

HMRC urges universities to warn new students of tax scams danger

Students starting university this year are being warned by HM Revenue and Customs (HMRC) that they could be targeted by a fresh wave of tax scams.

As new students start the academic year, they can be particularly vulnerable to cybercrime. With universities taking a blended approach to online and face-to-face tuition this year, and an increase in remote working due to the pandemic, students could be left particularly exposed to the work of fraudsters.

Freshers might also be more vulnerable to these types of scams due to their limited experience of the tax system.

HMRC has written to universities, through Universities UK, asking them to help ensure their students know how to spot a scam.

In August this year HMRC received reports from the public of more than 74,800 scam emails, text messages and phone calls. Nearly 41,300 of these specifically offered bogus tax rebates.

Thousands of these scams were targeted at students and the criminals involved appear to have obtained their personal university email addresses by unlawful means. These scams often offer fake tax refunds or help with claiming Covid-related financial support.

Phishing email messages can also provide a gateway for criminals. Students who provide personal details in response can end up inadvertently giving access to important accounts, like email or online banking, leaving scammers free to commit fraud and steal their money.

Criminals also use phone scams to threaten taxpayers into handing over cash. Some 651,600 scams have been referred to HMRC since August last year. Of those, more than 215,660 were voice or phone scams, known as vishing.

If someone calls, emails or texts claiming to be from HMRC, saying that you can claim financial help, are due a tax refund or owe tax, and asks for bank details, it might be a scam. Check GOV.UK for [how to recognise genuine HMRC contact](#).

Jesse Norman, Financial Secretary to the Treasury, said:

Cyber criminals use every method they can to steal money and personal data from students.

We are concerned that remote working because of Covid-19 could lead to more tax scams targeting a new and potentially vulnerable university intake.

HM Revenue and Customs is doing everything it can to clamp down on cyber fraud, but students also need to be vigilant. We would urge university principals to take a lead in helping to protect their students from these cyber criminals by raising awareness of what to look out for.

Alistair Jarvis, Chief Executive of Universities UK, said:

The security and welfare of students is always a priority for universities. The message to students, at what is a particularly stressful time, is to remain vigilant and question anything that seems unusual.

Any student who fears their account may have been misused is encouraged to speak to either university support services, their bank, or to the police via [Action Fraud](#).

Universities Minister, Michelle Donelan, said:

I want every student to be as safe as possible this term, both online and offline, and it is absolutely vital they are aware of the risks posed by tax scams.

I encourage institutions to warn students about this issue and arm them with the information they need to identify and respond to tax scams if they should be targeted.

HMRC works with the telecoms industry to automatically block spoofed numbers used by scammers and since August last year, has worked with internet service providers to take down nearly 10,870 malicious web pages.

Read the letter that HMRC has asked Universities UK to share with Vice Chancellors so they can make their students aware of the risk of being scammed:

[HMRC letter to Vice Chancellors warning about cyber scams targeting new students](#) (PDF, 64.8KB, 2 pages)

HMRC's advice:

Stop:

- take a moment to think before parting with your information or money.
- don't give out private information or reply to text messages, and don't download attachments or click on links in texts or emails you weren't expecting

Challenge:

- it's ok to reject, refuse or ignore any requests – only criminals will try to rush or panic you
- [search 'scams' on GOV.UK](#) for information on how to recognise genuine HMRC contact and how to avoid and report scams

Protect:

- forward suspicious emails claiming to be from HMRC to phishing@hmrc.gov.uk and texts to 60599
- contact your bank immediately if you think you've fallen victim to a scam, and report it to [Action Fraud](#)

[Examples of current scamming frauds](#) can be found on GOV.UK..

HMRC prevents scams by:

- automatically identifying most cyber scams before customer have even reported them to us
- asking Internet Service Providers to remove the malicious web pages or phishing websites
- deploying innovative technologies to prevent misleading and malicious communications ever reaching our citizens
- warning the public through [sharing details and examples of genuine and scam communications on GOV.UK](#) and through the media
- maintaining channels through which people can report suspicious contact, at phishing@hmrc.gov.uk and 60599 for texts
- working with the telecoms industry to automatically block spoofed numbers
- tackling misleading websites designed to make customers pay for services that should be free or low cost, often charging customers for connection to HMRC phone helplines
- working closely with national and international law enforcement organisations