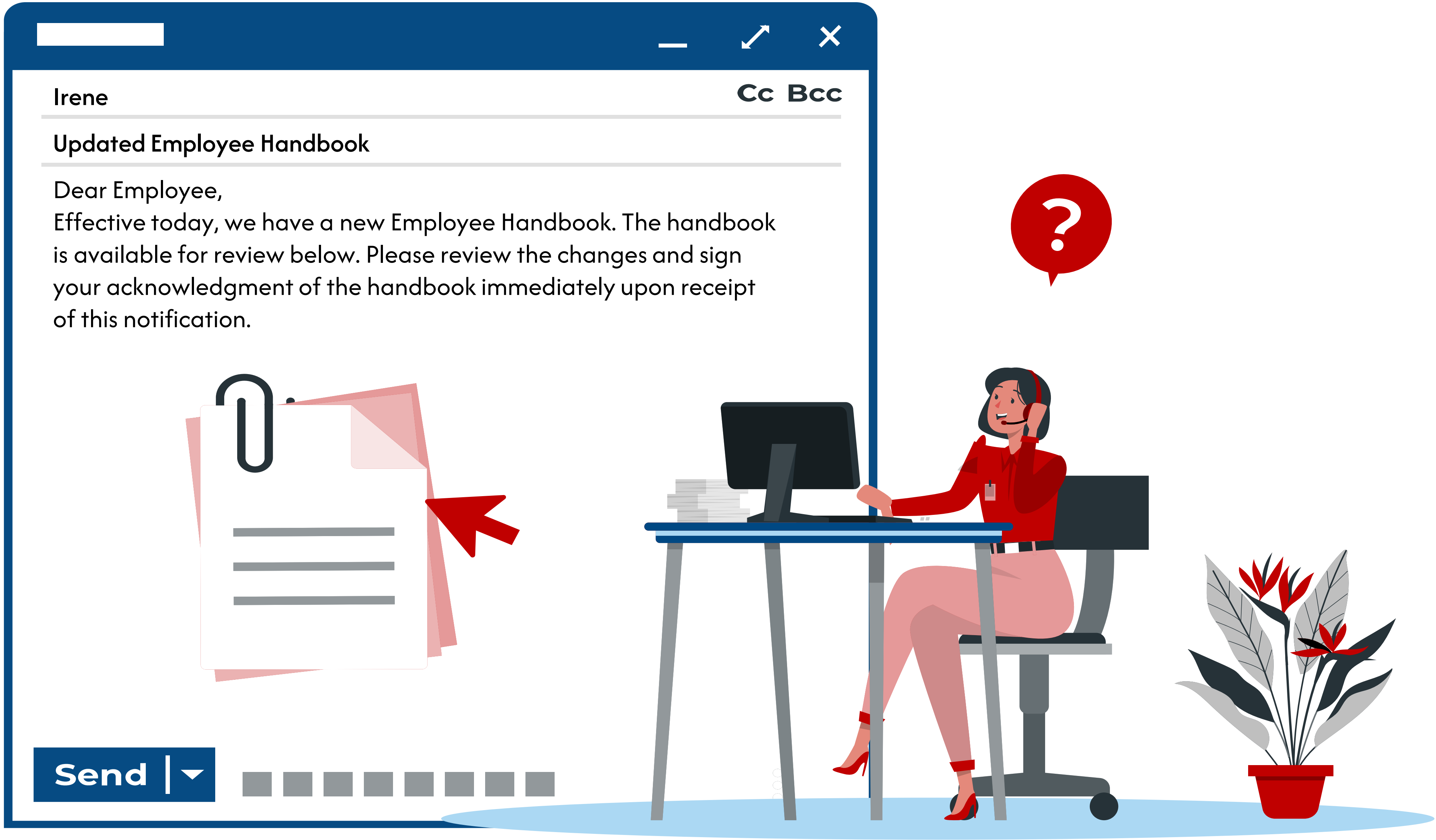
DKA Corporation

IDENTIFYING

Phishing Scams

Let's Get Started

Meet Irene



Irene

Updated Employee Handbook

Dear Employee,
Effective today, we have a new Employee Handbook. The handbook is available for review below. Please review the changes and sign your acknowledgment of the handbook immediately upon receipt of this notification.

Irene
Cc Bcc
Update
Send

In this course we're going to help Irene:

- Identify the common signs of phishing scams
- Identify when to report phishing attempts
- How to accurately report a phishing scam to the IT department

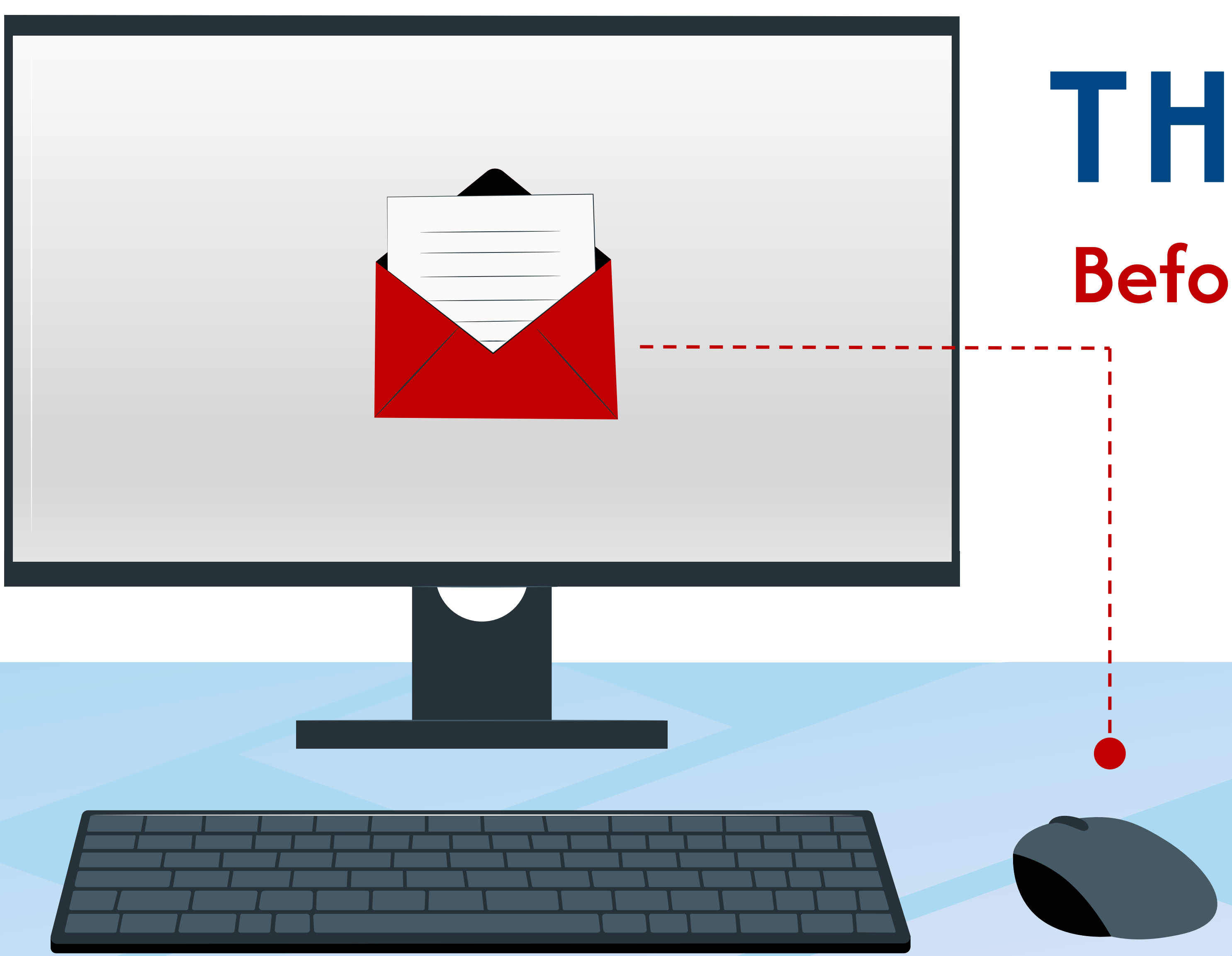
Next

What is Phishing?

Phishing is the practice of sending fraudulent communications that appear to come from a legitimate and reputable company you trust.

Phishing is a dangerous, damaging, and an increasingly common type of cyberattack. The attacker's goal is to steal money, gain access to sensitive data and login information, or to install malware on the victim's device.

Next



THINK ?

Before you Click!

Next

Personal Risks

Professional Risks

Personal phishing risks include:

- Money stolen from your bank account
- Fraudulent charges on credit cards
- Lost access to photos, videos, and files
- Fake social media posts made in your accounts, putting friends or family members at risk

