



How to protect yourself against Exhibition Scammers

Scamming is a huge problem across the globe, with the total cost to the world of cybercrime estimated to rise to a staggering \$10 trillion by 2025. It's a fact that scammers are getting smarter, more sophisticated, and more aggressive.

Trade shows are not immune from this worrying trend and exhibitors at trade shows can represent an attractive target for scammers, who harvest data from public websites and directories and pretend to represent the organiser of the event, or companies associated with the event.

We want you to enjoy your exhibition experience, to be alert and to protect yourself and your company from potential scams. This short fact sheet aims to help you to identify scams you should look out for, what makes something look suspicious, and what to do if you are a victim of scamming.

Most common types of scams

An email claiming to represent the organiser offering a free directory listing. The small print often shows that this is only free for the first year, with substantial fees in subsequent years. This type of scam is common and has been going on for many years.

An email claiming to be from the organiser or a company associated with the organiser offering data for sale. We as organisers will never contact you with an offer like that. This is also against GDPR rules. From time to time, scammers use our branding. If you're ever unsure, please contact us directly.

An email offering to provide services on behalf of the organiser, such as hotel bookings.

An email, or increasingly telephone calls, claiming to be from the organiser, warning that your details need updating, and if you don't do it immediately, your contract will be terminated, or other a similar threat.

An unexpected email or telephone call requesting you to provide updated contact or banking details

People watching you in a crowded area, such as a hotel reception where they may be able to copy credit cards, or find out details about yourself which they can use for a scam.

An email asking for a special favour, or a refund of money, which you didn't expect

A social media message, such as What's App, asking for something you didn't expect. This may include a photo of the person being imitated.

Typical things you need to look out for

Do I know the person sending the email? And even if I do, is the address behind the email associated with that individual. To see the full address put your cursor over the email address

Is the email or call of an URGENT nature? Is there a deadline?

Is this the type of correspondence you expect from the organiser or the individual?

Is the company listed as an official contractor in the exhibition organiser's exhibition manual?

Is the email credible? Is it offering data for sale, asking for sensitive information or offering something you don't expect?

Does the language feel clumsy?

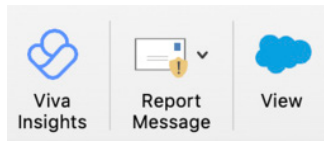
Are there click-throughs in the email, which may look innocent, but you wonder why they are there?

Is anyone observing you when you are providing sensitive information in a public space, such as a hotel

What to do if you feel you think you are being scammed

Do not reply to the email, and **DO NOT**, under any circumstances, click on any link in the email.

If it is an email in Outlook, click '**Report Message**' and the '**Phishing**' in the top right-hand corner, and move the email to **JUNK**.



If you are not sure, contact us as organisers on a number you know belongs to us, and ask if the email is from us.

If you receive a phone call that appears questionable, say you will call them back. **Check using our PUBLISHED numbers**, which you can find on our website or in the Exhibitor Manual. You can inform Ofcom via Unwanted calls and messages - Ofcom

If the scam is of an extreme nature, please contact us straight away and, if appropriate, the police - Reporting fraud and cyber crime | Action Fraud

What if you have fallen victim to scamming?

If your credit card or bank details are involved, phone your bank **IMMEDIATELY**, and follow up with other relevant parties, including the organiser, after that.

If you have unwillingly signed up for something, such as a directory listing, and are being chased for payment, **don't pay**. You are likely to be threatened with legal action, if you do not pay, but this is very unlikely to materialise and even less likely to be successful. Please inform us so we can offer further advice.

Do not enter into any communication with the scammer.

Inform the Police if you are a business, charity or other organisation which is currently suffering a live cyber attack (in progress). Please call the Police 0300 123 2040 immediately. This service is available 24 hours a day, 7 days a week.

The types of scams you may receive

Dear Exhibitor,

Natural & Organic Products Europe 2023 pre-registered attendees list is available now.

Please pick the number that describes your response:-

1. **Yes interested, send me pricing & other data information.**
2. **Leave-Out**

Regards,

Carol Smith

Event Attendees Specialist |

Natural & Organic Products Europe | 16-17 April 2023 | EXCEL LONDON



Dear Exhibitors - Hope you're doing good.

We have Q1 Offer for you !!

Accountex London 2023 attendee list is available, after our telemarketing and email marketing team approval.

Total register contacts - 5,125

Special offered price: £450 (Regular price: £900), You can avail **50% Flat off** on purchasing the list.

Looking forward for your response. I would be glad to assist you further

Sincerely,

Amy Goodman

Event and Trade Show Coordinator

<https://www.accountex.co.uk/london/>



Scamming unfortunately has become one of the most challenging parts of doing business and whilst we are doing everything, we can to protect you, scammers are always anonymous and incredibly difficult to track down. However, we hope that by following the basic steps outlined here, that you will have a trouble-free, successful exhibition experience. And if you have any questions or if you are ever in doubt, please contact us, as **we take your safety and security very seriously.**

Look out for the following:

- 1 **Email address of sender** – does it look unusual?
- 2 **Subject line** – would you expect to see that type of message?
- 3 **Do you know the person sending the email?**
- 4 **Would we, the organiser, send an offer like this?**
- 5 **Is the style of message in keeping with usual communications?**

If in any doubt, contact us as organisers of the event.

To Summarise:

- ▲ Think before you act
- ▲ If in doubt, contact us as organisers of the event

- ▲ If you fall victim to a scam, take immediate action
- ▲ Be Alert