News story: Reporting a phishing email scam

We have been working with National Cyber Security Centre to improve public sector cyber security. As part of the phishing and malware counter-measures, we have changed the email address for you to report a fraudulent email that pretends to be from HM Land Registry.

How to identify phishing emails

If you are unsure whether an email you have received is genuine, look at the sender address domain in the email's "From" field.

Genuine HM Land Registry emails have a sender domain ending in .gov.uk, for example Telford.OfficeMail [Telford.Office@landregistry.gov.uk]

Phishing emails may use our office names, but are being sent from other email domains, for example Telford.OfficeMail [noreply3@nlacpa.com].

What to do

If you are unsure about an email claiming to be from HM Land Registry, follow these steps.

1. Do not open the attachment or follow any links, as this may infect your computer with a virus. Computer viruses can help criminals to steal data from your computer.

2. Do not reply to the email.

3. Forward the email, along with any attachments, to scam@netcraft.com. Where possible, use the 'Forward as attachment' option on your email software. Netcraft will take action to remove any offending material or sites from the internet.

4. If you have lost money or information, or your computer has been taken over by a phishing or malware attack, report it to Action Fraud.

5. Delete the email.

Why we made the change

Our ambition is to become the world's leading land registry for speed, simplicity and an open approach to data. To achieve this ambition, we are committed to strengthening and maturing our cyber security defences continually to address increasingly sophisticated national and international threats.

As part of the Active Cyber Defence programme we are now working with Netcraft, a private sector company, on phishing and malware countermeasures.

The Netcraft service has taken down more than 62,849 attacks across government. The average ‘time to die’ for phishing sites relating to government has fallen from 27 hours prior to this change to under one hour. For malware this has decreased from 525 to 43 hours (roughly from 22 to less than 2 days).

For more information about phishing emails, read Action Fraud’s advice.