

Staying safe from fake ISSBD emails

Last updated: 10/1/2026

Scammers sometimes pretend to be ISSBD leaders to trick members into sending money or personal information. This page explains what we will and will not ask of you, how to spot a fake message, and what to do if one reaches you. It takes about two minutes to read.

CURRENT ALERT

Fraudulent emails are circulating in the name of ISSBD President, Professor Frosso Motti-Stefanidi. These messages are not from the President or anyone at ISSBD. Please do not reply to them.

The latest messages (30 September 2026) came from **excupress@gmail.com**, asking members to make a bank transfer for “delegate travel support” to be “reimbursed later”. Earlier messages came from **presidenthovboardcommittee@gmail.com**. Scammers change addresses often, so please use the rule below rather than relying on this list.

The one rule to remember

ISSBD officers and staff will never email you asking for money, gift cards, bank details, passwords or an urgent personal favour.

If a message asks for any of these, it is a scam, even if it uses a real name, a real title or the ISSBD logo.

What a genuine ISSBD message looks like

We contact members for things like membership renewals, conference and webinar information, newsletters, and calls for nominations. Genuine messages:

- Come from an official address ending in [**@issbd.org**], or from our membership platform [name of system, e.g. the Wiley/ISSBD member portal]
- Send any payment through the secure ISSBD website, never by reply email, gift card or transfer to a personal account
- Never ask you to keep a request secret or to act within minutes
- Will still be genuine if you take time to check them, so there is no harm in pausing

How to spot a fake

Impersonation scams follow a familiar script. Watch for these warning signs:

Warning sign	What it looks like
Unofficial sender	A Gmail, Outlook or similar free address with an official-sounding name, e.g. "president.board.committee@gmail.com". Check the actual address, not just the display name.
A vague opener	"Are you available?", "Do you have a moment?" or "I need a quick favour."
Urgency and secrecy	"I am in a meeting and cannot talk", "Please keep this between us", "I need this done today."
A warm-up message	A friendly first email ("Are you working or on leave?") with no request yet, just to see if you will reply.
Payment requests	Asking you to pay something on ISSBD's behalf ("delegate travel support", an invoice, gift cards, a wire transfer), with a promise to reimburse you later.
An excuse for not using official channels	"Our finance office has an audit issue", "I have no access to my bank token", "I am travelling."
Moving you off email	Asking for your mobile number or to continue on WhatsApp or text.
Something feels off	Unusual tone, odd grammar, or a request the person would never normally make of you.

A real example

This is a shortened version of a message an ISSBD member received in September 2026. The member's details have been removed. Notice how it builds trust over several emails before asking for money.

From: Frosso Motti-Stefanidi <excupress@gmail.com>
Subject: ISSBD

Email 1: "I hope you're doing well. Are you currently working or enjoying some time off? I'm reaching out to ask for your assistance with some delegate logistics services concerning the ISSBD."

Email 2 (after the member replied): "I need your assistance with a transfer of \$2,9750 for a delegate travel support. Due to some account auditing issues... my finance officer is unable to make bank appointments... I am currently away from the office with no remote access... the payment is needed urgently... I will have the amount fully reimbursed back to you immediately."

Red flags: a Gmail address with the President's name as the display name • a vague first message to see if you will reply • ISSBD business used as cover • a personal bank transfer • a story about why official channels cannot be used • urgency • a promise of "immediate" reimbursement • an odd amount.

What this member did right: before sending anything, they emailed the President at her known university address to ask if the request was real. That one step stopped the scam. If something feels off, check it with the person through a contact you already trust.

If you receive a suspicious email

1. **Do not reply**, click links or open attachments.
2. **Forward it to us** at [security/communications address] if you can. This helps us track new addresses and warn others.
3. **Report it** as phishing or spam in your email program (in Gmail and Outlook, use the “Report phishing” option).
4. **Delete it.**

If you have already replied, paid or shared details

Do not worry. These scams are designed to be convincing, and acting quickly makes a real difference.

- **Contact your bank or card provider** straight away if you sent money or shared financial details. If you bought gift cards, contact the card company too, as funds can sometimes be frozen.
- **Change your password** if you entered it anywhere, and turn on two-step verification.
- **Let us know** at [address] so we can warn other members.
- **Report it** to your national fraud or cybercrime authority (see below).

Checking whether a message is genuine

If in doubt, check it out, and always use contact details you already trust. Do not use the phone number, address or link given in the suspicious message. Email us at [official address] or use the contact page at [issbd.org/contact]. We are always happy to confirm whether a message is from us.

Frequently asked questions

Has ISSBD been hacked?

[Confirm with the web team before publishing.] We have no evidence that ISSBD systems have been compromised. Impersonation scams like this are common across professional associations, universities and charities. Scammers often gather names and titles from public websites and conference programmes.

Why did I receive this message?

Scammers often target members of well-known organisations using publicly available information. Receiving one does not mean you did anything wrong.

Will ISSBD ever ask me to pay by email?

No. Membership fees, registrations and donations are only ever paid through the secure ISSBD website or official invoices from [ISSBD / partner]. We will never ask for gift cards or payment to a personal account.

Can ISSBD stop these emails?

We report fraudulent accounts to the email providers so they can be shut down, and we keep this page updated. Scammers can create new free addresses quickly, though, which is why the one rule above is your best protection.

Someone is impersonating me as an ISSBD officer. What should I do?

Tell us at [address] so we can update this page and alert members. Consider posting a short warning on your own professional channels.

Known fraudulent addresses

We list addresses that members have reported. This list will never be complete, so a message is not safe just because its sender does not appear here.

Address	Impersonating	First reported
excupress@gmail.com	ISSBD President	30 September 2026
presidenthovboardcommittee@gmail.com	ISSBD President	August 2026

Report and learn more

You can also report phishing to independent bodies that help take scam accounts down:

- **Anyone, worldwide:** forward to the Anti-Phishing Working Group at reportphishing@apwg.org (apwg.org/reportphishing)
- **United Kingdom:** forward to report@phishing.gov.uk ([GOV.UK guidance](https://gov.uk/guidance))
- **United States:** [FTC consumer advice on gift card scams](https://www.ftc.gov/consumer/advice-on-gift-card-scams)
- **Other countries:** contact your national cybercrime or consumer protection authority.

Thank you for helping keep the ISSBD community safe. Every message you report helps protect a colleague.