Would you know if you were about to be scammed?

GET SAFE ONLINE .org ®

www.getsafeonline.org

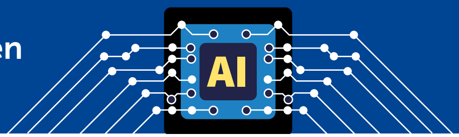
Whether you're first fixing on a new estate, replacing a boiler or changing a tap washer, you always seem to be busy. Earning money and keeping your customers happy is often done at the expense of everyday jobs essential to every business, like admin and finances.

And protecting yourself against fraud.

That's why the plumbing and heating trade is a prime target for fraudsters. Like you, they have a number of different tools to do their work, but theirs include:

- Purchase fraud, where you're tricked into paying for supplies, sundries or tools that don't exist when buying online.
- Payment diversion fraud (aka invoice fraud), where you're tricked into paying regular or one-off payments to suppliers into fraudulent bank accounts.
- Impersonation fraud, where you or an employee receives an email, text or phone call from someone impersonating a supplier or someone else in your business, requesting an urgent one-off payment, bank login details or other confidential information.
- Investment fraud, where you're tricked into investing company or your own money into fake investments, a pension fund or cryptocurrency.
- Ransomware, where your computers are infected by malware and files locked, accompanied by a ransom demand.

And now, many frauds are made even more convincing with the use of AI.



No business can afford to lose money to frauds like these. That's why we've got together with Lloyds Banking Group to put together some top tips to help you protect your business.

- If you're making one-off purchases of supplies, sundries or tools online, always pay by credit card, never by bank transfer. If you can, see the goods in person. Take a moment to think about the advertisement. Does it seem genuine? Does anything seem 'not quite right'? Is it easy to contact the seller to ask questions?
- If you receive an irregular request or instruction for a payment or changing payee bank details, always check with the company, organisation or individual it claims to come from, on a phone number you know to be correct.
- Fraudsters are skilled at gathering information from multiple sources like combing your social media posts and profiles or setting up bogus websites inviting you to submit confidential details. Always be careful about what details you share on any website/app and even social media, dating or gaming platforms. This includes information about your customers, employees and subcontractors.
- Choose, use and protect passwords carefully, with a different one for every online account. Using three random words and adding capitals, numbers and symbols is a good way to start.
- Always download software, app and operating systems updates when prompted. Better still, set your systems and programs/apps to download updates automatically.
- Reputable internet security (antivirus) software and apps should always be loaded, kept updated and switched on.
- Don't click on attachments, or links in emails, texts or WhatsApp messages or on social media unless the source is 100% known and trustworthy. Check if a website is likely to be legitimate or fraudulent at **www.getsafeonline.org/checkawebsite**.
- It's a good idea to make sure new and existing employees, apprentices and subcontractors are aware of this advice by means of regular communication on online safety and fraud prevention. Plus, if you work with other trades, help them to protect themselves too by sharing our advice.

If you've been scammed, report it to your bank immediately, then to Report Fraud at **www.reportfraud.police.uk** or on **0300 123 2040**.

Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by law enforcement agencies and leading organisations in internet security, banking and retail.

For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit **www.getsafeonline.org**

If you think you have been defrauded, report it to **Report Fraud** at **www.reportfraud.police.uk** or by calling **0300 123 2040**.
If you are in Scotland, contact **Police Scotland** on **101**.

GET SAFE ONLINE .org ®

www.getsafeonline.org

OFFICIAL PARTNERS

airbnb
BARCLAYS
barclaycard
UK International Development
Partnership | Progress | Prosperity
ARMY BE THE BEST
LLOYDS
HALIFAX
BANK OF SCOTLAND
viagogo
Llywodraeth Cymru
Welsh Government

Report Fraud
METROPOLITAN POLICE
NPCC National Police Chiefs' Council
HEDDLU GOGLEDD CYMRU
NORTH WALES POLICE
NATIONAL TRADING STANDARDS
Protecting Consumers
Safeguarding Businesses
Renfrewshire Council
Ofcom
cifas Fighting Economic Crime Together
VS VICTIM SUPPORT
neighbourhood ALERT
TAKE FIVE TO STOP FRAUD
NEIGHBOURHOOD WATCH 1982 - TODAY