Next

Personal Risks

Professional Risks

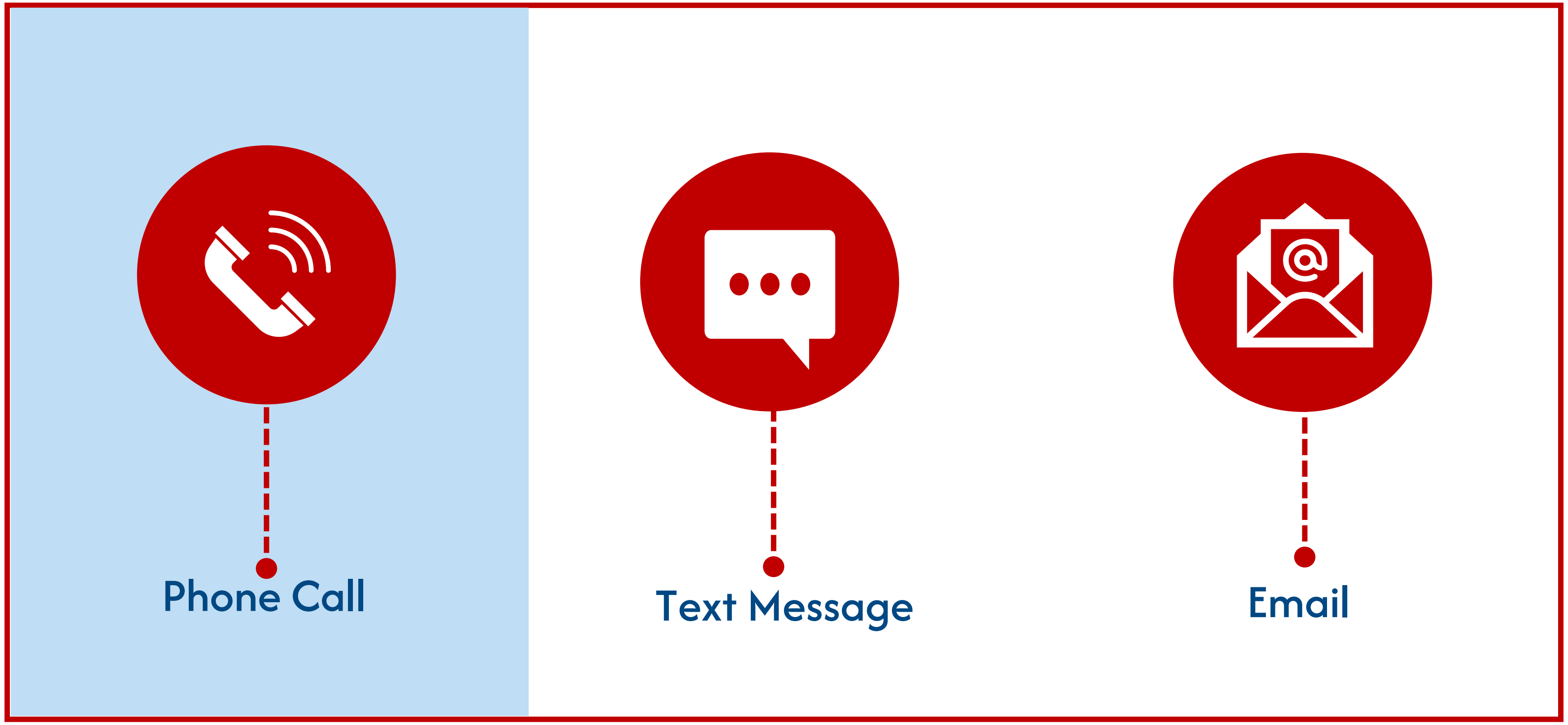
Professional phishing risks include:

- Loss of corporate funds
- Exposing information of partners, coworkers, and customers
- Files becoming locked and inaccessible
- Damage to the organization's reputation

Next

Phishing Examples

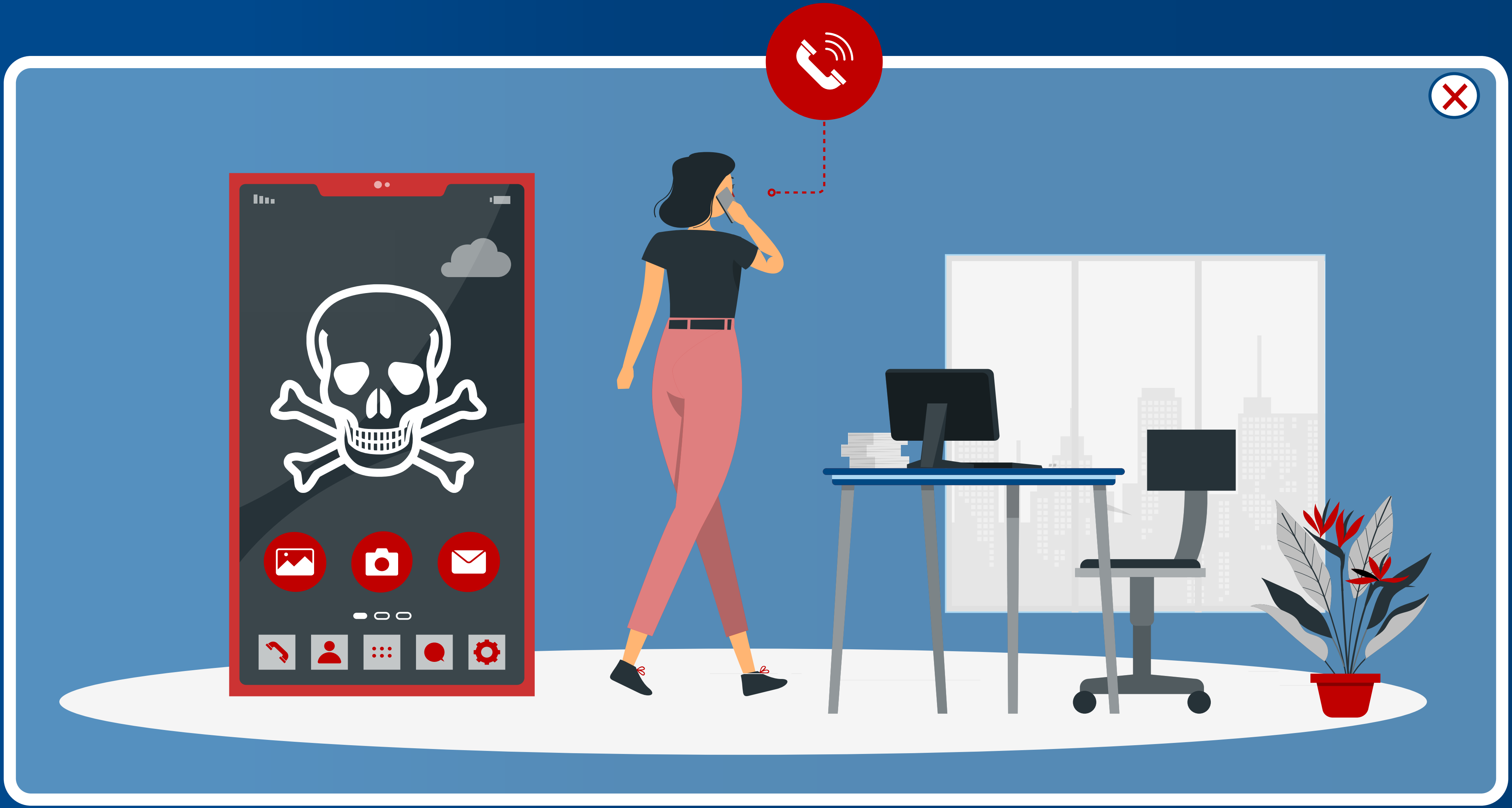
Click the Phone Call icon below to learn more.



Phone Call

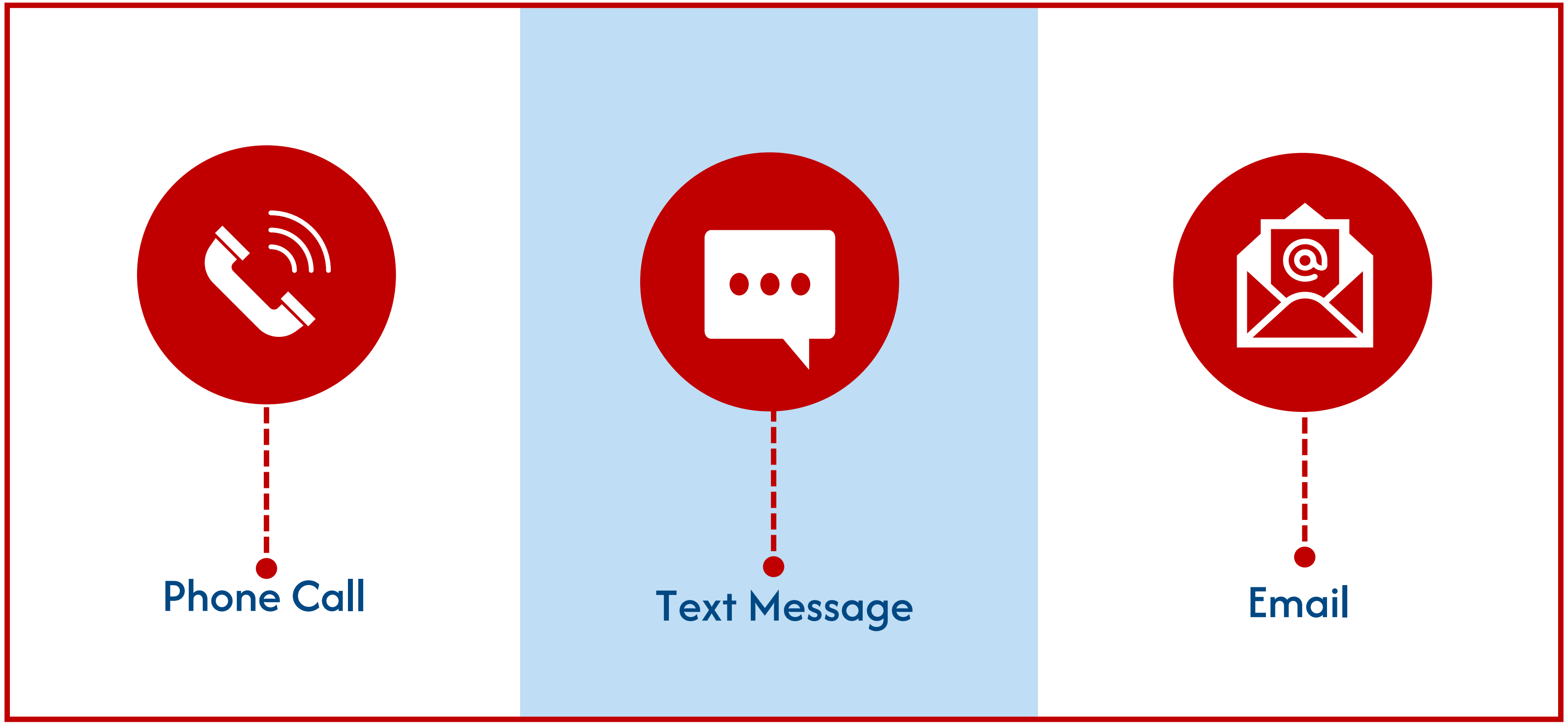
Text Message

Email



Phishing Examples

Click the Text Message icon below to learn more.



