

**Action Fraud** is warning the public about a sharp rise in reports relating to fake emails purporting to be from Ofgem, the independent energy regulator for Great Britain. The emails claim that the recipient is due a rebate payment as part of a government scheme and provides links for the recipient to follow in order to apply for the rebate. The links in the emails lead to malicious websites designed to steal personal and financial information.

**Between Monday 22nd August 2022 and Monday 5th September 2022, a total of 1,567 phishing emails related to this scam have been reported via the Suspicious Email Reporting Service (SERS).** All the emails display the email subject header “Claim your bill rebate now”. Offenders are using the Ofgem brand logo and colours to make the emails look as authentic as possible. However, the emails ask recipients to “apply for an energy bill rebate before September 2020”, which is what prompted many recipients to realise the emails weren’t genuine.

You can view examples of the fake emails in our social media posts on [Twitter](#), [Facebook](#) and [Instagram](#).

### **How you can protect yourself and others**

- If you have any doubts about a message, contact the organisation directly. Don’t use the numbers or address in the message – use the details from their official website. Remember, your bank (or any other official source) **will never ask you to supply personal information via email.**
- If you have received an email which you’re not quite sure about, forward it to [report@phishing.gov.uk](mailto:report@phishing.gov.uk). Send us emails that feel suspicious, even if you're not certain they're a scam - we can check.

For advice on how to stay secure online, please visit: [www.cyberaware.gov.uk](http://www.cyberaware.gov.uk)