How to spot scammers claiming to be from the NCSC

Check that you're talking to a genuine NCSC employee, and not a criminal.

We have received reports of criminals impersonating NCSC officials in order to scam members of the public. These scams, usually conducted by phone, try and trick people into transferring money, or revealing sensitive information.

This page explains:

- how to verify an NCSC contact
- how to spot common scams
- what to do if you think you've been scammed

Contact by phone

An NCSC official may contact you by phone. You can use the process described below to verify this before taking any further action.

However, official NCSC callers will never:

❌ ask for your bank details or PIN

❌ request you transfer funds to another account

❌ ask you to hand over cash or bank cards

❌ ask you to pay a fine

❌ request passwords or logon details so they can access your computer (or for any other reason)

❌ ask you to provide personal details in an email attachment, or on a website

---

❌ ask you to assist in an investigation by doing any of the above (or state that you are committing a crime by not complying)

❌ communicate in an abusive, threatening or coercive manner

⚠

If you do receive a call of this nature, please hang up and report it to Report Fraud.

Contact by email

An NCSC official may contact you by email. You can use the process described below to verify this before taking any further action.

However, official NCSC emails will never:

- ask for remote access to your computer
- send unsolicited emails with attached files (especially .zip or Microsoft Office files)
- ask you for any login details (including passwords)
- direct you to third party organisations to verify the identity of NCSC staff

If you believe you have received a suspicious email, please report it to us

Contact by SMS or WhatsApp

An NCSC official will never contact you by text message or WhatsApp (or other instant messaging service).

If you receive a message claiming to be from the NCSC, please report it to us.

How to verify a contact from the NCSC

The NCSC may need to contact you for operational reasons. You can verify that the contact you are speaking to is from the NCSC by using our **Verify an NCSC contact** service.

1. Go to our **Verify an NCSC contact form.**

2. Complete the form and click **Submit.**

   An NCSC official will reply to verify if the contact is genuine.

How to spot scam messages

It used to be easier to spot scams. They would often contain bad spelling or grammar, come from an unusual email address, or feature imagery or design that feels 'off'. But scams are getting smarter and some even fool the experts. For this reason, the NCSC has produced detailed guidance to help you spot and report suspicious messages, emails, web sites and phone calls, but in summary:

- Scammers try to quickly gain your trust. They aim to pressure you into acting without thinking. If a message or call makes you suspicious, stop, and break the contact.

- Your bank (or any other official source) will **never** ask you to supply personal information via email, or call and ask you to confirm your bank account details.
- If you suspect someone is not who they claim to be, hang up and contact the organisation directly (for example using their official website).

If you've lost money, or been hacked

If you think you may have been a victim of fraud or cyber crime, whether that's from visiting a website, or responding to an email or a text message, you should report it.

- If you live in England, Wales or Northern Ireland, you can report it to Report Fraud at **https://www.reportfraud.police.uk/** or by calling **0300 123 2040**.
- If you live in Scotland, you can report it to Police Scotland by calling **101**.

PUBLISHED

30 June 2023

REVIEWED

29 May 2024

VERSION

1.0

WRITTEN FOR

Cyber security professionals Large organisations Public sector Self employed & sole traders Small & medium sized organisations You & your family