Phone Call

Text Message

Email

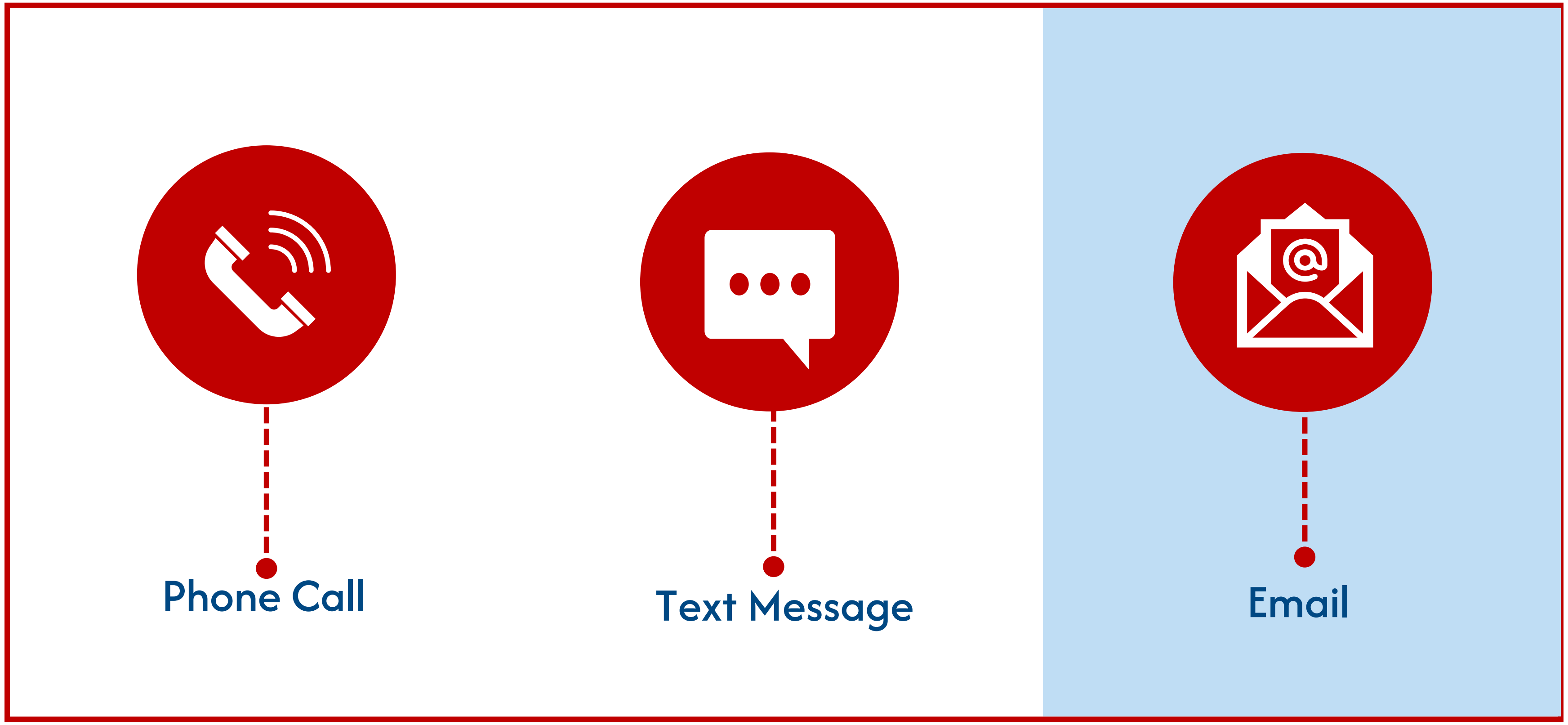
USPS: Your package is being held due to incorrect delivery information.

Click here to update your address: Link

Failure to respond in 24 hours will result in the package being returned.

Phishing Examples

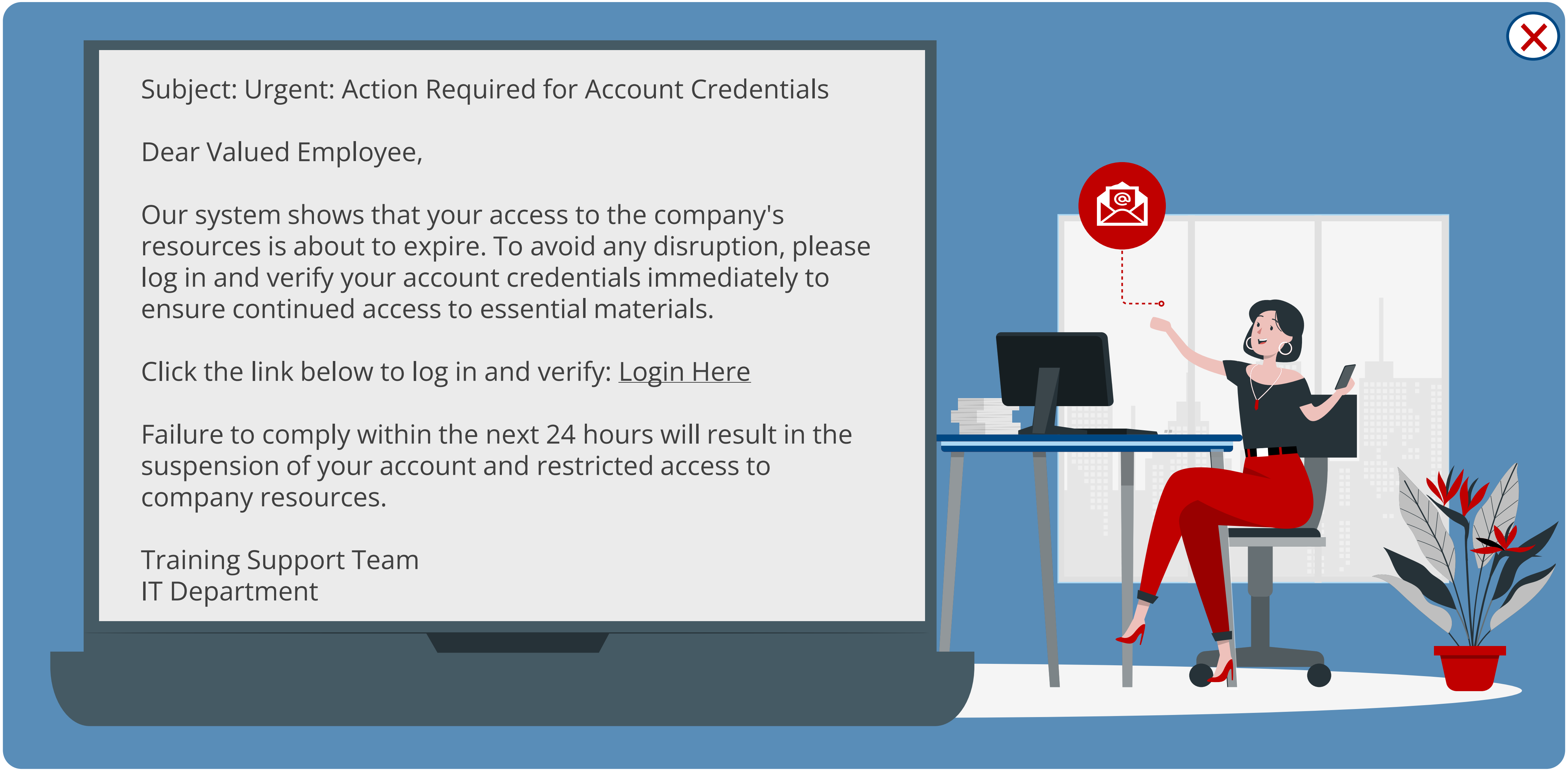
Click the Email icon below to learn more.



Phone Call

Text Message

Email



Subject: Urgent: Action Required for Account Credentials

Dear Valued Employee,

Our system shows that your access to the company's resources is about to expire. To avoid any disruption, please log in and verify your account credentials immediately to ensure continued access to essential materials.

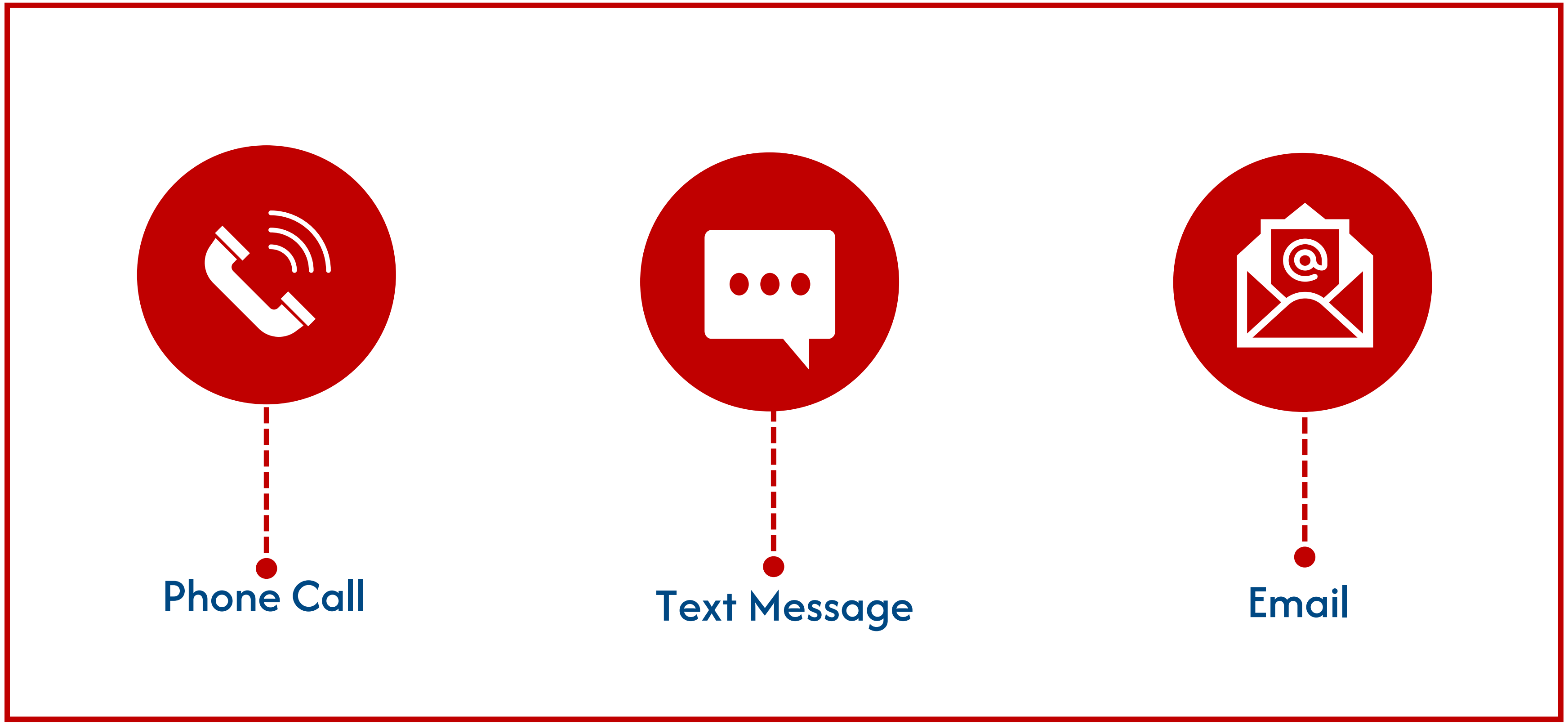
Click the link below to log in and verify: Login Here

