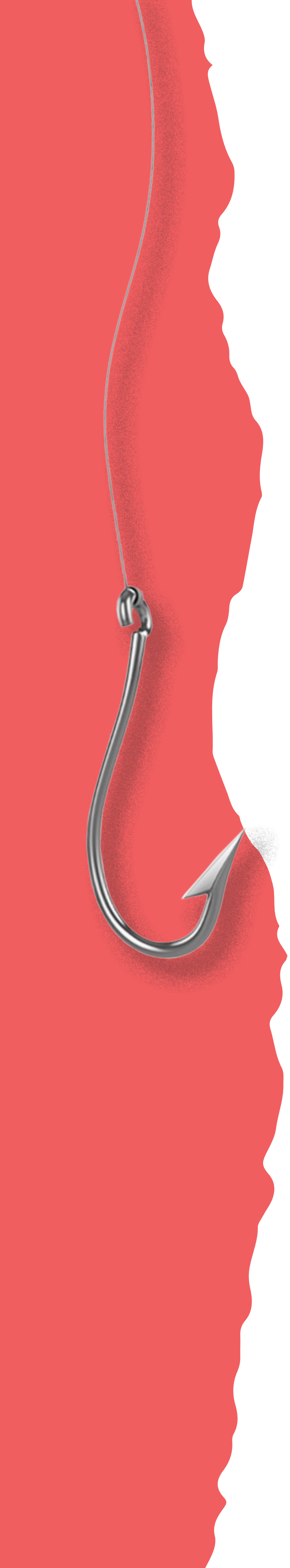
KALARA®

YOUR GUIDE TO

EMAIL SAFETY



CONTENTS

INTRODUCTION

Email plays a crucial role in communication in today's fast-paced digital world. It's an essential tool for both internal and external business communication. However, the convenience of email comes with a significant challenge — keeping your inbox safe from cyber threats.

Email safety is like securing your virtual front door. It helps protect sensitive information, maintain data integrity and safeguard your digital reputation. Increasing cybersecurity concerns have made prioritising email safety more critical than ever.

This eBook will serve as your first step to strengthening your inbox. Following the best practices outlined in this guide will give you insights into a more secure email experience.
Our goal is to empower you without overwhelming you and to ensure that email becomes your source of success instead of burnout.

Below we detail a few simple steps that can amplify the security of your email communication.

THE IMPORTANCE

of email safety in protecting your digital life

Within your inbox lies a trove of sensitive data, from personally identifiable information to financial details. Inadequate protection could lead to unauthorised access, resulting in identity theft or fraudulent activities.

Spam emails serve as instruments for spreading phishing, malware and ransomware attacks. Prioritising email security thus becomes imperative to thwart these insidious attacks.

Whether for business transactions or private conversations, maintaining the confidentiality of your emails is pivotal.

Email safety assures that only intended recipients can access your messages.

> *“Maintaining the confidentiality of your emails is pivotal”*

Email account takeovers mirror unwelcome guests intruding on your privacy. They disrupt your peace by dispatching unsolicited emails, proliferating malware and causing chaos. Implementing safety measures erects barriers against these digital trespassers.

Prioritising email safety serves as a road to legal compliance, considering the multiple data protection laws in place. Therefore, to keep your business in line, it would help to address email safety.

