

DVLA warns customers to stay safe online



Scam emails and text messages

We don't send emails or text messages that ask you to confirm your personal details or payment information, such as for a vehicle tax refund. If you get anything like this, don't open any links and delete the email or text immediately.

Misleading websites

Beware of misleading third party websites passing themselves off as DVLA. These sites might, for example, offer to help you apply for a driving licence, tax your car or connect you to our contact centre. These sites will often charge additional fees for [services that you can get for free or at a lower cost](#) on GOV.UK.

To try and pass themselves off as genuine, these sites might include 'DVLA' in their web address (URL). They might also design their site to appear as if it's DVLA – for example, using DVLA's old 'green triangle' logo, which we no longer use.

Don't be fooled by these sites – even if they appear at the top of search engine results. Always [double check](#) you're using GOV.UK.

Top tips to protect yourself and others

Only use GOV.UK so you can be sure that you're [dealing directly with DVLA](#).

Never share images on social media that contain personal information, such as your driving licence and [vehicle documents](#).

Report phishing emails to the [National Cyber Security Centre](#).

Report online scams to [Action Fraud](#).

[Report misleading adverts](#) to search engines.

Keep up to date with internet safety – read more about [online scams and](#)

[phishing](#), and how to [stay safe online](#).

Published 6 February 2018

Last updated 21 April 2020 [+ show all updates](#)

1. 21 April 2020

We have added a link to report phishing emails

2. 30 August 2018

Added translation

3. 6 February 2018

First published.