Failure to comply within the next 24 hours will result in the suspension of your account and restricted access to company resources.

Training Support Team
IT Department

Phishing Examples

Click the Next button below to continue.



Phone Call

Text Message

Email

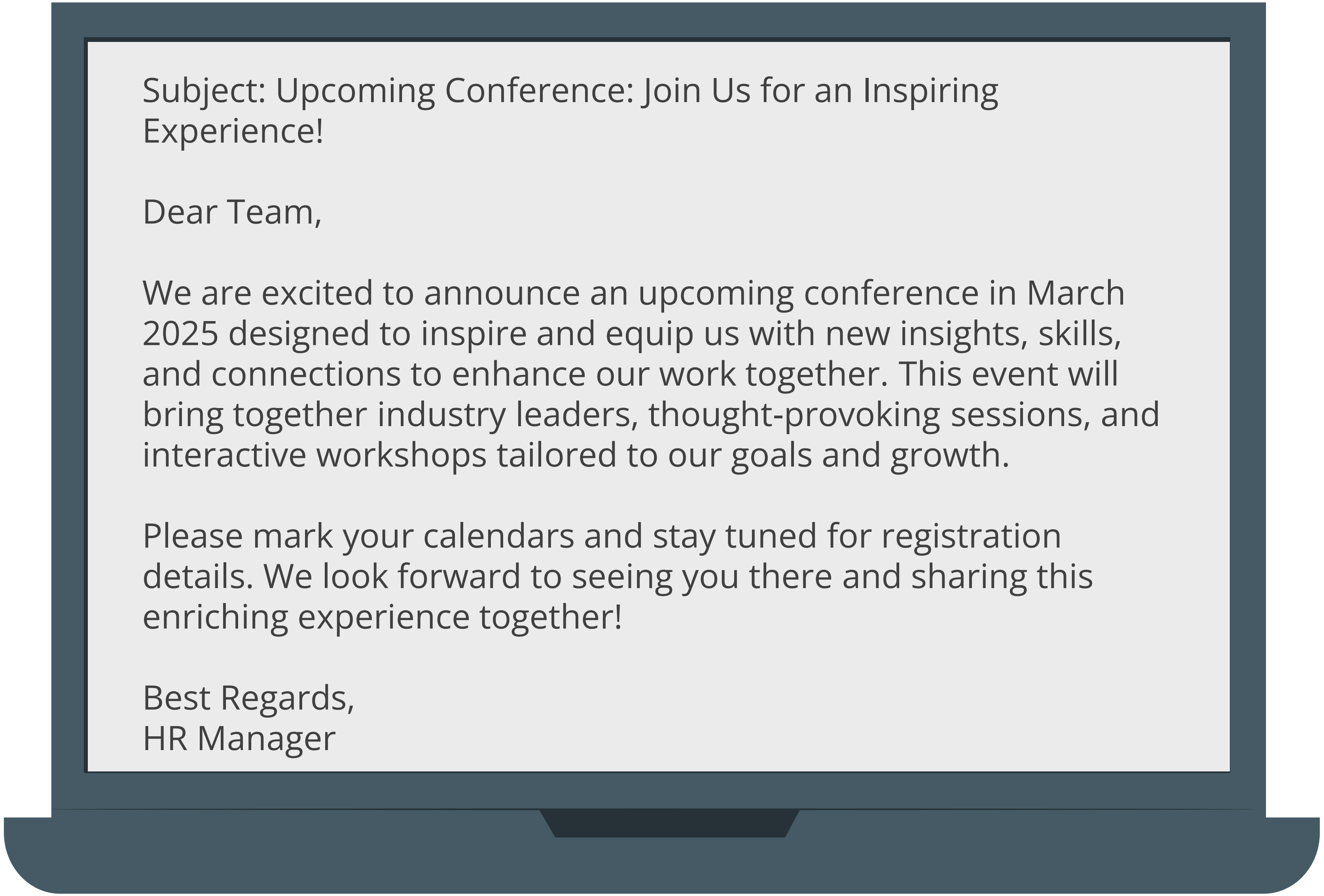
Next

What do phishing attempts have in common?

- Sense of Urgency
- Impersonation of Legitimate Entities
- Requests for Personal Information
- Suspicious Links or Attachments
- Unexpected Communication
- Poor Grammar or Inconsistencies

Next

Check Your Knowledge



Subject: Upcoming Conference: Join Us for an Inspiring Experience!

Dear Team,

We are excited to announce an upcoming conference in March 2025 designed to inspire and equip us with new insights, skills, and connections to enhance our work together. This event will bring together industry leaders, thought-provoking sessions, and interactive workshops tailored to our goals and growth.

Please mark your calendars and stay tuned for registration details. We look forward to seeing you there and sharing this enriching experience together!

Best Regards,
HR Manager

Is the following email a phishing attempt?

Yes

No

Submit

✓

Correct!

The email is authentic with a professional tone with no signs of urgent language, request personal data, or include suspicious links.

Next

Sorry, that's not the right answer.

The email is authentic with a professional tone. Legitimate communications typically align with standard business practices, while phishing emails often use urgent language, request personal data, or include suspicious links.

Next

Check Your Knowledge

Which of the following could be a sign of a phishing email?

Language that implies immediate action

A standard request for customer service feedback

A friendly greeting that includes your full name

A link that leads to a trusted company’s website

Submit

Correct!

Scammers rely on emotional pressure to make you act quickly without considering the legitimacy of the request.

Next

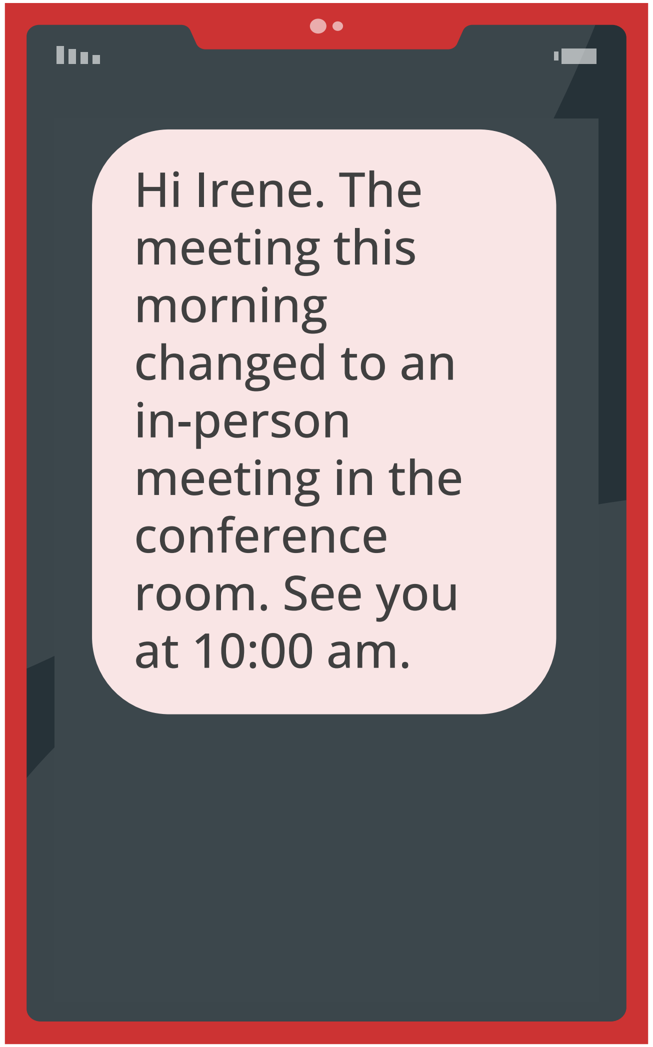
❌

Sorry, that’s not the right answer.

Language that implies immediate action is the correct answer. Phishing messages create a sense of urgency or panic, such as “Your account will be suspended!” or “Action required now!” Scammers rely on emotional pressure to make you act quickly without considering the legitimacy of the request.

Next

Check Your Knowledge



Hi Irene. The meeting this morning changed to an in-person meeting in the conference room. See you at 10:00 am.

Irene received the following text message. Is it a phishing attempt?

Yes

No

Submit

✓

Correct!

The text message is legitimate.

