



Your checklist for **Spotting Scams**

97%

*of Scots experienced
a scam last year*

You're scrolling through your phone and suddenly, there it is: a scam masquerading as something totally innocent. It could be an email, a text message, a social media friend request, or even an enticing online advert.

This is called “**phishing**”. This is when scammers are trying to get their hooks into your personal information, and it usually starts by getting you to click a link. Phishing is the most common way that online scams start.

What can you do to stay ahead of the scammer? Well, the best thing you can do is learn how to spot a scam.

Look out for these telltale signs. If you spot these, you should be suspicious.



Authority:

Is the message claiming to be from someone official? For example, your bank, your doctor, a solicitor, the government; a friend or family member. Criminals often pretend to be important people or organisations to trick you into doing what they want.



Urgency:

Are you told you have a limited time to respond (telling you to reply ‘within 24 hours’ or ‘immediately’)? Criminals often threaten you with fines or other negative consequences, like saying your account will be closed. They want to pressure you to act quickly!



Emotion:

Does the message make you feel something? It might make you panic or be worried about losing money. Or it might make you feel flattered or curious—“who is that beautiful stranger that wants to chat”? Not every scam looks the same, criminals can sound threatening, or they might pretend to want to help you.

AMAZON SCAMS  Scam calls saying that there have been issues with your Amazon Prime subscription or account.	PRIZE DRAW SCAMS  Emails or adverts that mimic big brands, promising prizes if you enter your details in a survey.	BANK SCAMS  Pretending to be your bank, attempting to obtain account details or transfer money.
COST OF LIVING SCAMS  Scam emails, texts and calls related to cost of living support payments or bill rebates.	REMOTE ACCESS SCAMS  Scam calls requesting access to your computer to fix a 'problem' or asking you to download software.	INVESTMENT SCAMS  Adverts or emails offering amazing investment opportunities or quick and easy loans.
HRMC SCAMS  Scams offering Government grants, tax refunds, or say your NI number is going to be suspended.	ONLINE SHOPPING  Adverts that lead to scam websites offering non-existent, cheap, or luxury products.	BROADBAND SCAMS  Purportedly from your broadband provider or phone company, trying to get your account details.
ONLINE SHOPPING SCAMS  Messages often beginning with "Hello Mum/Dad" from someone posing as a family member asking for an urgent money transfer.	DELIVERY SCAMS  Pretending to be delivery companies asking you to click a link to rearrange a missed delivery or pay a fee.	ENERGY GRANT SCAMS  Cold calls and adverts giving misleading information about grants or funding boilers or insulation.

79%

of people avoided a scam after reading about it

Have you seen any of these?

Scammers are always on the lookout for new ways to make their phishing scams more effective by adapting to the latest news and trends to make their scams more convincing.

