

ReelsNode Q&A

Email Scam Warning Signs

10 Questions with Juhi & Sahil

Book 108

VIPUL PATEL

reelsnode.com

Visit reelsnode.com for more mini-PDF Books

About Vipul Patel

Vipul Patel holds a Master's degree in Electronics and has spent his career exploring technology, business, finance, and lifelong learning. Through the Booklets series and reelsnode.com, he combines his passion for learning with a simple mission: to make practical knowledge easy to understand and useful in everyday life.

Copyright

Copyright (c) 2026 VIPUL PATEL. All rights reserved. No part of this publication may be reproduced, stored, or transmitted without prior written permission from the copyright owner. Published by Babli Booklets Things School Never Taught. www.reelsnode.com

reelsnode.com

Visit reelsnode.com for more mini-PDF Books

Sahil asks:

Juhi, can I tell an email is a scam just by looking at it?

Juhi explains:

Not always. Scam emails can look professional and may copy real companies. Instead of trusting the appearance, check the sender, message, links, and request carefully.

JUHI'S ACTION: Judge the request, not just the design.

reelsnode.com

Visit reelsnode.com for more mini-PDF Books

Sahil asks:

What should I check about the sender?

Juhi explains:

Look carefully at the full email address. A scammer may use an address that looks similar to a real one but contains extra letters, misspellings, or an unexpected domain.

JUHI'S ACTION: Check the full sender address.

Sahil asks:

Why do scam emails often say something is urgent?

Juhi explains:

Pressure can make you act before you verify the message. Be cautious with claims that your account will be closed, money will be lost, or immediate action is required.

JUHI'S ACTION: Don't let urgency rush you.

Sahil asks:

What if the email asks me to click a link?

Juhi explains:

Be careful with unexpected links, especially when the email asks you to sign in, make a payment, or provide personal information. Go to the organization's official app or website yourself instead.

JUHI'S ACTION: Avoid unexpected sign-in and payment links.

reelsnode.com

Visit reelsnode.com for more mini-PDF Books

Sahil asks:

Are unexpected attachments dangerous too?

Juhi explains:

They can be. An unexpected attachment may contain harmful software or lead you to a fake document. Verify the sender and reason for the file before opening it.

JUHI'S ACTION: Verify unexpected attachments first.

Sahil asks:

What information should I never send just because an email asks?

Juhi explains:

Be especially protective of passwords, verification codes, banking details, and government ID numbers. A legitimate-looking email is not proof that the request is safe.

JUHI'S ACTION: Protect sensitive information.

reelsnode.com

Visit reelsnode.com for more mini-PDF Books

Sahil asks:

What if the email says I won a prize or I'm owed a refund?

Juhi explains:

Unexpected prizes, refunds, or rewards deserve extra checking, especially if you must pay a fee or provide financial information to receive them.

JUHI'S ACTION: Verify unexpected money offers independently.

reelsnode.com

Visit reelsnode.com for more mini-PDF Books

Sahil asks:

What if the email appears to come from my boss, friend, or family member?

Juhi explains:

Their account could be compromised, or the sender could be impersonating them. If the request involves money, passwords, gift cards, or sensitive information, confirm it another way.

JUHI'S ACTION: Verify unusual requests outside email.

Sahil asks:

What should I do if I'm still not sure whether an email is real?

Juhi explains:

Don't use the contact information in the suspicious email. Open the organization's official app or website, or use a trusted phone number you already have to verify the message.

JUHI'S ACTION: Use an independent way to verify.

reelsnode.com

Visit reelsnode.com for more mini-PDF Books

Sahil asks:

What if I already clicked or entered information?

Juhi explains:

Act quickly. Change any exposed passwords, contact the affected organization through an official channel, and review relevant accounts for suspicious activity. If you downloaded a suspicious file, use trusted security tools or professional help to check the device.

JUHI'S ACTION: Respond quickly after a mistake.

reelsnode.com

Visit reelsnode.com for more mini-PDF Books

Juhi's Quick Check

- Before trusting an unexpected email, check:
- Does the full sender address look correct?
- Is the message creating unusual urgency?
- Does it contain an unexpected link or attachment?
- Is it asking for money or sensitive information?
- Is the offer or story unexpected?
- Can I verify the request another way?

Simple Rule

Remember

If an email pressures you to click, pay, sign in, or share sensitive information, stop and verify the request independently.

reelsnode.com

Visit reelsnode.com for more mini-PDF Books