Next

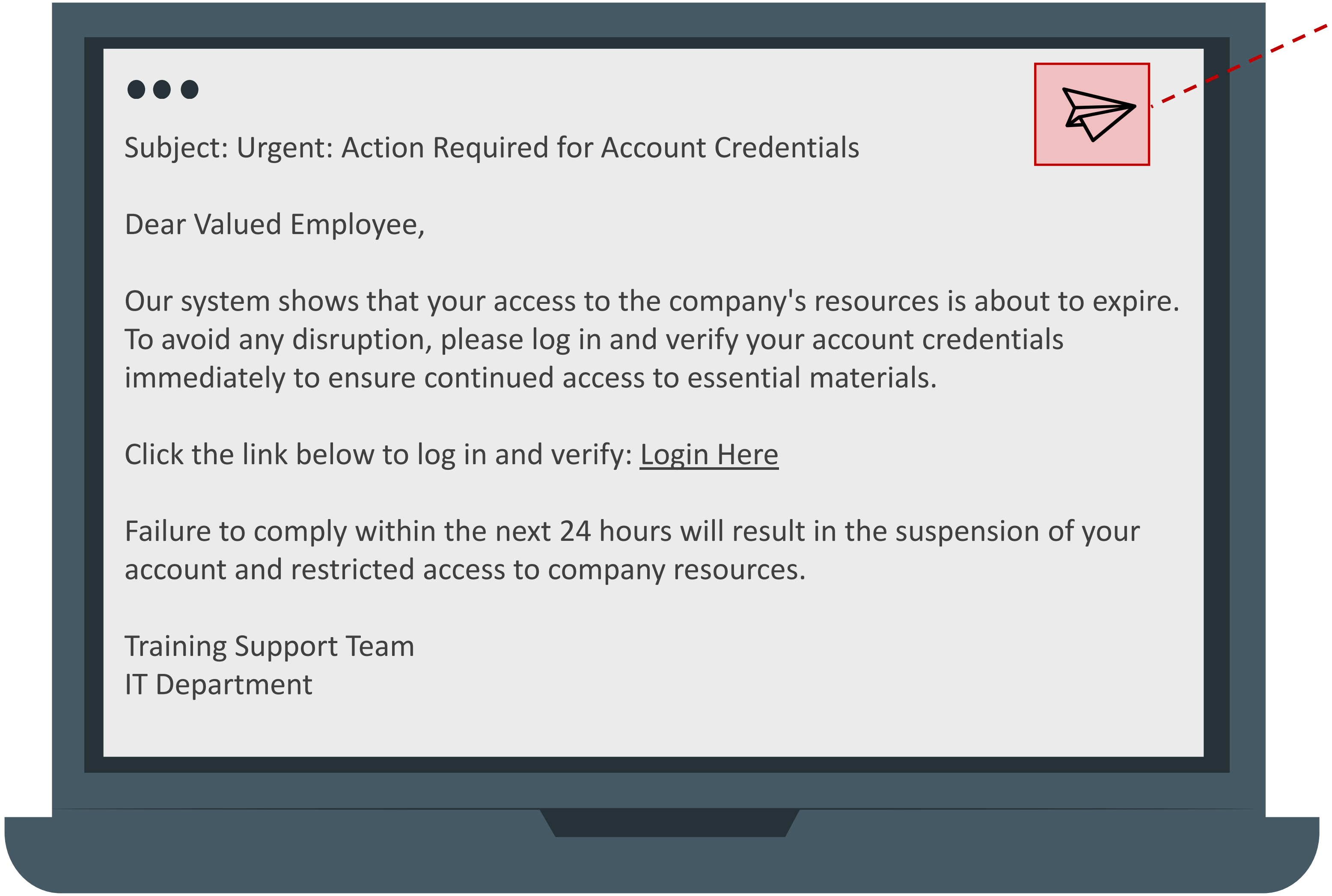
❌

Sorry, that is incorrect, it is not a phishing attempt.

Legitimate communications typically align with standard business practices, while phishing emails often use urgent language, request personal data, or include suspicious links.

Next

What should Irene NOT do if she suspects a phishing email?



Subject: Urgent: Action Required for Account Credentials

Dear Valued Employee,

Our system shows that your access to the company's resources is about to expire. To avoid any disruption, please log in and verify your account credentials immediately to ensure continued access to essential materials.

Click the link below to log in and verify: Login Here

Failure to comply within the next 24 hours will result in the suspension of your account and restricted access to company resources.

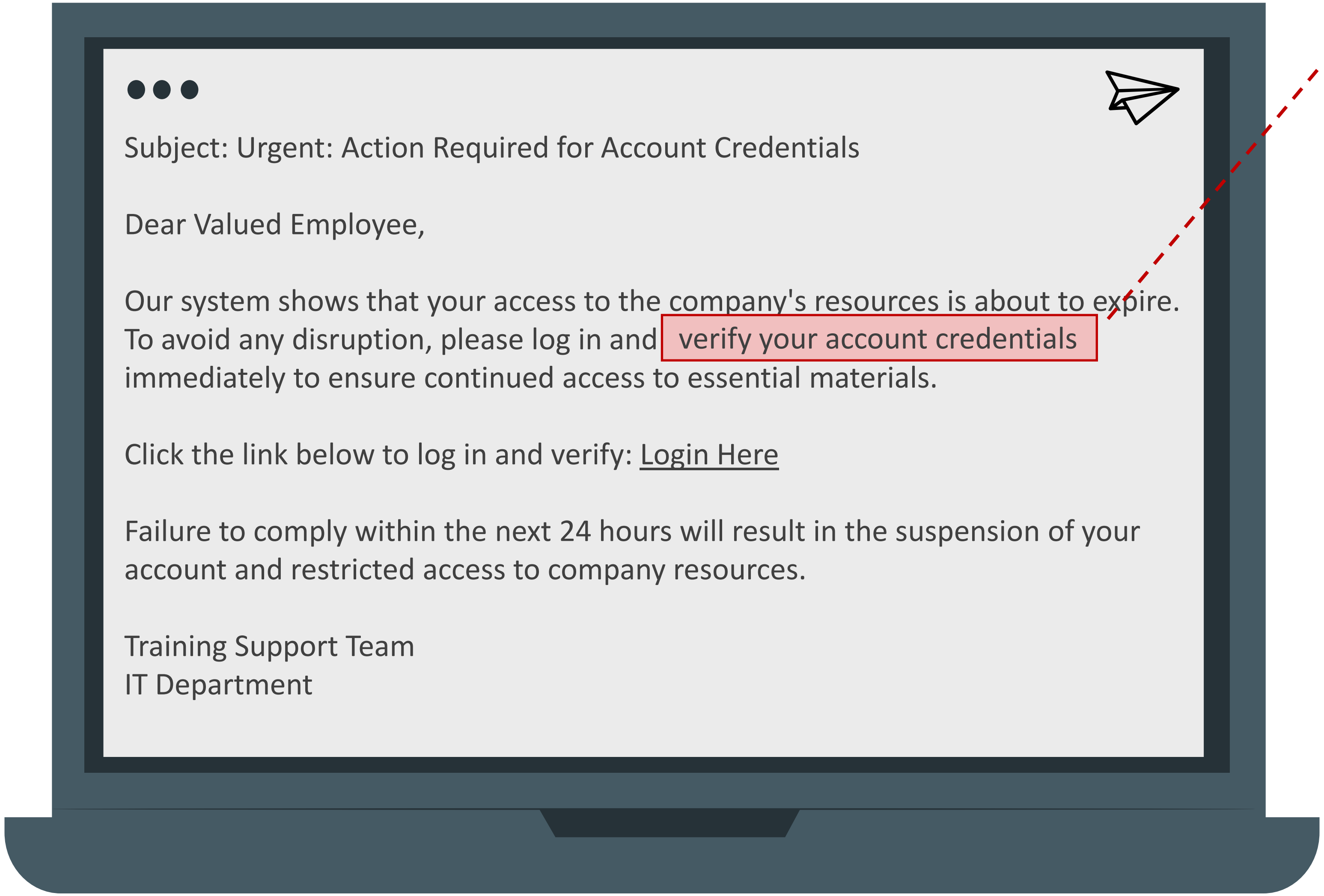
Training Support Team
IT Department

❌ **DO NOT reply to the email.**

Engaging with the sender signals that your account is active and monitored, potentially leading to more targeted phishing attempts.

Next

What should Irene NOT do if she suspects a phishing email?



Subject: Urgent: Action Required for Account Credentials

Dear Valued Employee,

Our system shows that your access to the company's resources is about to expire. To avoid any disruption, please log in and verify your account credentials immediately to ensure continued access to essential materials.

