Use new fast-track reporting for suspicious emails - Citizens Advice

Scam emails, one of life's most tiresome phenomena, are becoming so smooth and sophisticated that even computer experts can be deceived by them, and the rest of us are in constant danger of being taken for a ride.

There is no need to feel isolated with the problem, though. If you are suspicious of an email or simply unsure, you can use a new, dedicated reporting service which is very quick and convenient: forward the email to report@phishing.gov.uk and the National Cyber Security Centre (NCSC) will investigate it.

How does a scam email work? The usual methods are persuading you to divulge sensitive information, like bank details, or urging you to click on certain links. If you click on those links, you could be directed to an unsafe website which might download viruses on your computer or steal your passwords or data.

It's crucial to bear in mind that a scam email is designed in such a way as to get you to act quickly and without thinking, so NEVER give way to that pressure.

How do you spot a phishing email? This is very tricky, since many of them look just like the real thing. Scammers are quite capable of producing professional quality graphic design with pleasant pastel colours, for example. This makes the email look authoritative and trustworthy and thoroughly up to date.

However, and fortunately for us, if you examine a scam email carefully it will reveal its true nature. Remember these key points:

First, it is very unlikely to be a message you are expecting.

Second, the language of most scam emails has an uncompromising toughness that isn't characteristic of the average business email. It might try to rush you into making a decision or threaten you with legal action or financial losses, telling you that you have to act right away to avoid them. The email might claim to be from a bank, a government department or the Inland Revenue, perhaps saying that a warrant has been issued for your arrest.

The email could also be from a company that doesn't normally contact you or from an organisation that you normally deal with in a different way, e.g. TV Licensing or the district council - which, it might strike you, have never emailed you before.

Beware too of topical scams: an email might offer you a cure for coronavirus or encourage you to donate to a related cause.

Always check the sender's email address because this is the only part of the message which can't be beautified. There will be something peculiar about it for sure. For instance, it might be extremely long and complicated with lots of numbers and letters, or the country code might be unfamiliar.

If you are in any doubt, don't open the email and don't click on any of its links, but forward it right away to report@phishing.gov.uk. The NCSC says it acts on every message received, analysing it and the dubious websites it links to. Government specialists can then block the criminal's email address and instruct hosting companies to remove the websites from the Internet.

For essential reading see https://www.ncsc.gov.uk/information/report-suspicious-emails or ring Citizens Advice Adviceline on 0300 330 9042.