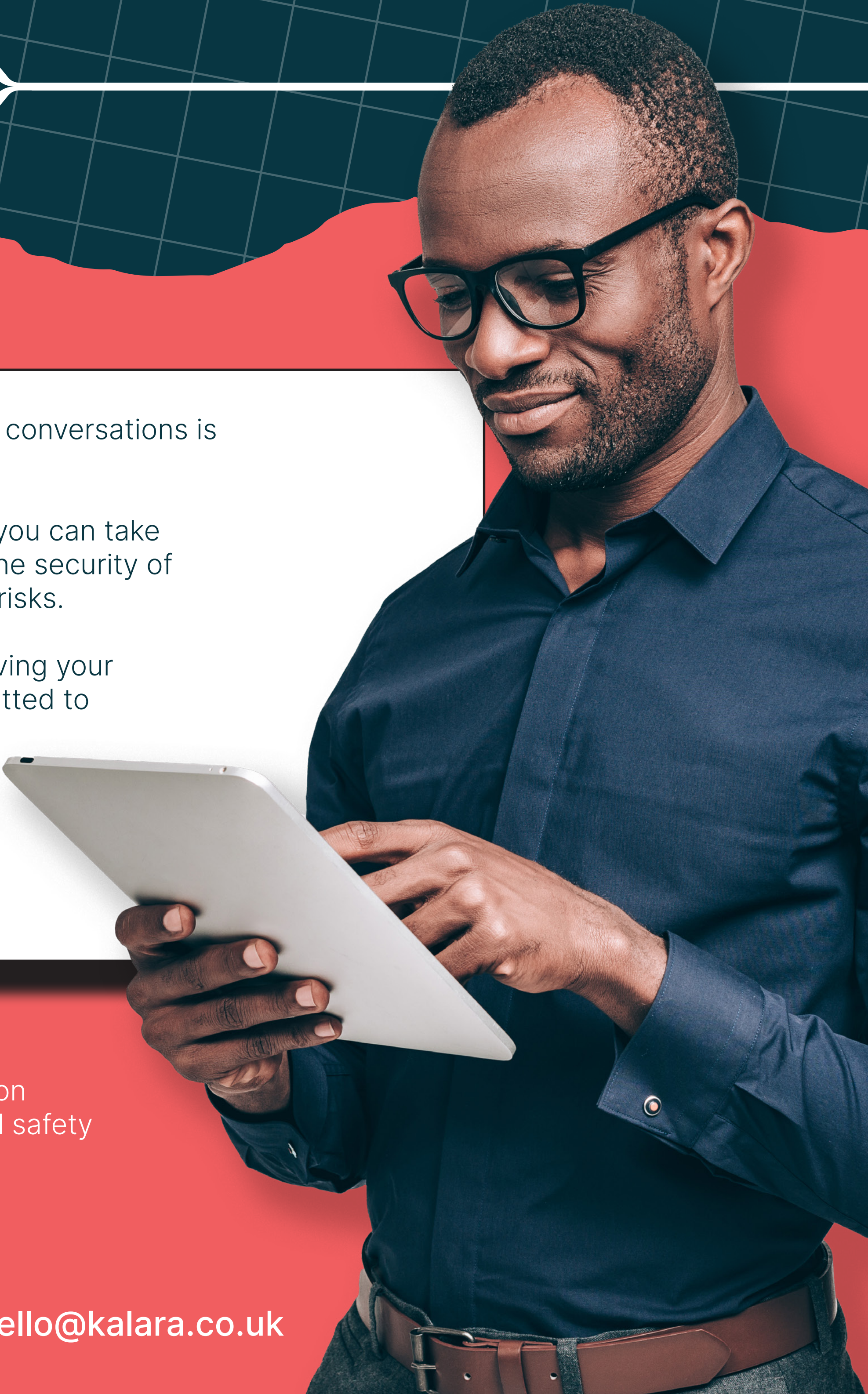
Imagine losing crucial emails due to accidental deletions or security breaches. Email safety measures function as a safety net, averting unfortunate incidents.

STEPS TO STAY SAFE FROM EMAIL TRAPS

Follow these simple steps to ensure the safety of your inbox:

- Secure your email account with a robust, unique password, as you would secure your front door. Make sure not to share it with anyone.
- Employ two-factor authentication (2FA) to add another layer of security. 2FA acts as a digital bodyguard by verifying your identity before granting access.
- Be cautious of suspicious email links and unfamiliar attachments. These could harbour digital trojans ready to take down your network.
- Exercise caution while sharing personal details. Reserve this for instances where the sender’s identity is beyond doubt.
- Keep your email software and antivirus defences updated to thwart security breaches.
- Avoid using public Wi-Fi for sensitive emails since data shared on open networks lacks the privacy you need.
- Stay vigilant against sophisticated phishing attempts capable of threatening your sensitive data.
- Regularly monitor your email for anomalies, ensuring prompt detection of any unusual activity.
- Safeguard crucial emails with secure backups, similar to how you safeguard your valuable items.
- Deploy spam filters to intercept sneaky attackers before they infiltrate your inbox.
- Use encrypted connections like HTTPS to shield data during transmission.
- Stay informed of emerging email threats to sustain a state of perpetual readiness.

START YOUR EMAIL SAFETY JOURNEY NOW



Remember that protecting digital conversations is your responsibility.

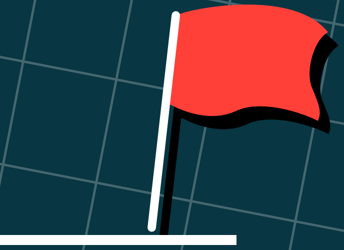
By following the steps provided, you can take proactive measures to increase the security of your inbox and prevent potential risks.

If you need additional help improving your email security, our team is committed to supporting you on this journey.

Contact us to schedule a no-obligation consultation, and let's start your email safety journey together.

Contact us to schedule a no-obligation consultation and let's start your email safety journey together.

t: 01293265777 e: hello@kalara.co.uk

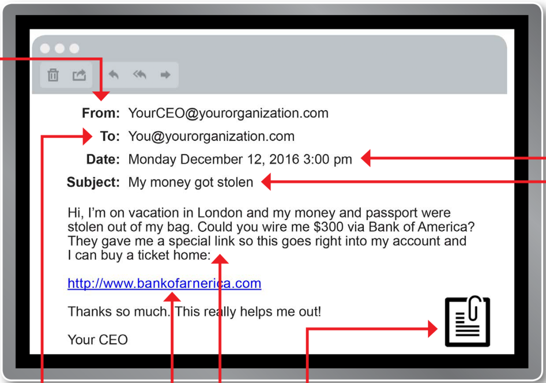


SPOT THE RED FLAGS

Can you find the red flags in this

Recognising a BEC attack

Business Email Compromise (BEC) is a cyberattack where criminals impersonate trusted individuals or organisations through emails to deceive victims into transferring funds or sharing sensitive information.



From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday December 12, 2016 3:00 pm
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:

http://www.bankofarnerica.com

Thanks so much. This really helps me out!

Your CEO

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

Get in touch

t: 01293265777

e: hello@kalara.co.uk