Click the link below to log in and verify: Login Here

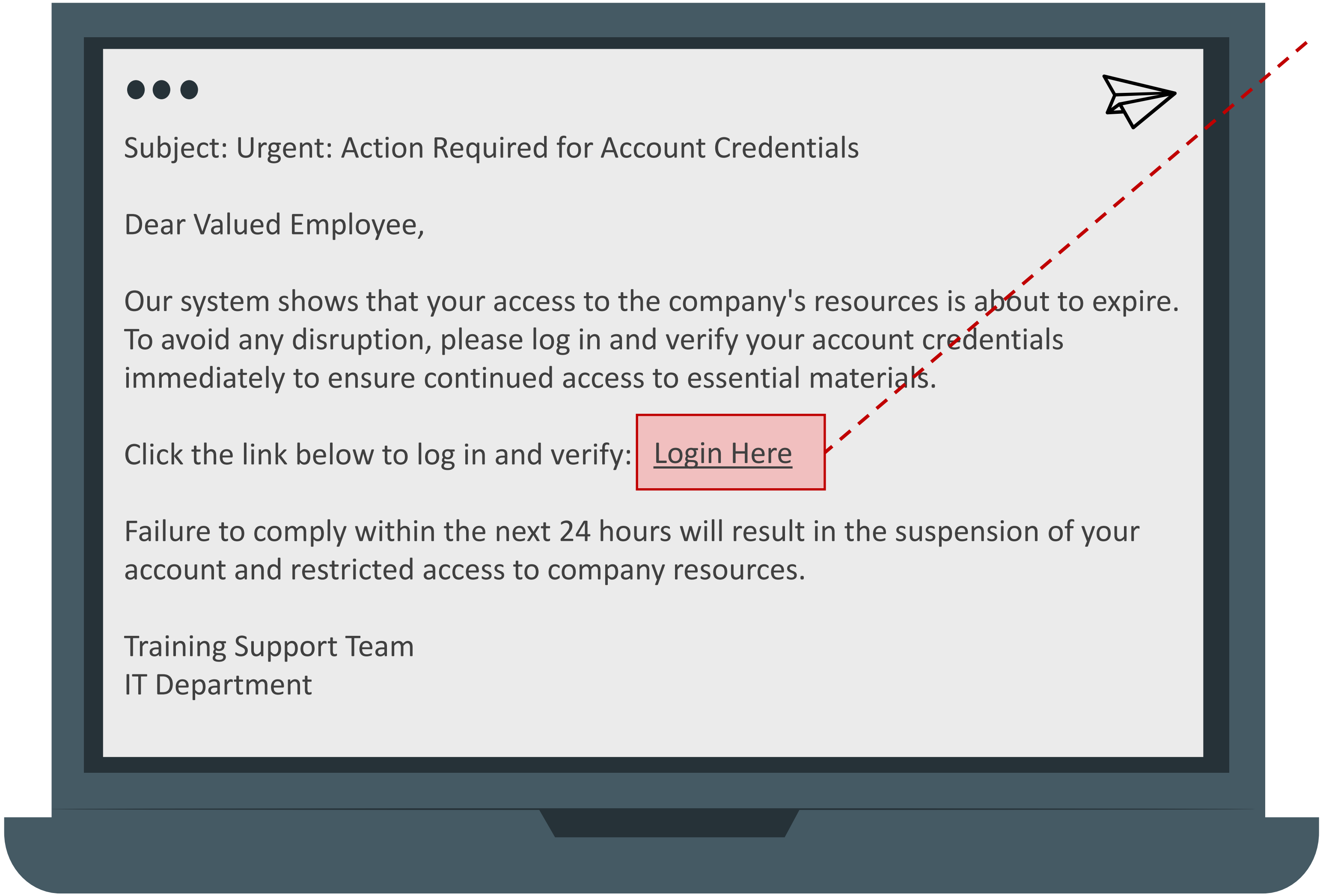
Failure to comply within the next 24 hours will result in the suspension of your account and restricted access to company resources.

Training Support Team
IT Department

✗ **DO NOT provide personal or financial information**
Any shared data, like login credentials or banking details, can be misused for identity theft or financial fraud.

Next

What should Irene NOT do if she suspects a phishing email?



Subject: Urgent: Action Required for Account Credentials

Dear Valued Employee,

Our system shows that your access to the company's resources is about to expire. To avoid any disruption, please log in and verify your account credentials immediately to ensure continued access to essential materials.

Click the link below to log in and verify: Login Here

Failure to comply within the next 24 hours will result in the suspension of your account and restricted access to company resources.

Training Support Team
IT Department

✗ **DO NOT click on any links or open any attachments.** Phishing emails often contain malicious links or attachments that, once clicked or downloaded, can install malware on your device, allowing attackers access to sensitive information.

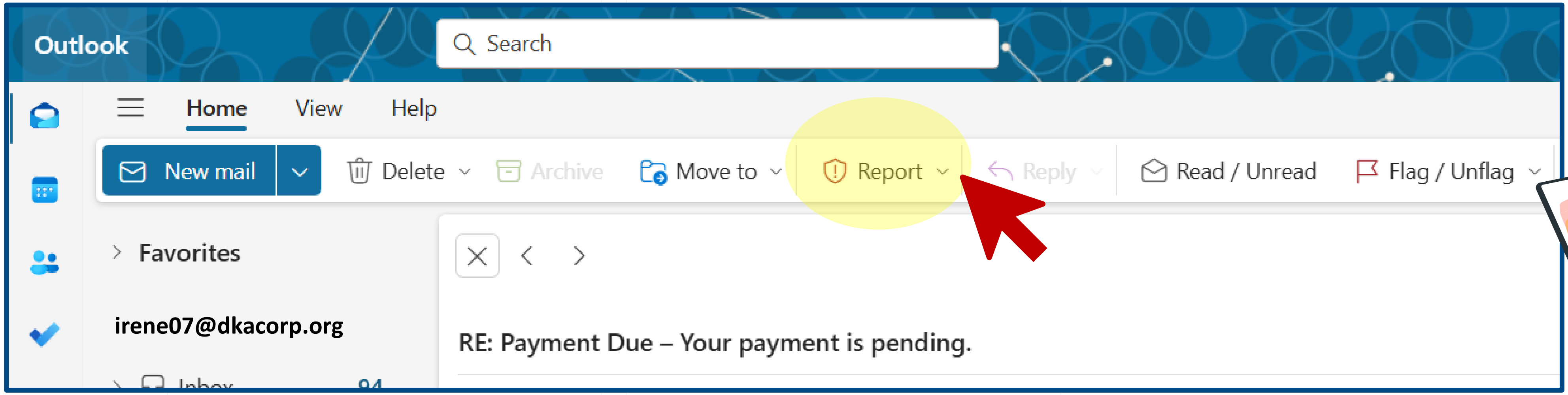
Next

How would Irene report phishing attempts to the IT department?

Next

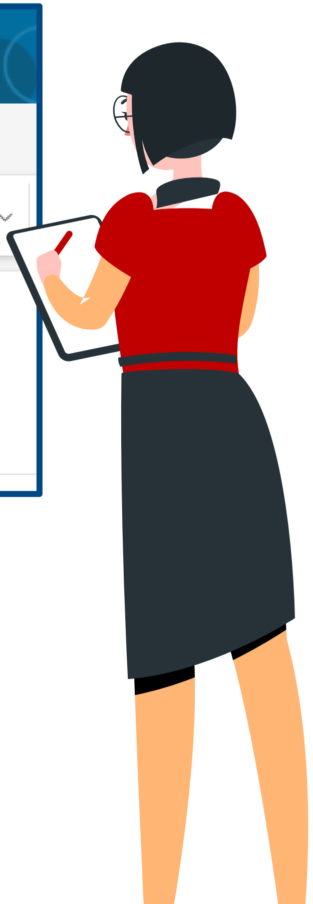
How would Irene report phishing attempts to the IT department?

1 2 3



irene07@dkacorp.org

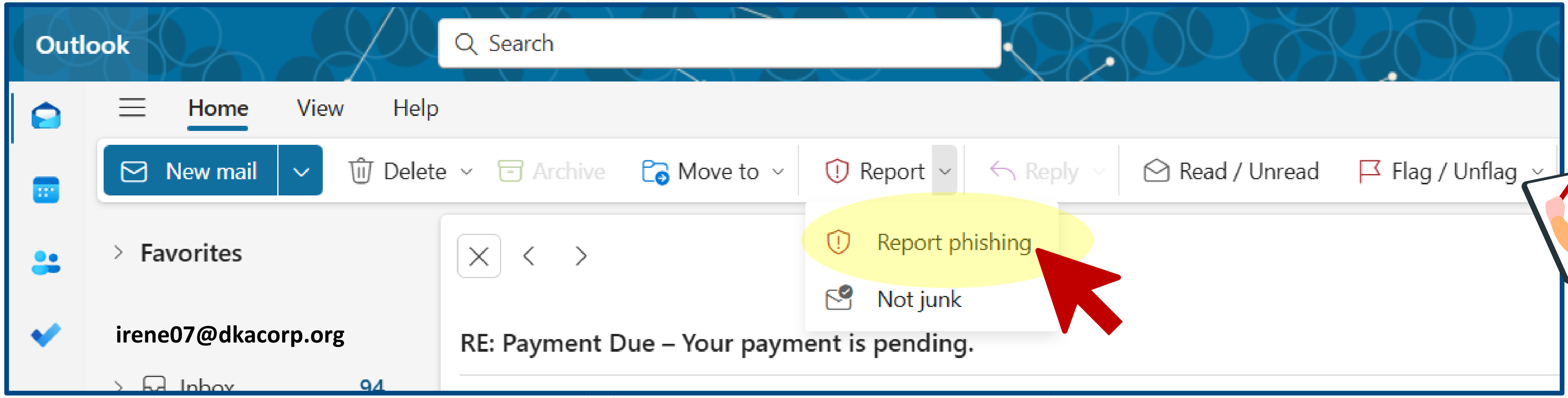
RE: Payment Due – Your payment is pending.



Next

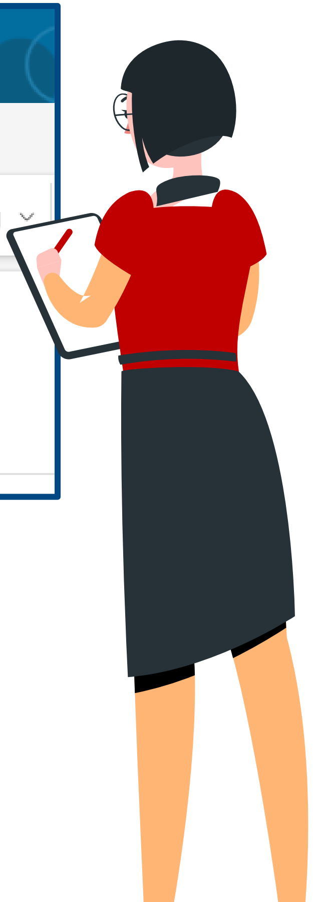
How would Irene report phishing attempts to the IT department?

