What Educators Need to Know about

INVOICE FRAUD

Invoice fraud, including payment diversion fraud, occurs when criminals deceive you into paying a fake invoice or redirect a genuine payment into their own bank account. Fraudsters may impersonate suppliers, intercept emails, or send convincing invoices to prompt urgent payment into fraudulent accounts. It is one of the most common and costly forms of financial crime affecting individuals, businesses, and schools.

WHAT ARE THE RISKS?

COMMUNICATIONS CLAIMING URGENCY

Communications that claim to be urgent or highlight late payments may be a key sign. Fraudsters often apply pressure to rush decisions and stop checks. Take a moment to verify the request using trusted contacts before making any payment.

CHANGES TO BANK DETAILS

Receiving messages saying a regular supplier has changed their bank account details can be a warning sign. Fraudsters may impersonate contacts to redirect payments. Always verify changes first using known supplier contact details.

DISCREPANCIES AGAINST PREVIOUS INVOICES

Be wary of invoice details that don't match authentic, previously issued invoices, such as amounts, reference numbers or contact names. Fraudsters often alter small details to avoid detection. Always query any differences using your supplier's contact details.

MINOR EMAIL CHANGES

Look out for slight changes to a supplier's email address, such as extra characters or spelling differences. Fraudsters often use similar looking addresses to appear genuine. Always check the sender carefully and verify any concerns using known contact details before responding or making a payment.

UNEXPECTED PAYMENT REQUESTS

Invoices or payment requests for goods or services you do not recognise can be a warning sign. Fraudsters may send false invoices hoping they will be paid without question. Check records and confirm with the supplier before processing any unfamiliar request.

UNUSUAL LANGUAGE OR TONE

Messages with unusual wording, grammar or spelling compared to your usual supplier communications may indicate fraud. Criminals often copy legitimate messages but may not match the usual tone or style. The rise in artificial intelligence (AI) means errors are no longer as common or obvious. Be cautious and verify the request if anything seems out of place.

Advice for Parents & Educators

VERIFY BANK DETAILS

Always confirm any change to a supplier's bank details before making a payment. Use a trusted phone number or a long-standing contact you have used before, not the details provided in the request. This helps ensure you are dealing with a genuine supplier and prevents payments being redirected to fraudsters.

CROSS-CHECK INVOICES

Compare new invoices with those previously issued by the supplier in question. Check key details such as amounts, bank details, reference numbers and contact information. Differences may indicate fraud, so always investigate and verify anything that does not match before making a payment.

DUAL PAYMENT APPROVAL

Ask a trusted person to review and approve high-value payments. A second set of eyes can help spot unusual details or warning signs that might otherwise be missed. This adds an extra layer of control and reduces the risk of errors or fraudulent payments being processed.

REPORT FRAUD QUICKLY

If you suspect fraud, act immediately. Contact your bank using 159 or their official number and report it to Report Fraud online or by calling 0300 123 2040. Keep all emails and documents. For more guidance, or to register for counter fraud alerts, see DfE counter fraud guidance. You can find the invoice fraud leaflet on the National Crime Agency website.

Meet Our Expert

Evan Williams is a counter fraud manager at the Department for Education. Having led the function there for many years, he now focuses on continual improvement, communication, and innovation. He proudly oversaw the growth of the counter fraud team during the pandemic, having worked in counter fraud for 16 years since starting his civil service career with the National Crime Agency back in 2010.

#WakeUpWednesday®

The National College®

See full reference list on our website