

THE CHECK BEFORE YOU PAY

Client logins, kept out of the wrong hands.

An agency holds the logins to its clients' websites, ad accounts and social media, and sends each of them an invoice every month. One convincing email to the wrong person can reach all of it.

How it happens here

PRESS CHECK HERE**1. A platform notice arrives**

An email posing as an ad or social platform's policy notice or partner invitation asks the agency to act.

2. A sign-in page

Its link leads to a page that collects the business login and the two-step code.

3. Client accounts are taken

With that login, the criminal controls the client accounts it reaches.

4. Money is asked for

The hacked accounts are then used to ask people for money, in the client's name.

Before any payment to new or changed bank details

- 1 Keep every client login in a password manager, never in email, chat or a shared document.
- 2 Turn on two-step verification on every client account you hold, with an app or security key rather than a text message where the service allows it.
- 3 Treat any email asking you to sign in, accept a partner request or restore access as suspect, and go to the service yourself rather than through the link.
- 4 Tell every client in writing that your bank details will never change by email.
- 5 If a client's bank details change by email, ring them on a number you already hold before paying.

If money has gone

Ring your bank's fraud line at once, then report to Report Fraud on 0300 123 2040 or reportfraud.police.uk (Police Scotland on 101 in Scotland).

Also on day one: tell each client whose account may be affected, change their passwords from a device you trust, and use each platform's own recovery process.

What your sector's own bodies say

- Use multi-factor authentication on every online service the organisation relies on, and prefer the kinds that resist phishing. (NCSC, Multi-factor authentication for your corporate online services, September 2024)
- Fraudsters hack supplier email accounts or create lookalike domains to send fake invoices with updated bank details; confirm the old and new details on a known phone number, not one in the message. (GOV.UK, Stop! Think Fraud: Protect your business, current guidance)

Where Jatzo fits. Jatzo does not replace the call. It helps whoever reads the email notice that it needs one, before anybody pays.

Check the notice before signing in

Anybody unsure about a platform notice or partner request presses Check in Outlook or Gmail and sees a score out of 100 with the reasons.

Your managing director hears at once

When anybody checks a message scoring High risk or above, an email goes to addresses you choose at your own domain, such as your managing director's.

More at jatzo.co.uk/for-teams/marketing-agencies

Training for everyone holding client logins

Business Pro includes every Training Centre course, Protecting your work account among them, for everyone in the team, with a record of who completed it.

Addresses made to look like yours

Domain Watch, on Business Pro, looks for new web addresses registered to look like your agency's, the address a fake invoice to your clients would come from.

UK Finance recorded £41.3 million lost to invoice and mandate fraud across 2,305 cases in 2025, 68% of it from business accounts. Criminals intercept emails or take over an email account, then pose as a supplier, a solicitor or a builder with new bank details. (UK Finance, Annual Fraud Report 2026, June 2026.) Report Fraud replaced Action Fraud in December 2025; the number did not change.