The Great Invoice Swindle

Fake Invoices and Financial Fraud

Financial fraud is all around us and the bane of the internet age, but it's nothing new. The earliest recorded economic fraud inscribed on clay tablets, dates back to dawn of civilisation with the Sumerian culture over 7,000 years ago.

We all like to think we're pretty savvy and can spot a scam a mile away, but the increasing sophistication of invoice rip-offs is frightening.

Recent research shows SMEs are losing more than £9bn through invoice fraud every year. Often overlooked is the damage it does to both parties.

The payor will often lose their money with little or no recompense and the payee may receive bad publicity for issuing false invoices. The author certainly knows of several cases where an invoicing scam has proceeded a bankruptcy.

The majority of organisations now present electronic invoices for their customers to pay. The big guys may have invested in EDI or payment portals but these often don't work for the SME.

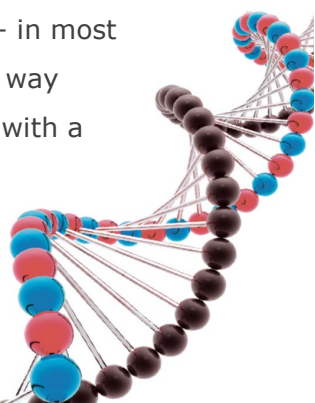
Typically, a company now sends their invoice in a PDF format via email. This makes sense – it saves a fortune in paper and postage costs, plus, it's environmentally friendly. However, this change of technology presents many opportunities for the crook and by using software, a successful fraud can be scaled very quickly to thousands of potential victims.

The common scams

Let's look at a few common frauds:

1. Inflated Invoices – sending invoices for more than the goods or services delivered
2. Duplicate Invoices – sending the same invoice twice and hoping for payment twice
3. False Invoices – creating new or modified invoices with amended payment details

The first two are not uncommon and are generally not the activity of a criminal – in most cases it's caused by a poor invoicing process, or an employee's incompetence. 3 way matching of the invoice to the purchase order and goods received note, coupled with a sound payment workflow process should eliminate these two scenarios.



The 3rd problem of false invoices is a little more worrying. Clever criminals can spend time researching a company's customer base and obtaining copies of real invoices:

- In a simple case, they merely create false PDF invoices with exactly the type of goods a customer would buy, but with their bank details (account code and sort code) rather than the legitimate supplier.
- Further criminal cunning may include a discount for early payment via an electronic hyperlink in the PDF invoice - again, the payment goes straight to the fraudster's bank account.
- Probably the most worrying trend is where an email account is hacked. This allows a crook to intercept real invoices and simply replace the payment information for their own.

Software tools exist which can automatically open and edit thousands of PDFs in a matter of minutes. The fake invoices will contain the right purchase order number and the correct goods and will pass a 3-way matching process. This scam will only fail if a robust accounts payable process is in place which picks up if the invoice has already been paid, or flags the change of bank details. Ideally, any change of bank details should be verified via a phone call directly to the supplier.

Help is at hand

Not all is lost, there are some simple safeguards which will help avoid some of these scenarios:

For the payor:

- Wherever possible always issue purchase order numbers to suppliers.
- 3 way match all invoices against the purchase order and good received note. Software is available to help automate this process to avoid a bottle neck (e.g. ABBYY for Invoices).
- Make sure your financial system or process will pick up duplicate invoices.
- Manually verify all changes to payment details directly with the supplier via a telephone call.

For the payee:

- Take IT security seriously to avoid any loss of data, or the hacking of an email system. Keep update on security patches, run the latest anti-virus/firewall technology and control who has access to passwords and key systems.
- Communicate with your customer to never pay an invoice if the bank details have changed without checking first the validity of the request. Reinforce this with a message on your invoice and via a message in the body of the email.
- If you're sending PDF invoices via email, add another layer of security to the PDF file: switch off the ability to edit the PDF file and only allow viewing, or printing. Consider adding a password or a digital signature at the customers discretion.
- Send digital invoices via a trusted HTTPS hyperlink in the body of the email. This type of delivery mechanism can offer the ability to trace the delivery, which is great for credit controllers and will automatically expire after a period of time - meaning if emails are hacked then most invoices will no longer be available.

Note: Not all financial, or ERP systems can control security of PDF files, or deliver invoices via a traceable hyperlink. Third party software tools, or services exist (e.g. Formate eVo software) which can be rapidly added to an existing invoicing process to implement many of the suggested improvements.

About

Document Genetics is an established UK based company providing a comprehensive range of business automation software.

We focus on improving document automation, workflow and collaboration within our client organisations, and our range of innovative solutions and specialist services help to save time and money by processing documents and data more efficiently.

t: 01604 671177
e: joe.hyde@document-genetics.co.uk
w: www.document-genetics.co.uk

DOCUMENT genetics
business automation software