

# SCAM

# WARNING

## EE Smishing Scam

One of our Facebook followers has kindly alerted us to this smishing message he received purporting to be from EE. As our informant is a customer of EE, he did the right thing and contacted their customer services separately, using a number he knows to be correct, to check whether this was a genuine communication. EE confirmed it was not and is a scam.



The text came from 07399 852738 and reads '**EE: we are unable to process your latest bill. In order to avoid restrictions please update your billing information via: <https://www.eebilling-updated.com>**'

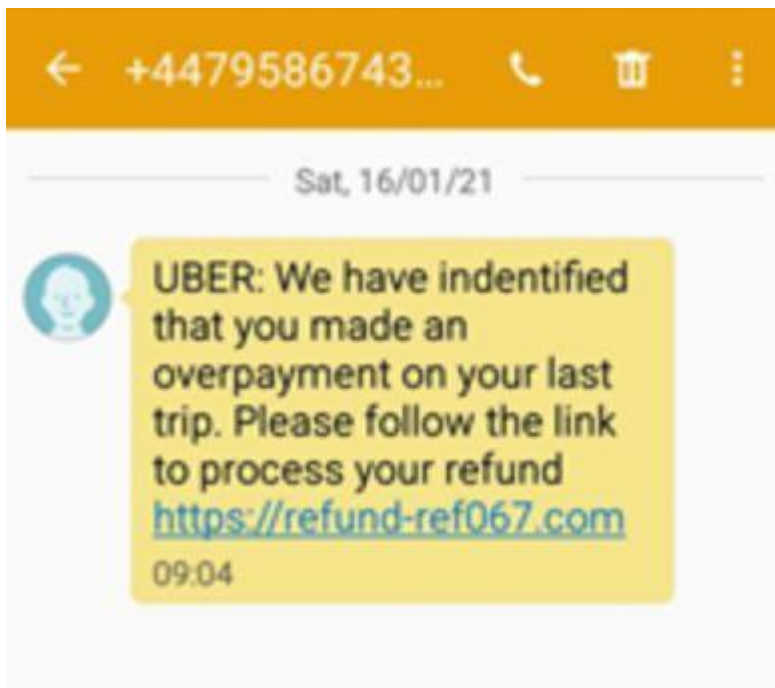
As with all smishing texts, this message is a trick to get the recipient to click on the link to give some personal information or to unknowingly install some malware (malicious software) on their device. Malware can give the scammer access to your device where they can steal lots of personal information for identify theft and can steal from your online banking accounts.

Please warn all your contacts about smishing texts - they are very common, come in many different guises and can be very convincing. Passing the message on could save someone from a lot of distress.

Suspicious texts should be forwarded to 7726, free of charge.

---

The text came from 07399 852738 and reads 'EE: we are unable to process your latest bill. In order to avoid restrictions please update your billing information via: [https://www.eebilling-updated\(dot\)com](https://www.eebilling-updated(dot)com)'



As with all smishing texts, this message is a trick to get the recipient to click on the link to give some personal information or to unknowingly install some malware (malicious software) on their device. Malware can give the scammer access to your device where they can steal lots of personal information for identify theft and can steal from your online banking accounts.

Please warn all your contacts about smishing texts - they are very common, come in many different guises and can be very convincing. Passing the message on could save someone from a lot of distress. Suspicious texts should be forwarded to 7726, free of charge. The text was sent from a mobile telephone number and reads

**'UBER: We have identified that you made an overpayment on your last trip. Please follow the link to process your refund [https://refund-ref067\(dot\)com](https://refund-ref067(dot)com)'**

As with the EE message above, this message is bogus and is just a ploy to trick you into inputting personal information or installing malware to your device.

Smishing messages are usually sent on a large scale to ensure that some of the recipients will be customers of the organisation being mimicked. And in turn the scammers may receive responses from a proportion of those customers who don't spot that it's a scam.

Many people receive messages purporting to be from companies that they do not deal with and will immediately recognise them to be fake. But where you are a customer of the company in question it can be difficult to know whether to ignore the message or whether you must act.

The simple advice is to **never click on a link in a text message that you were not expecting**. If you are a customer of the company in question and you are not sure about the communication, always contact them using a number, e-mail address or chatbot you know to be correct to find out if the message is genuine. Remember the link given in a text message might look like a genuine web address but it is very easy for fraudsters to give a link a false identity in their communications.

Forward suspicious texts to 7726, free of charge.

Please share to help others stay safe.

---

**RG Note All links disabled....**