Help disrupt fraudsters by reporting scam emails that you receive. People receiving scam emails are urged to report them.

The reports received by Action Fraud will be forwarded to the National Fraud Intelligence Bureau run by the City of London Police for collation and analysis. This will enable crucial intelligence to be gathered and preventative action to be taken. The activity will seek to disrupt the fraudsters and close down the links between them and the victim.

Last year (January 2015 – December 2015) they received on average 8,000 reports per month, with 96,699 people reporting that they had received a phishing scam.

What should you do if you've received a scam email?

- Do not click on any links in the scam email.
- Do not reply to the email or contact the senders in any way.
- If you have clicked on a link in the email, do not supply any information on the website that may open.
- Do not open any attachments that arrive with the email.
- Genuine computer firms do not make unsolicited phone calls to help you fix your computer.

If you think you may have compromised the safety of your bank details and/or have lost money due to fraudulent misuse of your cards, you should immediately contact your bank.

If you've been a victim of fraud, report it to Action Fraud.

Fake emails often (but not always) display some of the following characteristics:

- The sender's email address doesn't tally with the trusted organisation's website address.
- The email is sent from a completely different address or a free web mail address.
- The email does not use your proper name, but uses a non-specific greeting like "dear customer".
- A sense of urgency; for example the threat that unless you act immediately your account may be closed.
- A prominent website link. These can be forged or seem very similar to the proper address, but even a single character's difference means a different website.
- A request for personal information such as user name, password or bank details.
- The email contains spelling and grammatical errors.
- You weren't expecting to get an email from the company that appears to have sent it.
- The entire text of the email is contained within an image rather than the usual text format.
- The image contains an embedded hyperlink to a bogus site.

Sent by PS 71468 Julie Mackay

To update your profile including unsubscription, click here and sign into your ECM profile to change your preferences.