Can you spot a scam?

Most of us can't all of the time - that's how the scammers make money.

Take our quiz to find out if you can.

Click on the  and  symbols to move through the quiz

Halton Trading Standards

Email scam

NatWest Helpful Banking

Your latest statement is available online

Just to let you know that your latest card statement is available. **Click here** to Log In to Online card services then select Statements.

Don't forget to check your transactions regularly and please remember we'll never ask you for your PIN and Password by email.

Don't hesitate to call us if you have any queries, but please do not respond to this email. You'll find phone numbers for all of our services in the 'contact us' section of natwest.com.

Internet support team

Disclaimer
This email was sent from a notification-only address that does not accept email replies. Please do not reply directly to this email. Many internet users have recently been targeted through bogus emails by fraudsters claiming to be from the bank. These emails ask customers to provide their internet banking security details in order to reactivate their account or verify an email address. Please be on your guard against emails that request any of your security details. If you receive an email like this you should not respond. Please remember that, for security reasons, apart from when you create them at registration or when you change your Internet PIN or Password, we will only ever ask you to enter random characters from your Internet PIN and Password when you logon to this service. We would never ask you, by email, to enter (or record) these details and we would therefore request that you do not respond to emails asking for this information.

Legal Information
This email message is confidential and for use by the addressee only. If the message is received by anyone other than the addressee, please delete the message from your computer. Internet emails are not necessarily secure. National Westminster Bank plc does not accept responsibility for changes made to this message after it was sent.

Whilst all reasonable care has been taken to avoid the transmission of viruses, it is the responsibility of the recipient to ensure that the onward transmission, opening or use of this message and any attachments will not adversely affect its systems or data. No responsibility is accepted by National Westminster Bank plc in this regard and the recipient should carry out such virus and other checks

Can you guess the scam?

How it works

By clicking the link in the email the Scammer will take you to their website which they've created to look like the real thing.

When you log in, you will give them the information they need to log into your online account.

They know you bank with Natwest and have an online account because you have responded to their email.

People get caught out because:

- The bank's logo is on the email
- The email 'From' address looks like it's from the bank – hover the mouse over the address to display the address of who who it's really from
- The email provides a link to log in to the Natwest website – but is it?
- The email provides a link to the 'contact us' section of the Natwest website – but is it?
- You have an online account with the bank and are used to getting emails to say your statements are available
- The email contains Legal Information, a disclaimer and a warning about scam emails
- You're busy/distracted so you don't look at the email carefully

How it works

NatWest Helpful Banking

Your latest statement is available online

www.scamsareus.co.uk

Just to let you know that your latest card statement is available. Click here to Log In to Online card services then select Statements.

Don't forget to check your transactions regularly and please remember we'll never ask you for your PIN and Password by email.

Don't hesitate to call us if you have any queries, but please do not respond to this email. You'll find phone numbers for all of our services in the 'contact us' section of natwest.com.