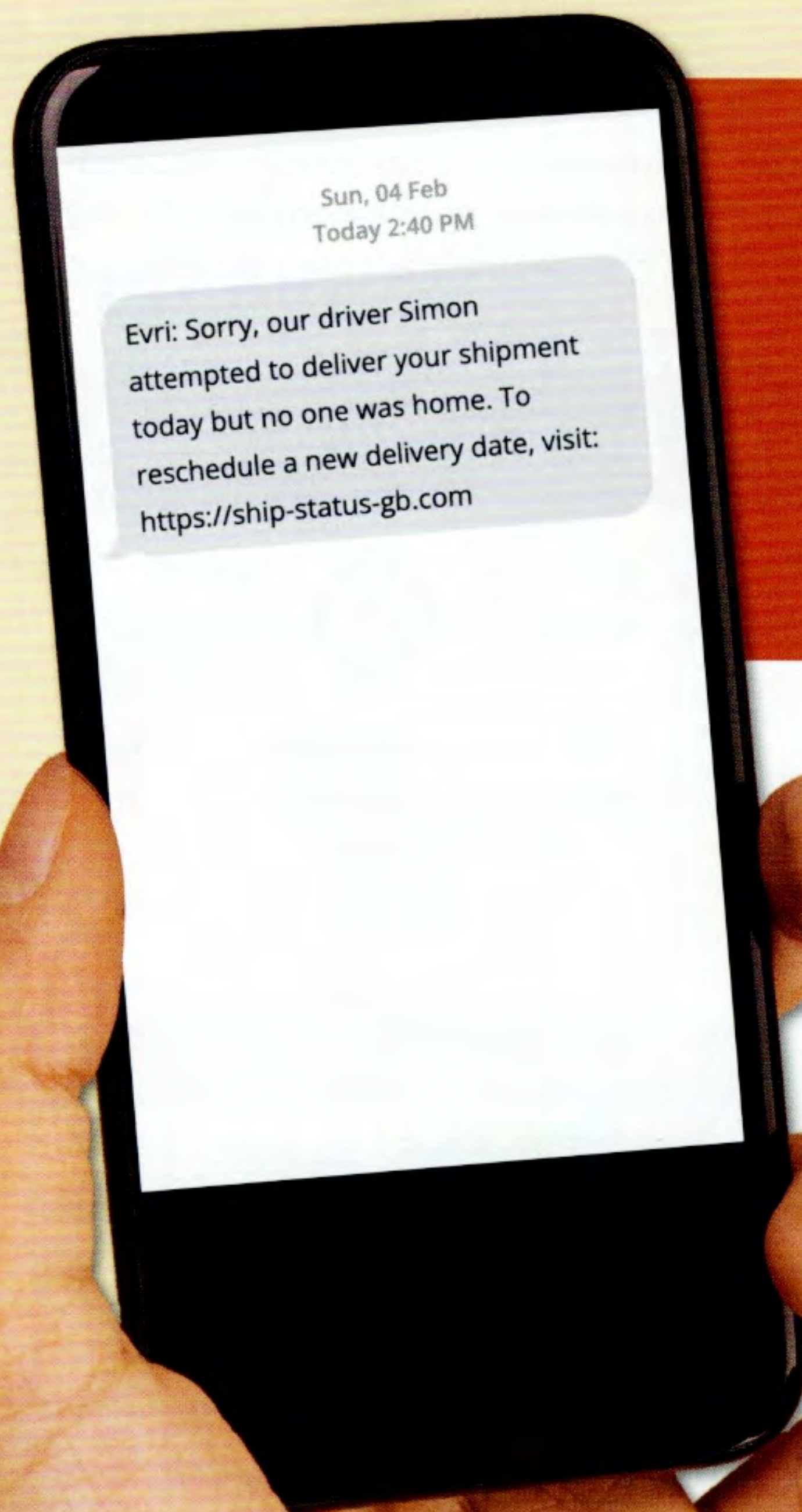
Spot the Scams

Let's use our checklist to help spot the scam! Craig shows us how in these examples.



Craig is a security specialist who teaches people the best ways to stay safe online.

“Track your parcel using the company’s official website or app.”



The Delivery Scam:

This scam text links to a malicious website with official-looking branding and logos, where you are asked to enter your contact details and pay a fee for storage or redelivery. Legitimate parcel delivery companies will not contact you unexpectedly to ask for personal information or payment.



Authority:

They're pretending to be from Evri, the delivery company.



Urgency:

If you think you've missed a delivery, you'll want to rearrange it quickly.



Emotion:

The criminals know you might be curious about what's being delivered, so you're more likely to click on the link to find out.

Forward suspicious emails to **report@phishing.gov.uk**
Forward scam texts to **7726**

“If in doubt, contact the person or organisation directly.”

The Bank Scam:



Authority:

Criminals often mimic organisations we trust to trick us, like posing as a bank. They’re using the correct logos and the email looks genuine.



