TAX HELP FOR OLDER PEOPLE

Don’t let it happen to you!

It seems that in these unprecedented times we are all living through there are now even more ways for scammers to try and con people out of money by obtaining bank details etc. So it would be a good time to give everyone a reminder of what those are and what to look out for.

Scammers have become more sophisticated in their bid to part us from our cash. From email scams and copycat websites to nuisance calls and tax rebate scams, we need our wits about us.

What is a Scam?

A Scam is a term used to describe a fraudulent business or scheme that takes money or goods from an unsuspecting person. With the world becoming more connected thanks to the internet and organisation’s keen to promote digital contact we are becoming more and more exposed to the possibility of being targeted. Cybercriminals have become quite savvy in their attempts to lure people in and get you to click on a link or open an attachment. The email they send can appear to look like it comes from a financial institution, e-commerce site government agent such as HMRC or DVLA or any other service or business.

Phishing (pronounced fishing) is another term that is used to describe a malicious individual or group of individuals who scam users. They do so by sending e-mails or creating web pages that are designed to collect an individual's online bank, credit card, or other login information. Because these e-mails and web pages look like legitimate companies, users trust them and enter their personal information.

How to spot a scam or a phishing email

1. Contacted out of the blue? If you're not 100% convinced of the identity of the caller, hang up and contact the company from a different phone.

2. Deal too good to be true? If a deal sounds too good to be true, it probably is.

3. Asked to share personal details? Never share your personal details with anyone you cannot validate are who they say they are. Phishing emails or phone scammers will often try and get valuable personal data from you, and they can use this to steal your identity or steal your money.

4. Under pressure to respond quickly? Scammers will often try to hurry your decision making requesting an urgent response or deadline to be met. Always take some time and think things through.

5. Vague contact details? Vague contact details can be a PO Box and premium rate numbers (starting ‘09’) or mobile number.

6. Spelling and grammar? Legitimate organisations will rarely, if ever, make glaring grammatical or spelling mistakes, and if they do, it will usually be an isolated incident. Scammers often use bad grammar and spelling to ensure only the most vulnerable people will respond to their messages.

7. Asked to keep it quiet? Being asked to keep something quiet should be a red flag. It's important to discuss any agreements with your friends, family or independent advisors.

To stay safe don't give out private information (such as bank details or passwords), reply to text messages, download attachments or click on any links in emails if you're not sure they're genuine.

One of the organisation's scammers typically seem to impersonate is HMRC. HMRC will never send notifications of a tax rebate/refund by email, or ask you to disclose personal or payment information by email. If you've had an HMRC email or text message you suspect isn't genuine report it to phishing@hmrc.gsi.gov.uk

Coronavirus (COVID-19) Scams

Email scams

HMRC is aware of a phishing campaign telling customers they can claim a tax refund to help protect themselves from the coronavirus outbreak. Do not reply to the email and do not open any links in the message.

'Goodwill payment' SMS

HMRC is aware of coronavirus SMS scams telling customers they can claim a 'goodwill payment'. Do not reply to the SMS and do not open any links in the message.

This is an example of the scam wording:

'As part of the NHS promise to battle the COV-19 virus, HMRC has issued a payment of £258 as a goodwill payment, follow link to apply.

'£250 fine' SMS

HMRC is aware of a SMS scam which states you will be fined £250 for leaving the house more than once. The message asks recipients to call an 0800 telephone number to appeal.

Do not reply to the SMS or call the phone number listed.

Tax refund and other email scams

HMRC will never send notifications by email about tax rebates or refunds.

Do not:

- visit the website
- open any attachments
- disclose any personal or payment information

Fraudsters may spoof a genuine email address or change the 'display name' to make it appear genuine.

TAX HELP FOR OLDER PEOPLE

Text messages

HMRC will never ask for personal or financial information when they send text messages.

Do not reply if you get a text message claiming to be from HMRC offering you a tax refund in exchange for personal or financial details. Do not open any links in the message.

Bogus phone calls

HMRC is aware of an automated phone call scam which will tell you HMRC is filing a lawsuit against you, and to press one to speak to a caseworker to make a payment. HMRC can confirm this is a scam and you should end the call immediately.

This scam has been widely reported and often targets elderly and vulnerable people.

Other scam calls may offer a tax refund and request you to provide your bank or credit card information. If you cannot verify the identity of the caller, HMRC recommends that you do not speak to them.

If you've been a victim of the scam and suffered financial loss, report it to Action Fraud, which is the UK's national fraud and crime reporting centre. It provides a central point of contact about fraud and financially motivated internet crime. It offers an online reporting tool at www.actionfraud.police.uk or you can call and speak to an adviser on **0300 123 2040**.

As the calls use a variety of phone numbers, to help HMRC investigations you should report full details of the scam by email to: phishing@hmrc.gov.uk, including the:

- date of the call
- phone number used
- content of the call

Social media scams

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

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

These messages are not from genuine HMRC social media accounts and are a scam. HMRC never uses social media to:

- offer a tax rebate
- request personal or financial information

WhatsApp messages

HMRC will never use 'WhatsApp' to contact customers about a tax refund. If you receive any communication through 'WhatsApp' saying it's from HMRC, it is a scam. Email details of the message to phishing@hmrc.gov.uk then delete it.

So remember, do not visit any website contained within a bogus email or disclose any personal or payment information.

If you are still concerned about a contact or your personal information, contact the organisation directly, either by finding their bona fide e-mail address or telephone number.

It is so important to check on any form of communications before you react. Scams target people of all backgrounds, ages and income levels. There's no one group of people who are more likely to become a victim of a scam. Outsmart the scammers and stay safe.

This article is by Tax Help for Older People Registered Charity no 1102276 (Scotland no SC045819), offering free tax advice to older people on a low income who cannot afford professional help. The Helpline number is 01308 488066.