Rother Neighbourhood Watch.

These are some of the scams that are sent out too the public on email.

HMRC related 'scam's, phishing emails and bogus text messages

Phishing emails and bogus contact: HM Revenue and Customs examples

Updated 5 January 2018

If you think you've received an HM Revenue and Customs (HMRC) related phishing or bogus email or text message, you can check it against the examples in this guide.

It will help our investigations if you report all 'HMRC related' phishing emails and bogus text messages to us. Even if you get the same or similar phishing email or text message on multiple occasions, please forward it to email phishing@hmrc.gsi.gov.uk and then delete it.

Don't open any attachments or click on any links within the email or text message, as they may contain malicious software or direct you to a bogus website.

Tax refund and rebate scams

Email addresses

HMRC will never send notifications by email for:

- **tax rebates**
- **refunds**

- **personal or payment information**

Don’t visit the website within the email or disclose any personal or payment information.

A selection of email addresses used to distribute the tax rebate scam emails are below:

- **service.refund@hmrc.gov**
- **secure@hmrc.co.uk**
- **taxrefund-notice@hmrc.gov.uk**
- **taxrefund@hmrc.gov.uk**
- **refund-help@hmrc.gov.uk**
- **refund.alert@hmrc.gov.uk**
- **refunds@hmrc.gov.uk**
- **rebate@hmrc.gov.uk**
- **HM-Revenue-&-Customs@ztoro.com**

……

Text messages

HMRC may sometimes send text messages, however we will never ask for personal or financial information. If you get a text message claiming to be from HMRC offering a ‘tax refund’ in exchange for personal or financial details you shouldn’t reply. Don’t open any links in the message.

It would help our investigations if you could forward details of the text message to 60599 (network charges apply) or email phishing@hmrc.gsi.gov.uk before deleting it.

An example of a phishing text message is below:

Tax rebate scams containing PDF attachments

HMRC is aware of a phishing campaign telling customers they need to 'download a PDF attachment' to get a tax refund.

The PDF attachment contains a link to a phishing site asking for personal or financial information. Don't reply to the email or download the attachment.

Forward it to email phishing@hmrc.gsi.gov.uk and then delete it.

Bogus phone calls

HMRC is aware of bogus phone call scams, where the caller claims to be from HMRC. The fraudster may either:

- **encourage you to give personal and financial information in exchange for a tax refund**
- **say that HMRC is filing a lawsuit against you and that you must make an immediate payment**

This scam has been widely reported and appears to be targeting elderly and vulnerable people.

If you can't verify the identity of the caller, we recommend that you don't speak to them.

If you've been a victim of the scam and suffered a financial loss you can report it to Action Fraud.

It would also help our investigations if you could send us details of the scam (such as the date and time of call and the telephone number that made the call) to email: phishing@hmrc.gsi.gov.uk.

Social media scams

HMRC is aware of direct messages being sent to customers via social media.

A recent scam was identified on Twitter offering a tax refund.

These messages aren't from genuine HMRC social media accounts and are a scam. We would never offer a tax rebate or request personal or financial information via a social media direct message.

If you can't verify the identity of the social media account, we recommend you send the details to email phishing@hmrc.gsi.gov.uk and ignore it.

Refund companies

HMRC is aware of companies that send emails or texts advertising their services. They offer to apply to HMRC for a tax rebate on the customer's behalf, usually for a fee. These companies aren't connected with HMRC in any way.

We advise you to read the 'small print' and disclaimers before using their services.

Export clearance process (delivery stop order) emails

Emails which claim that goods have been withheld by customs and need a payment before release are known as '419 scams.

HMRC is aware that customers have received emails asking for personal and financial information or upfront payments in exchange for the fictitious items:

- **lottery winnings or prize money, including lottery winnings**
- **seized goods or packages (held by customs and excise)**
- **certificates or bonds**
- **inheritance payments**

Fraudsters may sign off such scams using the name of a real HMRC member of staff to make the scam appear genuine. If you're in any doubt, please forward the email to HMRC for verification to email: phishing@hmrc.gsi.gov.uk.