1 2 3



irene07@dkacorp.org

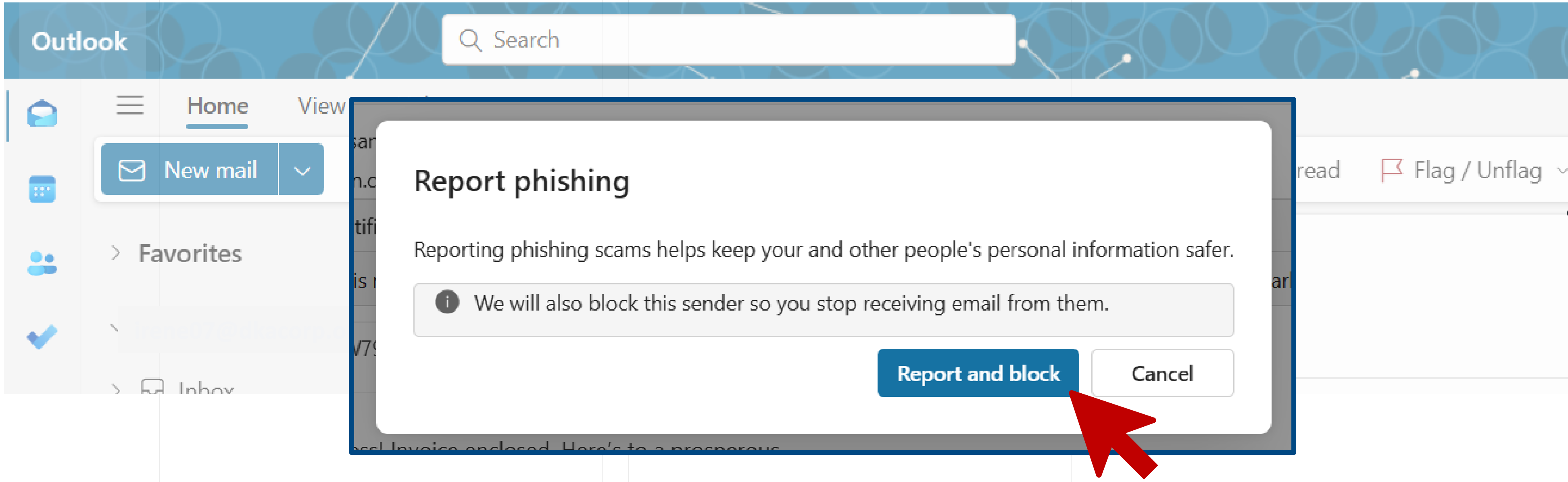
RE: Payment Due – Your payment is pending.



Next

How would Irene report phishing attempts to the IT department?

1 2 3



Report phishing

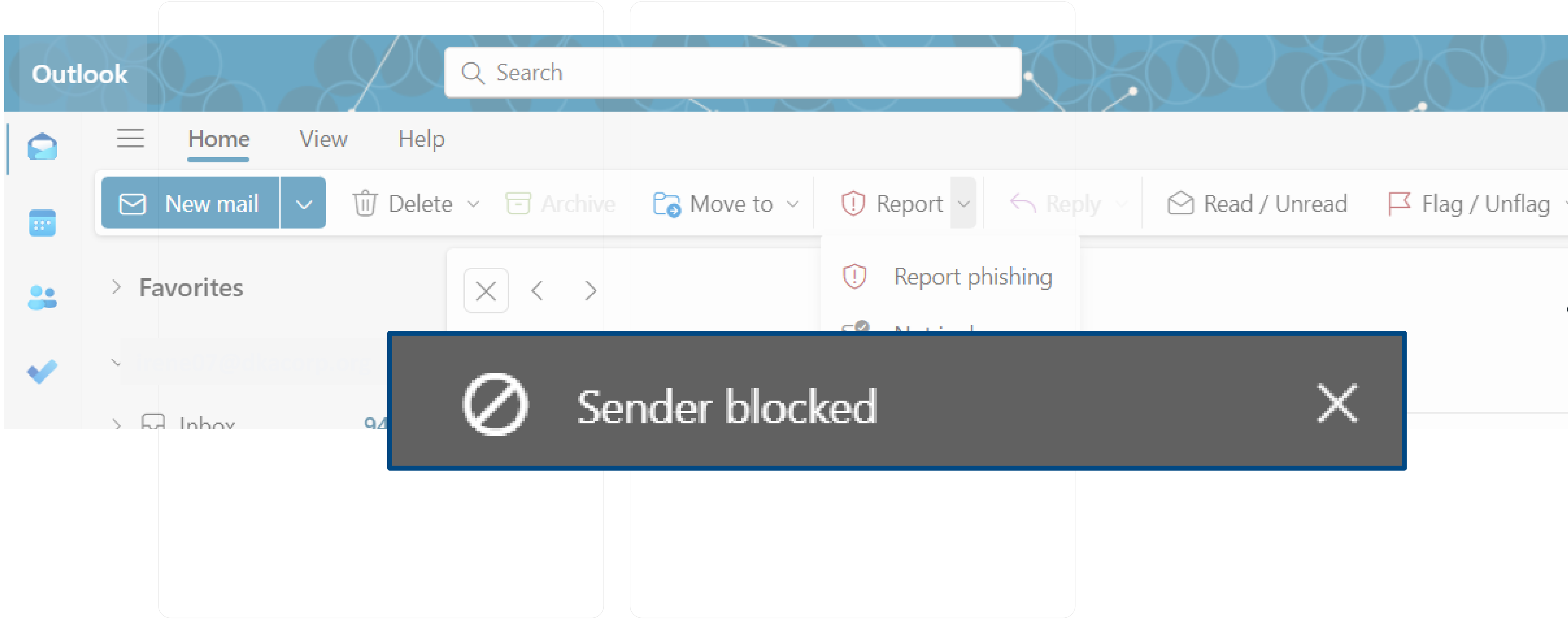
Reporting phishing scams helps keep your and other people's personal information safer.

We will also block this sender so you stop receiving email from them.

Report and block Cancel

Next

How would Irene report phishing attempts to the IT department?



Sender blocked

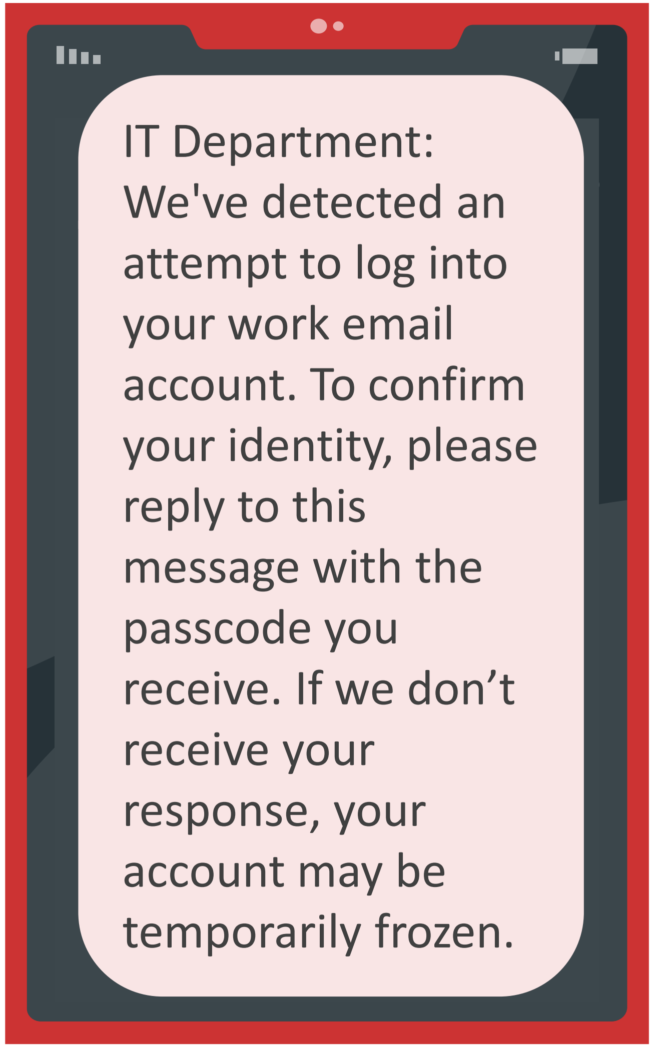
Next

Any questions about the validity of the email?

Contact the IT Department at **800-888-6708**

Next

Check Your Knowledge



IT Department: We've detected an attempt to log into your work email account. To confirm your identity, please reply to this message with the passcode you receive. If we don’t receive your response, your account may be temporarily frozen.

Irene received the following text message on her work issued phone, what should she do?

Send the passcode

Reply to the message and ask follow-up questions

Report the incident to the IT Department

Copy the message and send it to her friend

Submit

✓

Correct!

The cell phone belongs to DKA Corporation and Irene needs to report the incident to the IT Department.

