Stay one step ahead of the scammers

There's growing evidence of a spike in email and phone scammers as criminals look to seize on people's vulnerabilities during the pandemic.

Maybe you've received one claiming to be from organisations you would trust such as:

- the Government asking for your bank details so money related to free school meals can be transferred;
- HMRC stating you have a tax refund;
- banks asking you to confirm your details;
- emails from criminals disguising themselves as an organisation;
- callers offering coronavirus testing kits and protective equipment; or
- calls telling you your internet is going to be cut off in 24 hours because you've been hacked.
- A direct debit payment has failed

The common factor with emails is that you can only find out more if you click on a link or open an attachment.

An automated call will invariably ask you to press buttons on your phone and skilled criminals on live calls can deftly convince you of their legitimacy. And that's when the damage starts. Either by inadvertently giving criminals access to your computer or phone or, at the extreme end of the scale, emptying your bank account.

The good news is there are some simple steps to take to ensure you stay safe and don't fall victim to these invisible criminals.

Before you take any action, pause and take a moment to consider:

- Is the email addressed to you personally or is it addressed to "Dear customer" or "Valued customer"?
- Is the spelling, punctuation and grammar correct?
- Does the email ask you to urgently verify details within a specific time limit?
- Does the sender's email address look legitimate?
- Does the email look like previous emails you have legitimately had from the same organisation?
- Does the email ask for your bank account details, online banking passwords or your PIN number and CVC code for your debit card?
- Does the caller's offer sound too good to be true? Then it probably is.
- Do you actually have an existing relationship with the caller?

Agencies across the UK, and beyond, are working together providing advice on how to stay safe online.

The National Cyber Security Centre has an abundance of guidance including how to spot and deal with suspicious emails; top tips for staying safe online and securing your devices.