Watch out for the latest Royal Mail parcel scam.

A new swathe of scam emails purporting to be from Royal Mail is doing the rounds. The official-looking emails claim that a package has been seized by HMRC upon arrival into the UK and that you need to declare them genuine so that they can be returned to you. All you need to do is click a link to a document.
As you might have guessed, this link will install malicious software on your computer designed to steal personal details like account names, email addresses and passwords.

What you should look out for

This is an example email provided by Action Fraud:

'Your parcel has been seized. Royal Mail is sorry to inform you that a package addressed to you was seized by HM Revenue & Customs upon arrival into the United Kingdom.
A close inspection deemed your items as counterfeit and the manufacturers have been notified. If your items are declared genuine then they will be returned back to you with the appropriate custom charges.
You may have been a victim of counterfeit merchandise and the RM Group UK will notify you on how to get your money back. ..etc…etc….'

To help spread the virus, the emails say "you will need to have access to a computer to download and open the Zip file." But it goes without saying that you shouldn't click the Zip file or any other attachments!

How to avoid falling for these scams

The best advice we could give you is to just be careful – unsolicited emails that ask you to download attachments or pass on personal details are sure fire signs of a scam. Keep a look out for poor spelling and grammar too.