Energy UK

The voice of the energy industry

Guide: Helping energy customers stay vigilant against social engineering fraud

November 2025

This guide seeks to help energy customers avoid social engineering fraud by offering simple steps to stay alert, verify contacts, and protect personal information. It also includes real-life examples from energy customers who have acted to protect themselves.

Read our explainer for more information about social engineering fraud.

Quick tips for when you suspect someone is trying to trick you

- If it is a telephone call, hang up immediately. Note the number.
- If it is a suspicious WhatsApp message, text message or email, do not click on any links.
- If the person you are suspicious of has come to your door, do not let them in until you have confirmed their identity by looking at their work identification. People may use fake ID so ff you are still unsure, contact your energy supplier directly.
- However you have been contacted, get in touch with your energy supplier, or the company the person is representing, independently using the details on your energy bill or on the supplier's official website.
- Report a suspicious phone call or message to your energy supplier and to Action Fraud (the UK's national fraud reporting centre) and block the caller's number. Call Action Fraud on 0300 123 2040 or visit https://www.actionfraud.police.uk/.

Anyone who approaches you for legitimate reasons will give you time to check that they are who they say they are. They want you to keep you and your personal information safe.

Other ways to protect yourself

Managing your energy account

Energy customers should check bills regularly for errors or unexpected charges. If you are concerned, get in touch with your supplier using the contact details on your energy bill or other official correspondence from them – or their official website as it comes up on an independent internet search.

Energy customers should use secure payment methods and avoid transferring money via links in emails or texts. Energy suppliers have processes in place to help customers pay only through secure methods that protect the customer.

When registering an email address with your energy account online, try to use one that you have not shared publicly. Be careful of the personal information you share online as scammers can harvest this information to try to access your accounts.

Checking the identity of someone who says they are an energy supplier

There are various ways energy customers can do identity checks when they are contacted by someone saying they are a supplier.

- If you get a home visit from someone who says they're there to work at your property – for example, to install or inspect something:
    - The person should be carrying visible identification such as an ID badge, and they are likely to be wearing the supplier's uniform. Call your supplier using the number on your bill or on their website to check that the person is their representative.
    - You can also ask your supplier to arrange with you for their staff to use an agreed password when they visit you or call you so that you know it is really the supplier. You can also request this for friends and family.

- If you receive a phone call from someone saying they are from your supplier or they represent your supplier and you feel something is not right, you can protect yourself by:
    - Not sharing account numbers, passwords, or payment details until you have checked the caller's identity independently and that they are legitimately calling you for the reason they gave you.
    - Asking the caller's full name, their department or the team they work on as well as the reason they have called you.
    - Hanging up then calling back on the energy supplier's official customer service number listed on your energy bill or the supplier's website.
    - Being wary if the caller tries to pressure you urgently – for example, by claiming your energy supply will be cut off shortly, or that you must act immediately to secure a price. They may say there's no time for you to check for yourself independently with the energy supplier.

- If you receive a WhatsApp or text message claiming to be from your supplier and you feel something is not right, take your time to check:
    - If the message addresses you by name as the energy account holder (or someone you have nominated to represent you) and has a reference number you can check independently with your supplier.
    - If the sender's number is listed on the supplier's website or one you know they have used before. You can call your supplier on the phone number included on your bill.

  - If the sender uses a green business account checkmark on their WhatsApp profile ID – something a genuine company is more likely to do.
  - If the language includes poor grammar, spelling mistakes, odd phrasing or urgency and threats. This could be a sign of a scam.

- You can protect yourself by:
  - Not sharing your account numbers, passwords, or payment details.
  - Avoiding clicking on suspicious links straightaway. Use a search engine to find the web page the message is trying to get you to go to.
  - Using the contact details on your bill or the supplier's official website to ask them if they messaged you and what they wanted to tell you.

- Taking seriously any warnings from the messaging service provider that the message you received could be a scam or that suspicious activity has been detected.

These precautions also apply to emails, which are more likely to have an official reference number that you can double check by calling your supplier.

- If you receive an email looking like it is from your supplier, you can examine it more carefully to see if it is a threat by:
  - Checking the domain name (the words after the @) that the email has been sent from. Energy suppliers do not use generic email accounts such as Gmail, Outlook or Yahoo. to send emails.
  - Making sure that none of the characters in the domain name have been modified or misspelled to make it look like the email has been sent by a genuine supplier (e.g. scottishp0wer; briitishgas etc).
  - Hovering over any links provided to make sure the web address isn't modified or misspelled
  - Reviewing whether the email is addressed to you personally or uses an impersonal greeting that could be used by someone who doesn't know who you are.
  - If in any doubt, contacting your supplier directly using the contact details on your bill or the supplier's website to confirm that they tried to contact you and asking why.

Real-life stories

These are real situations where energy customers successfully avoided becoming victims of social engineering. These customers spoke with their supplier after they had been contacted by someone whom they were not sure about, and the supplier was able to confirm that the contact from that person was not legitimate.

- An individual pretending to be an energy supplier called trying to get the customer to switch suppliers. The customer became suspicious when the person asked for their Direct Debit information before even discussing the energy price tariff options available if they switched suppliers. When the customer told their supplier about this, the supplier confirmed the contact had not come from them.
- An energy customer avoided being tricked into sharing their bank details. Someone pretending to be their energy supplier tried to get them to set up a payment plan for arrears on their energy account. As the customer regularly checks the status of that account and knew they were in credit, they suspected the contact was not legitimate and contacted their energy supplier to check. The supplier confirmed they had not been trying to get in touch with the customer and that they were correct about the status of their account.
- An energy customer received a call from someone pretending to be their supplier wanting to discuss switching their tariff despite the customer only recently having done so. The customer grew suspicious and did not continue the conversation. When they told their supplier what happened, the supplier confirmed that the contact was not legitimate as they had not reached out to the customer.
- An energy customer avoided being tricked into sharing personal details. They were contacted by an individual who told them there was incorrect energy information about them on a national database, which needed to be updated with their correct personal details. The customer called their supplier, which confirmed that energy customers would not be asked for their personal details in this way.
- Someone pretending to be the customer's energy supplier called a customer on a Saturday morning and tried to get the customer to chat with them on WhatsApp. The customer knew they don't usually chat with their supplier on WhatsApp so they used the main contact details they had for their energy supplier to ask if this contact was from them. The supplier confirmed this was not the case and the customer did not continue speaking to the person.

Remember!

Report a suspicious phone call or message to your energy supplier and to Action Fraud, and block the caller's number.

Call Action Fraud on 0300 123 2040 or visit https://www.actionfraud.police.uk.

About Energy UK

Energy UK is the trade association for the energy industry, representing companies investing billions of pounds to secure our country's current and future energy needs. From growing start-ups to major electricity generators, grid and infrastructure developers and energy suppliers, our members are driving change across power, heat, transport and flexibility.

We champion initiatives such as our Vulnerability Commitment, which pushes suppliers to go beyond regulation to support customers with additional needs, and TIDE, the industry's drive for greater inclusion and diversity. Through our Young Energy Professionals Forum, with more than 3,000 members representing 350 organisations, we support the development of future leaders.