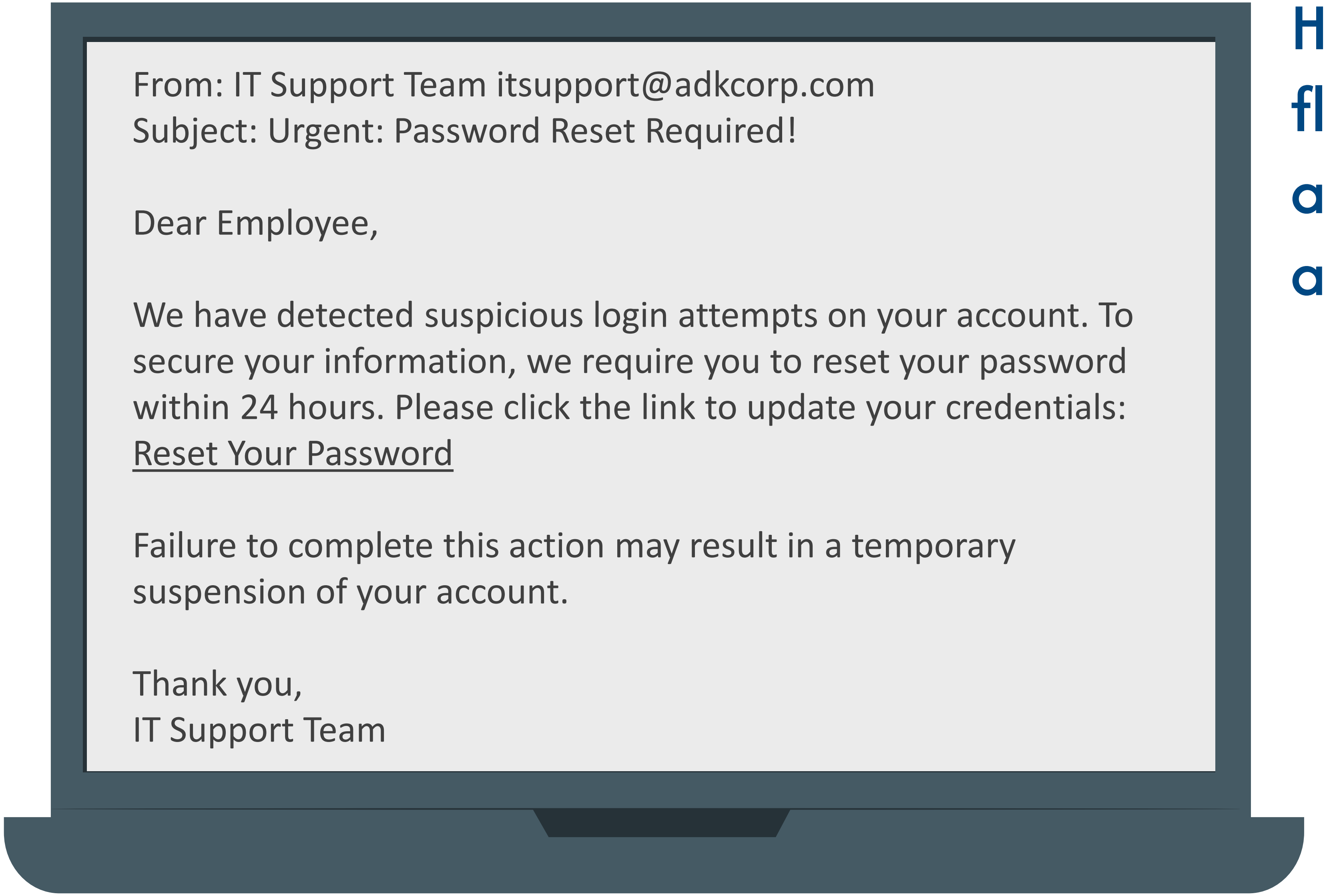
Next

Sorry, that is not the correct answer.

The cell phone belongs to DKA Corporation and Irene needs to report the incident to the IT Department.

Next

Check Your Knowledge



From: IT Support Team itsupport@adkcorp.com
Subject: Urgent: Password Reset Required!

Dear Employee,

We have detected suspicious login attempts on your account. To secure your information, we require you to reset your password within 24 hours. Please click the link to update your credentials: Reset Your Password

Failure to complete this action may result in a temporary suspension of your account.

Thank you,
IT Support Team

Help Irene identify the red flags in this phishing attempt? Select all that apply.

- Sense of Urgency
- Suspicious Link
- Generic Greeting
- Unexpected Communication

Submit

✓

Correct!

The email message indicates all the common signs of a phishing scam.

Next

Sorry, that is not the correct answer.

The email message indicates all the common signs of a phishing scam: Sense of Urgency, Suspicious Link, Generic Greeting, and Unexpected Communication.

Next

Check Your Knowledge

Irene just received a phone call from someone in the security department and they demanded that she give them remote access to her laptop immediately. What should Irene do?

- Immediately give them access to resolve the issue quickly
- Ask her co-worker what she should do
- Call the security department and verify the request
- Hang up and call them back

Submit

✓

Correct!

Irene needs to call the security department and verify the request.

Next

Sorry, that is not the correct answer.

Irene needs to call the security department number and verify the request.

Next

Check Your Knowledge

Irene received an email with an attachment from a co-worker, but she wasn't expecting it, what should she do?

Verify with her co-worker before opening it

If it's from someone she knows, she doesn't need to worry

Nothing, her email software will scan for anything malicious

Preview the attachment

Submit

✓

Correct!

This was an unexpected communication and Irene needs to verify with her co-worker before opening it.

Next

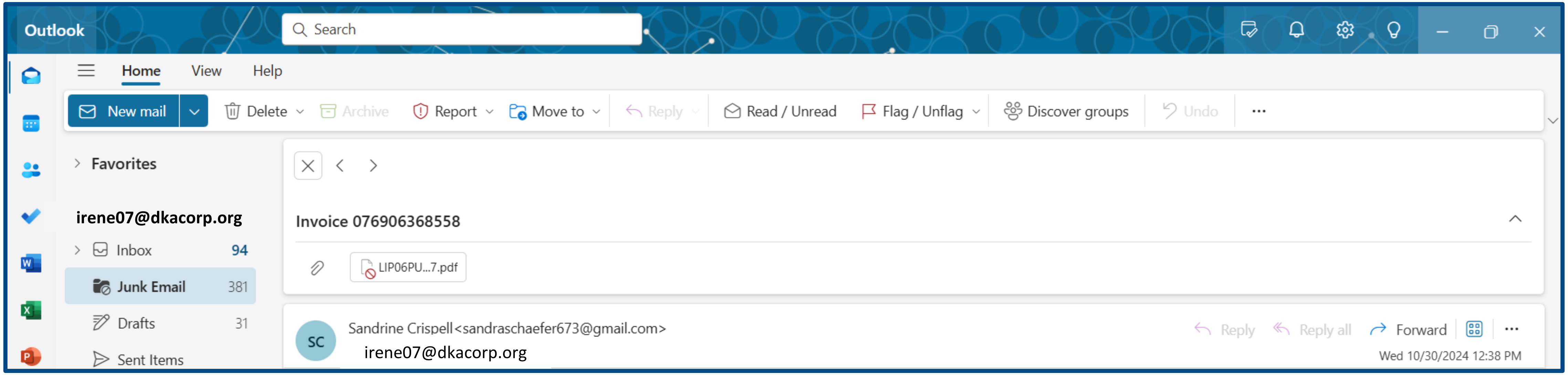
Sorry, that is not the correct answer.

This was an unexpected communication and the attachment can potentially be malicious, therefore Irene needs to verify with her co-worker before opening it.

Next

Check Your Knowledge

Irene has received a phishing email attempt. Click on the correct steps to report this email to the IT department.



irene07@dkacorp.org

Invoice 076906368558

LIP06PU...7.pdf

Sandrine Crispell<sandraschaefer673@gmail.com>
irene07@dkacorp.org

Wed 10/30/2024 12:38 PM

Great job!

Irene has reported the phishing attempt to the IT department and is keeping her device safe.

Next

Sorry, that’s not correct.

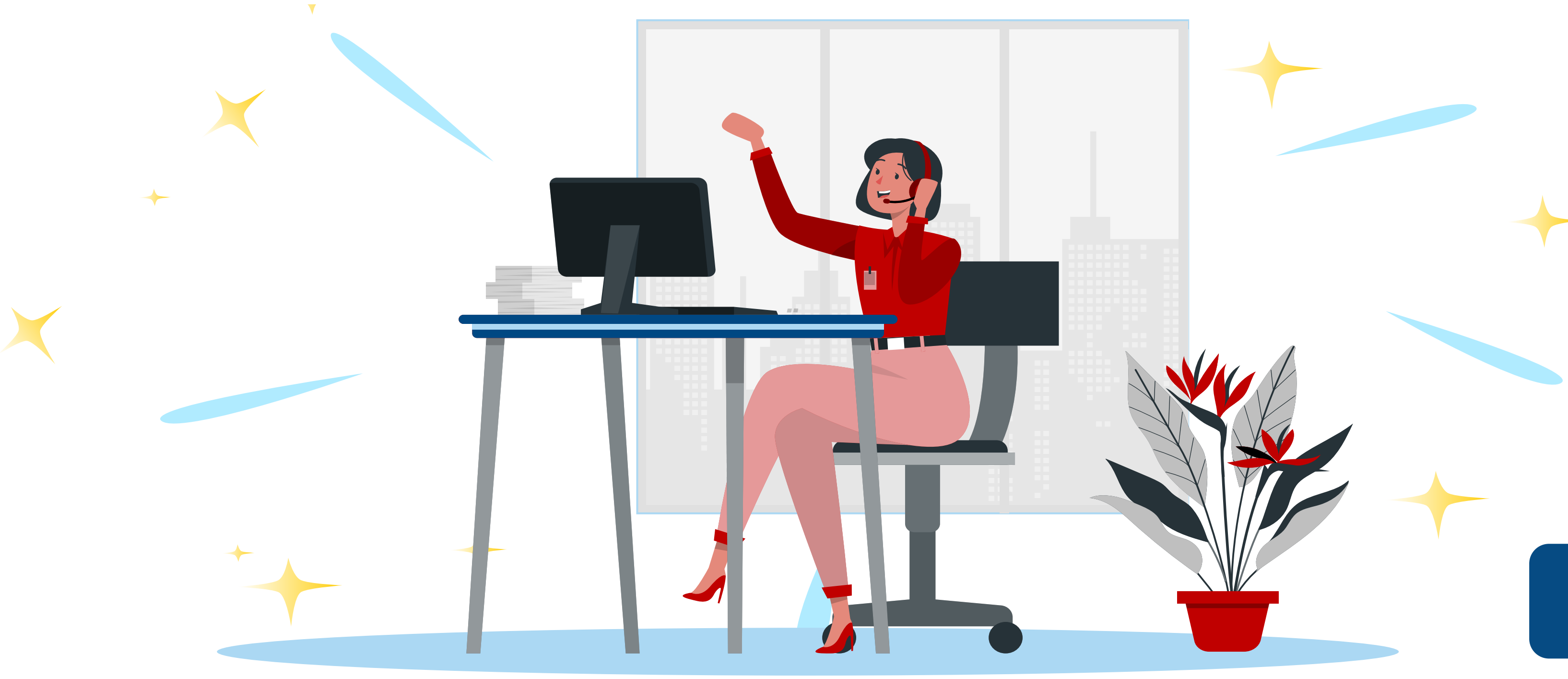
DKA Corporation’s email platform, Outlook, has a built-in phishing reporting tool. Please try again.

Try Again

DKA Corporation

Certificate of Completion

Identifying Phishing Scams



Next

THINK ?

Before you Click!

Resources

Exit