Request to complete NRL1 forms and return by fax

Lettings agents and landlords living abroad are being targeted by a series of scams asking for:

- **completion of a form NRL1 (by email, letter or fax)**
- **personal information**

These forms (which may be headed 'Application for Withholding Certificate for Dispositions by Foreign Persons of UK Real Property Interests' or 'Application for a tax-free account and to receive rental income without deduction of tax for Non-UK Residents') aren't sent by HMRC and shouldn't be completed.

We will never ask you to disclose personal information by email or fax.

Nationwide Scam?

Nationwide

Building Society

Your Current Account statement is here

Dear Mr Easily Scammed.

Your monthly statement is ready and waiting – view it now in three simple steps:

1. Visit our website using the link below, then log into the Internet Bank.

2. Select the Current Account you'd like to view the statement for.

3. Select 'Previous statements' from the menu on the left, then the statement you'd like to see.

Visit our website ›

Are your details up to date?

A new regulation is coming in to help make online payments even more secure. So, if you're someone who shops online, you'll start seeing a Verified by Visa screen pop up more often, when you go to pay. You'll then be asked to enter a one-time

code that will get sent to your mobile, to check it's really you.

So, now's the time to make sure we have your correct contact details - especially your mobile phone number. You can do this quickly and easily in the 'my details' section of the Internet Bank.

Find out more ›

Setting up a new person to pay?

If you are, you'll soon start seeing new security prompts when you set up a new payee. This is just one more way for us to help protect you against fraud scams, and allow you to decide whether you're happy to make the payment before it goes through.

If you want to find out more about fraud and scams, there's lots of information on our website.

Fraud awareness ›

We keep your financial details secure

For your security we'll always include your postcode at the top of any emails we send you. If you notice that your postcode is wrong, please update it using your Internet Bank or pop into your local branch. Your updated postcode will show on emails sent from us within 8 weeks.

Your financial security is important to us, which is why we'll never include or ask for confidential details or security information such as account numbers or PINs in our emails to

you. If you're ever suspicious of an email, please delete it immediately. If you think you've revealed your personal or security details visit our security web page >

Your postcode is: TN40 ???

Download our Banking app

Find your nearest branch

Send us a message

Nationwide Building Society

Important Information

Important information about the Financial Services Compensation Scheme (FSCS)

The FSCS pays compensation to customers if their financial provider is unable to meet its financial obligations. The money you hold with us is covered by this protection. The protection covers up to £85,000 for each customer. Please read the FSCS information sheet which gives you important information about the protection the scheme provides. For further information about the compensation provided by the FSCS, refer to the FSCS website at www.FSCS.org.uk.

Nationwide adheres to The Standards of Lending Practice which are monitored and enforced by the LSB: www.lendingstandardsboard.org.uk.

You can update the email address we hold for you in the following ways: Via the Internet Bank in the 'Manage my details and settings' tab or on the

.....

Email scam awareness

Email scams, also called phishing scams, are becoming increasingly common as fraudsters come up with new tricks to try and steal your personal information and bank details.

In some cases, the emails have malicious software attached which can infect your computer, tablet or mobile with a virus.

Cyber Breaches

Dear BT Customer,

Due to security breaches on an international scale. BT have launched preventative measures in ensuring your customer data remains safe.

BT have been busy upgrading our security to keep your personal details safe. To do this in the most secure way possible, we have temporarily limited access to profile features that contain your sensitive data. To confirm your security upgrade and reestablish full access to your BT account please follow the link below

Confirm security upgrade

Deficiency to do so will result in limited access to your profile.

Need more help?

Please don't reply to this email as we won't get your message. If you've got any questions, or for more ways to get in touch, go to bt.com/help

Thanks for choosing BT.
Libby Barr
Managing Director, Customer Care

What is a phishing scam?

Phishing when a cybercriminal contacts you out of the blue and convinces you to hand over your personal information or money or gets you to download a virus that infects your computer.

Phishing is a play on the word 'fishing' and usually happens over email, but can also happen through texts, social media or phone call

1 Check the 'from' address

It's always worth checking the address the email comes from for spoofing. Scammers often change its name to make it look more like it is from the company or organisation they are pretending to contact you from.