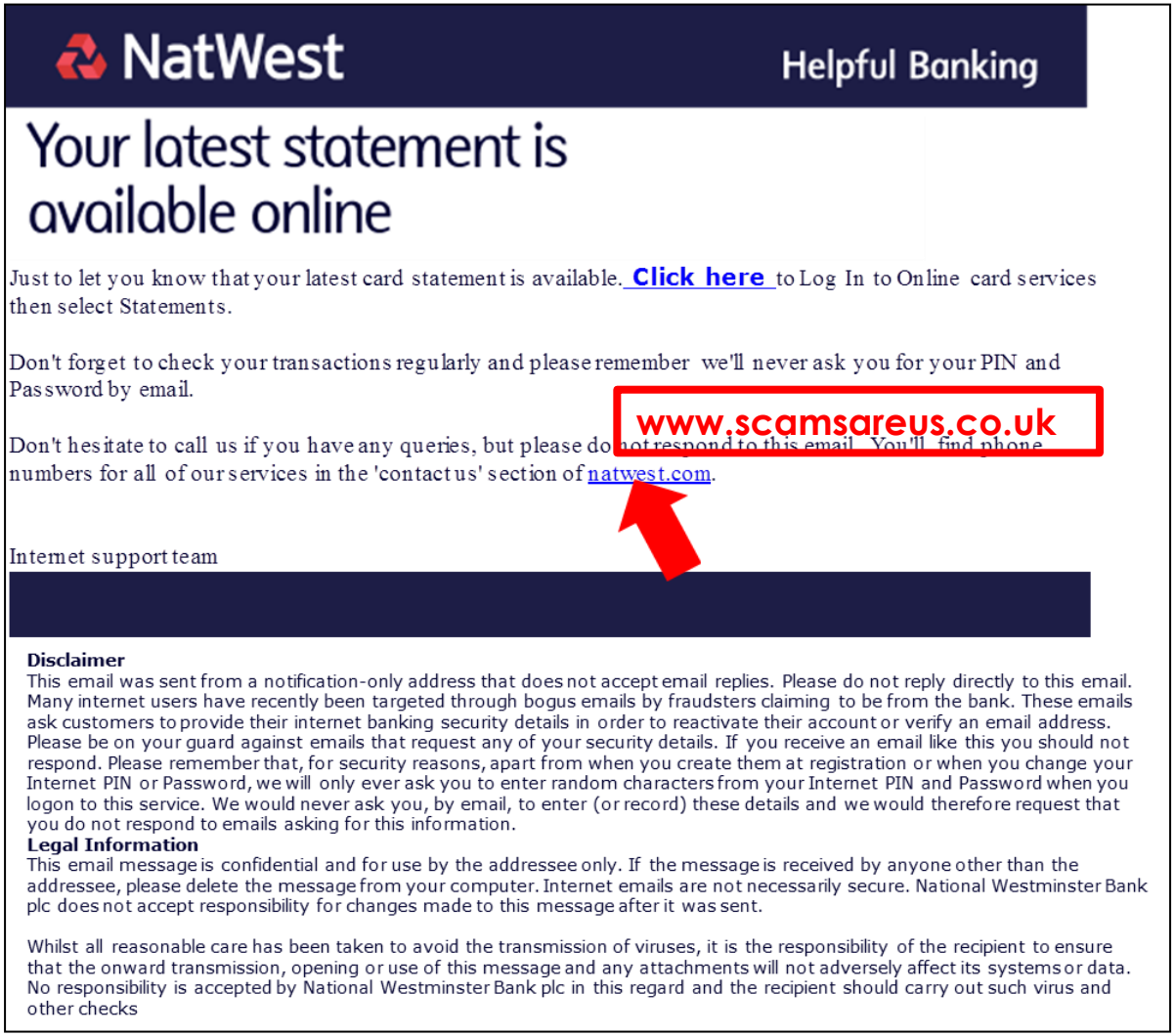
Internet support team

Disclaimer
This email was sent from a notification-only address that does not accept email replies. Please do not reply directly to this email. Many internet users have recently been targeted through bogus emails by fraudsters claiming to be from the bank. These emails ask customers to provide their internet banking security details in order to reactivate their account or verify an email address. Please be on your guard against emails that request any of your security details. If you receive an email like this you should not respond. Please remember that, for security reasons, apart from when you create them at registration or when you change your Internet PIN or Password, we will only ever ask you to enter random characters from your Internet PIN and Password when you logon to this service. We would never ask you, by email, to enter (or record) these details and we would therefore request that you do not respond to emails asking for this information.

Legal Information
This email message is confidential and for use by the addressee only. If the message is received by anyone other than the addressee, please delete the message from your computer. Internet emails are not necessarily secure. National Westminster Bank plc does not accept responsibility for changes made to this message after it was sent.

Whilst all reasonable care has been taken to avoid the transmission of viruses, it is the responsibility of the recipient to ensure that the onward transmission, opening or use of this message and any attachments will not adversely affect its systems or data. No responsibility is accepted by National Westminster Bank plc in this regard and the recipient should carry out such virus and other checks

How it works



NatWest Helpful Banking

Your latest statement is available online

Just to let you know that your latest card statement is available. **Click here** to Log In to Online card services then select Statements.

Don't forget to check your transactions regularly and please remember we'll never ask you for your PIN and Password by email.

www.scamsareus.co.uk

Don't hesitate to call us if you have any queries, but please do not respond to this email. You'll find phone numbers for all of our services in the 'contact us' section of natwest.com.

Internet support team

Disclaimer
This email was sent from a notification-only address that does not accept email replies. Please do not reply directly to this email. Many internet users have recently been targeted through bogus emails by fraudsters claiming to be from the bank. These emails ask customers to provide their internet banking security details in order to reactivate their account or verify an email address. Please be on your guard against emails that request any of your security details. If you receive an email like this you should not respond. Please remember that, for security reasons, apart from when you create them at registration or when you change your Internet PIN or Password, we will only ever ask you to enter random characters from your Internet PIN and Password when you logon to this service. We would never ask you, by email, to enter (or record) these details and we would therefore request that you do not respond to emails asking for this information.

Legal Information
This email message is confidential and for use by the addressee only. If the message is received by anyone other than the addressee, please delete the message from your computer. Internet emails are not necessarily secure. National Westminster Bank plc does not accept responsibility for changes made to this message after it was sent.

