MOTORS CAZOO

Stay safe from scams - here's what to look out for

Phishing is a common and fast-growing type of online fraud.

It usually involves fake messages sent by email, text, or social media designed to trick you into giving away personal information. In the case of MOTORS, this would relate to your **Dealer Centre login details** which might also be your email login too.

The good news? With a little awareness, phishing is easy to spot and avoid. Here's how to stay one step ahead.

What can you trust?

Only enter your Dealer Centre login details at this official MOTORS address: **dealercentre.motors.co.uk**

Emails from MOTORS will always come from one of these domains:

- **@motors.co.uk**
- **@partners.motors.co.uk**
- **@mail.motors.co.uk**
- **@info.raccars.co.uk**
- **@info.motors.co.uk**
- **@news.motors.co.uk**
- **@info.ebaymotorsgroup.co.uk**
- **@info.autoexposure.co.uk**

What are the red flags?

Watch out for these signs that something isn't right:

- **Requests for login details**
  MOTORS will never ask for your password.
- **Lookalike email addresses**
  Scammers often change one small detail to mimic a trusted address.
- **Poor spelling or grammar**
  Many phishing messages contain mistakes — a classic warning sign.
- **Unexpected links or attachments**
  Don't click or download unless you're 100% sure it's safe.

What to do if you spot a phishing attempt

If you've received something suspicious:

1. **Don't click on anything**
   Don't open links or reply to the message.
2. **Forward it to us**
   Send it to: **support@motors.co.uk**
3. **Delete the message**
   Once forwarded, remove it from your inbox.
4. **Update your passwords**
   Change your Dealer Centre and email passwords immediately. (Use strong, unique passwords for each).

Still unsure?

If something doesn't feel right, we're here to help:
Call us: **0333 038 2050**
Email us: **support@motors.co.uk**