A scam email usually has a bizarre email address behind what looks like a genuine sender name.

To find out if there's a fraudster behind what looks like a genuine sender, use your mouse to hover the cursor over or right-click on the sender name and you should see the email address behind it.

2 Is the greeting impersonal?

Increasingly you will notice that scammers are getting better at sending emails which include our name in the first line of the message. However, not all of them do.

Sometimes scam emails will just say "Hi" and not include your name, other times your email address will be used after "Hi". This impersonal approach to contacting you is another sign that it's likely to be a scammer behind the email.

3 Check contact information and dates

Does the 'contact us' information at the bottom of the email link to anything? Is it clickable? Are the websites it links to genuine? If the answer is no, you should be on your guard. To see where a weblink links to without clicking on it, simply hover your mouse cursor over the link. In the bottom left-hand corner of your web browser, the web address where the link goes to will appear.

Are the copyright dates (or any others) up to date? Often scammers will forget this detail. We came across an email scam in March 2017, which said the closing date of the competition being advertised in the email was December 31st, 2016. If you see this level of inconsistency, it's probably a scam.

4 Check branding

Scam emails are often pretending to be from big brands, companies, supermarkets, retailers and deal sites or from trusted government departments.

Checking branding and keeping an eye on the quality of branded logos, etc, in the email can strongly indicate if the email is a scam.

Is the branding on the email the same as it is on the company or government website? Does it match the last genuine email you received from them? If the answer is no, be suspicious.

5 Check if the linked website is legitimate

If you have clicked through to a website or landing page from an email thinking it is genuine, make sure you also double-check the authenticity of the website.

If it's a big brand or company, simply open a new tab and do a quick search for them. Click on their website and then compare the URL addresses.

Are they the same, similar or totally different? This should give you a good indication as to whether the landing page is a fake or genuine.

If you haven't yet clicked a link but are being asked to do so you can access an important message on your account, avoid the temptation to act quickly and log in via the email link. Instead, open your browser and log in to your account via the official website. Check if the message is there. If it isn't, you know the email you received is likely to be from a scammer.

Computer viruses can find their way onto your computer by scammers tricking you into installing them. For example, ransomware threatens to take action on your computer - such as deleting files - unless you pay a ransom.

If you suspect an email might be from a scammer, do not click on any links or download any attachments featured in the scam email as these may download a computer virus onto your computer.

Make sure you stay security-savvy and ensure your is always up to date, as this will provide an extra layer of protection if you have unknowingly downloaded a computer virus after clicking a link or downloading an attachment.

6 Asking for personal or bank details?

If an email is asking you to update or re-enter your personal or bank details out of the blue, it is likely going to be a scam.

Personal information includes things like your National Insurance number, your credit card number, Pin number, or credit card security code, your mother's maiden name or any other security answers you may have entered.

Most companies will never ask for personal information to be supplied via email.

7 Poor spelling, grammar and presentation?

Increasingly scammers are getting better at presenting phishing emails that are more or less free of poor spelling and grammar. But, you should still watch out for these tell-tale signs.

More common is to see a real lack of consistency with the presentation of the email, which may include several different font styles, font sizes and a mismatch of logos.

8 Trying hard to be 'official'?

Scammers often try hard to make the email sound official. They will do this in a number of ways, including using the word ‘official’.

You are unlikely to see the messaging in a truly official email shouting about how official it is.

Scam emails may also contain information such as account numbers and IDs designed to trick you into thinking the email is genuine. Check any of these against your records to see if they match.

9 Trying to rush you?

Fraudsters will try to pressure you with time-sensitive offers, encouraging you to act now or miss out on ‘exclusive’ deals.