Whilst all reasonable care has been taken to avoid the transmission of viruses, it is the responsibility of the recipient to ensure that the onward transmission, opening or use of this message and any attachments will not adversely affect its systems or data. No responsibility is accepted by National Westminster Bank plc in this regard and the recipient should carry out such virus and other checks

Postal scam

LOTTO 01 18 DE 27 ORO 44

Lotto de Oro 2014
45 Avenida de Lorca 28004 Madrid

CONGRATULATIONS!

The Spanish Lottery Corporation is delighted to inform you that you have won €500,000 (five hundred thousand euros)!

Why have you won? Your address was randomly selected by our new Java-based 'Golden Ballot' software. You are a very lucky person, we congratulate you on your victory! You should keep your good luck a secret in order to ensure security of verification.

This correspondance officially confirms that we are in receipt of instructions relating to the payment of your winnings. Please forward the following details to our official claims agent's email address so that he can release your funds without delay.

- Full name
- Country
- Age
- Gender
- Telephone Number
- Occupation
- Passport number

Please do this as soon as possible as a delay will mean that we will have to pick another winner.

Claims agent contact details:
Processing manager: Mr Ian Brown
Email: spanishlotteryagent@hotmail.com
Phone: 07023 449329

Congratulations again from all the staff's here, and thank you for being part of our programme.

Yours sincerely,

Sarah Johnson (Admin Secretary)

Can you guess the scam?

How it works

The scammers want your personal information – if you give them the information they ask for they can steal your identity.

People get caught out because:

- The letter uses an official looking logo
- It gives the names of individuals and their contact details
- You're not asked to pay anything or ring a premium rate number
- They tell you that if you don't act quickly they will choose another winner
- It gives you hope

<u>If you haven't bought a lottery ticket then you cannot win a lottery</u>

Phone scam

INITIAL CONVERSATION

Hello, this is your bank calling. We have identified fraudulent transactions on your account and believe your card has been compromised. Please verify this by calling the number on the back of your card straight away.

NEXT CALL

Hello, thanks for calling so quickly sir. I'm a dedicated fraud investigation officer and I'll be helping secure your account. I just need to confirm a few final security details so we can prevent any further fraud. Please tell me your full name, date of birth and address. We would like to confirm your current card details and PIN. You also need provide us with the details of any other accounts you hold with us so we can ensure these are safe. We will be sending a courier shortly to collect your card and issue a replacement. Please place it in an envelope – your reference for this collection is XG213.

COURIER CONVESATION

Hi, please sign here. The bank will send a replacement by special delivery today so you will have your new card very shortly.

Can you guess the scam ?

How it works

Your bank is telling you that your card has been used fraudulently. When you put the phone down to ring the bank, the scammer doesn't terminate the call - you can't call anybody else.

When you dial your bank you are still connected to the scammer who answers your call to the bank. You give your personal information. The courier collects your card - the scammer has all the information they need and your card.

People get caught out because:

- You believe the initial call is from your bank
- You are alarmed/distressed by what the caller says
- You want to act quickly to prevent further loss
- You are asked to phone the bank on their published number so you think this is a security measure
- You are given a reference number for when the courier calls to collect

Your bank will never send a courier or a police officer to collect your card

Courier scam

COURIER CONVERSATION

Delivery for you, please sign here.

You haven't ordered anything – you open the parcel to find a mobile phone or other high value item.

The sender of the parcel phones to explain the parcel has been delivered to the wrong address, a courier is on his way to collect it from you.

COURIER CONVERSATION

Within minutes a courier knocks on the door and takes the parcel off you.

Can you guess the scam?

How it works

The scammer has ordered goods (usually a mobile phone) in your name, to be delivered to your address. After delivery you receive a call - there's been a mistake and the goods should have been delivered to somebody else, a courier will collect it from you. The scammer arrives and collects the phone.

The scammers get to keep the phone, the bill will be in your name.

People get caught out because:

- You know you've not ordered anything so you're not surprised to get a call to say a mistake has been made
- You're not being inconvenienced or put to any cost because somebody is calling to your house to correct the mistake

<u>If you suddenly receive delivery of goods addressed to you or somebody else in your household that you know you have not ordered contact the sender immediately</u>.

Help to protect yourself and join our free email alert system

We use iCAN to warn members about doorstep, phone, email and online scams.

We can also let you know about free services, education and training opportunities and social events organised by the council or voluntary and charity groups.

We also want to ask you to be our eyes and ears and provide us with information about what is happening in your community.

If you don't want to receive all types of messages you can choose the categories that you're interested in:

1. Education or training opportunities
2. Free services
3. Acting as our eyes and ears
4. Scams and consumer information
5. Social events organised by the Council or charities and voluntary groups

If you live or work in Halton you can join iCAN by emailing us with your name, address and the categories of messages you want to receive.