Invoice Fraud
Factsheet for traders

How to protect your customers
Invoice fraud is a threat to everyone. It involves criminals sending fake invoices to steal money from individuals and businesses.
When you give customers a written quote, warn them about invoice fraud.
We've put together some resources to help you:
- **What to tell a customer about invoice fraud**
- **Postcard to include with their written quote (digital and print version available)**
- **Template quotation which includes advice on avoiding invoice fraud**

Find out more at www.which.co.uk/invoicefraud

What to tell a customer about invoice fraud
Criminals may send you fake invoices, posing as a legitimate business, to trick you into sending them money.
You are more likely to become a victim of this kind of fraud when you are expecting an invoice or payment request from a trader.
If you're paying a business for the first time, or you've received a payment request to a different bank account, confirm that it is genuine before sending any money.
To help protect you, I will include my bank details and a confirmed contact number on every written quotation.
If you accept my services and receive a request to pay a different bank account, please call us – using the number on the original quotation – to confirm we sent it.

Remember:
- **Criminals can impersonate a legitimate business and convince customers to pay into a fraudulent bank account**
- **Always verify change of details with a trusted source.**
- **Where has the invoice come from? Check the email address and contact details.**

If you think you have been scammed
- **Contact your bank immediately**
- **Report to Action Fraud or Police Scotland (if you live in Scotland)**
- **For advice, contact Citizens Advice, Advice Direct Scotland, or Consumerline (Northern Ireland)**

How to protect your business
As a business you may also be targeted.
Criminals can create flashy websites and official-looking emails to impersonate suppliers in an attempt to defraud you.
Spot the following signs:
- **An unusual or unexpected financial request**
- **Poor spelling and grammar or unusual language – it could be translated**
- **No sign-off**
- **Check for the spelling of the company name on the invoice for subtle differences and check the email address carefully (for example .org instead of .com).**

Be wary of links and attachments in emails and keep your guard up– especially if you receive an email you are not expecting. Train any staff to look out for invoice scams.
Ensure your online accounts are protected
Secure your online accounts to keep fraudsters out.
Here are a few top tips:
- **Keep your computer up to date – you will be better protected if you keep the operating system (such as Windows or Mac) updated. You should receive notifications when you need to update the system.**
- **Use the latest version of your internet browser (such as Edge, Chrome and Firefox) – this will help to provide better protection from scams, viruses and other possible threats.**
- **Use security software (for example anti-virus, anti-spyware and firewall) to protect your computer. Some computers already have security software installed, or you can check www.getsafeonline.org for advice on reputable providers.**
- **Use a different, strong password for every online account in case one gets hacked.**

You can use a password manager to help you store your passwords securely – this means you'll only have to remember one strong master password.
- **Enable multi-factor (or two-factor) authentication on your email account. This makes it much harder for someone to hack your account. Read more at www.which.co.uk/2fa**

Has your company been the victim of a data breach?
Company data breaches are quite common. This is where criminals attempt to hack into large databases to obtain personal information about customers and clients, which can put them at greater risk of falling for a scam.
Check the website haveibeenpwned.com to see if your email has been compromised. If your email address has appeared in a data breach, change your password immediately.

For tips on password security visit: www.which.co.uk/pw

Take Five to Stop Fraud

Friends Against SCAMS
www.friendsagainstscams.org.uk

Stop, Challenge, Protect Think about what you are being asked to do, do you have an account with this company? Could this be fraudulent? Contact the company using a phone number or an email that you have used before to ensure that it is a genuine request.