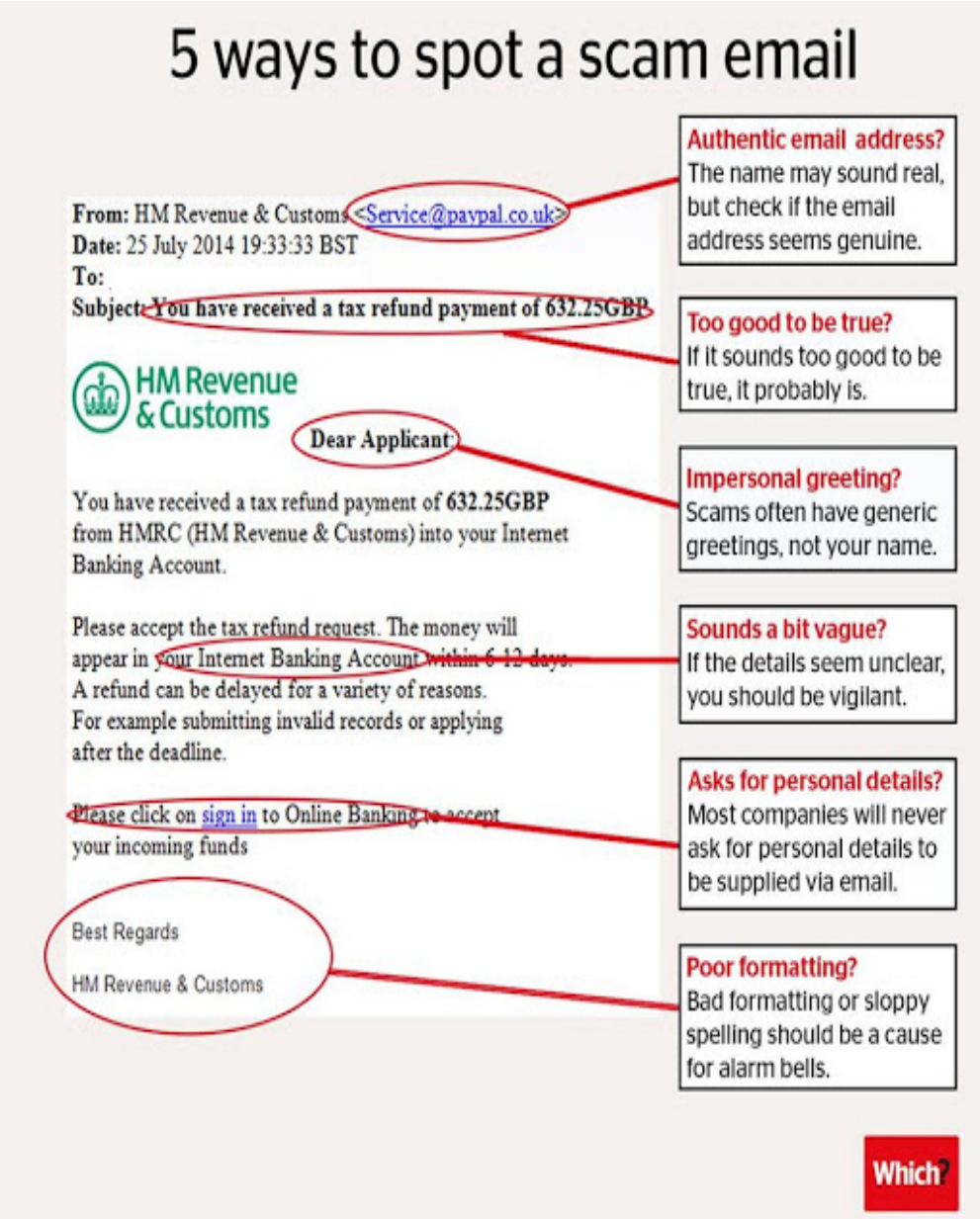
Take your time to make all the checks you need. If the message is alerting you to look at something linked to an account you have with the company, organisation or retailer, you should log in separately to your account in a new tab or window

It’s better to miss out on a genuine deal than risk compromising your personal details or money.

10 Check with real company, brand or department

If you're still unsure whether a scammer is behind the email you received, get in touch with the brand or company featured in your email directly via social media or their 'contact us' page.

Remember also to check the brand or company help and customer services pages. Often big companies are aware of scams circulating and have published advice for customers on what to watch out for.



If you wish to join
Rother Neighbourhood Watch.
Please contact Edward (Ted) Kemp.
chairman@rothernhw.co.uk
edward.kemp@sussex.pnn.police.uk

Sussex Police
Serving Sussex
www.sussex.police.uk