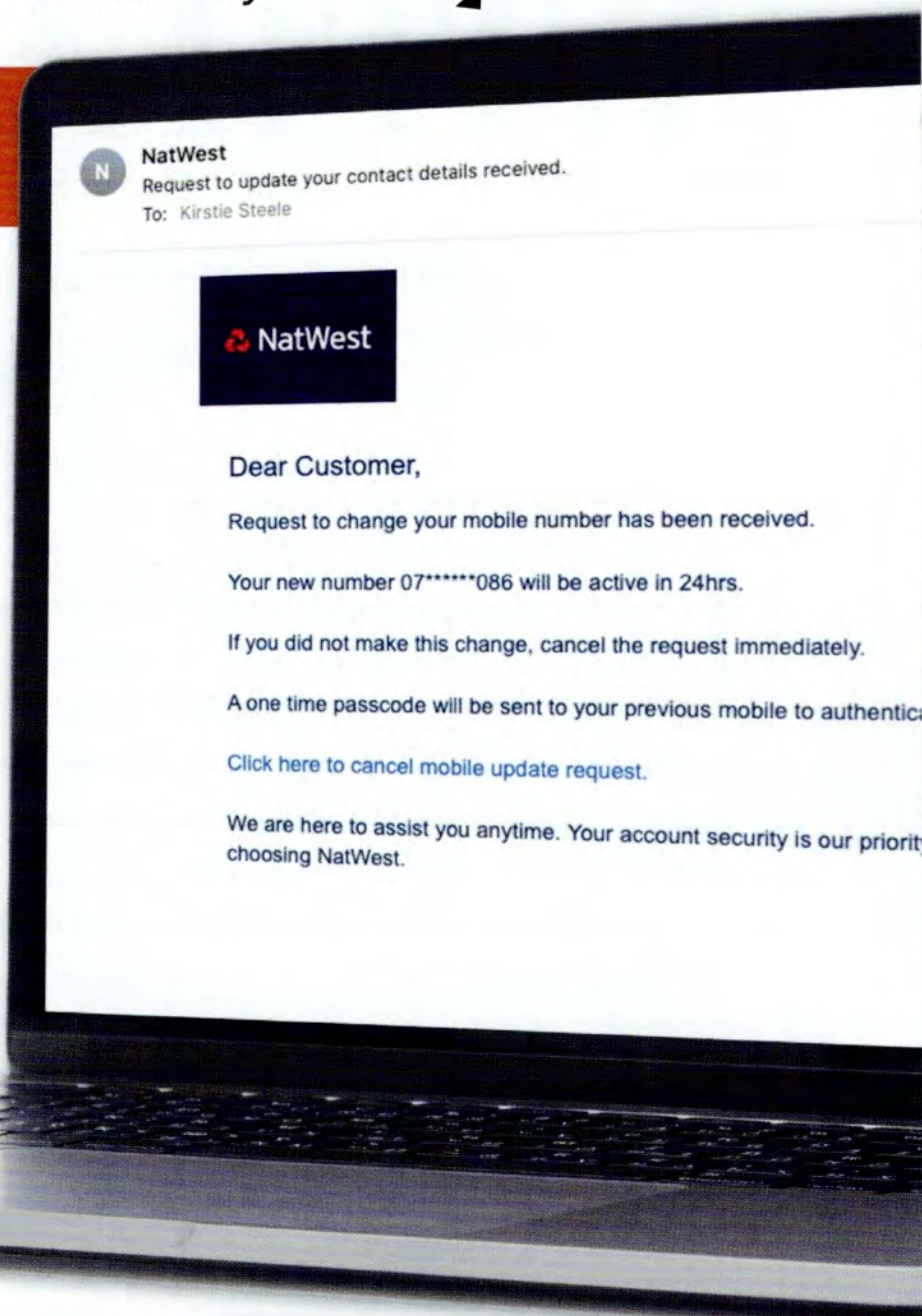
Urgency:

The scammers are trying to rush you to respond by setting a 24-hour deadline before your contact details are changed.



Emotion:

You’d feel panicked seeing this. You’d worry about your account’s security and want a quick resolution. The criminals know if you’re feeling like that, you’re less likely to think clearly.



The WhatsApp Scam:



Authority:

In this WhatsApp scam, the criminal is pretending to be your daughter and asking for help with money.



Urgency:

It says an invoice needs to be paid by noon. The scammer is pressuring you to act quickly by setting a deadline.



Emotion:

Criminals often exploit our desire to help and trust people. We are more likely to respond to messages from friends or family.

