safe community

by David Thomas
features@algarveresident.com

David Thomas is a former Assistant Commissioner of the Hong Kong Police, consultant to INTERPOL and the United Nations Office on Drugs and Crime. He has recently formed *ISECA the Independent Security Agency* and *Safe Communities Algarve* an on-line platform here in the Algarve to help authorities and the community prevent crime.

Phishing: how to avoid becoming a victim

A few days ago I received an email which looked on the surface to be late Christmas present from *HM Revenue and Customs* in the United Kingdom.

So what made it attractive? Well firstly it was the title "Claim Your Tax Refund online".

Basically the email stated that *HM Revenue and Customs* had reviewed my tax position and based on previous assessments were inviting me to claim a refund of £1,400 for overpayment. Could this be a great start to 2012?

The email looked genuine enough to the point that the various links to web pages were in fact those of *HM Revenue and Customs*. The timing was also perfect just three days after my annual UK tax demand had arrived by post.

What made me suspicious were three things: firstly the email address, alerts@hmrc.gov.uk, did not seem right; secondly the fact that the email was addressed to "undisclosed recipients" and thirdly under "Claim my Refund" was a grammatical mistake *"How to return itself have not changed."*

At this point, I would immediately warn anyone not to contact this email address as it is not a genuine *HM Revenue and Customs* email contact.

So what is Phishing and why could it be harmful to you? Phishing is the fraudulent act of emailing a person in order to obtain their personal/financial information such as passwords, credit card or bank account details.

These emails often include a link to a bogus website encouraging you to enter your personal details. One you have entered your details fraudsters usually have sufficient information to remove money from your bank account etc.

Various estimates put the cost of phishing to around $1 billion and $7 billion per year but these estimates may be conservative. According to an organisation named *Security Labs*, its global threat intelligence reports state that the phishing attack level against Portugal is between 0.02% to 0.13% of all emails over a one-year period. Although low by western standards, this undoubtedly results in considerable losses from unsuspecting email recipients.

The problem with phishing emails, which comes under the broad umbrella of cyber crime, is that it knows no boundaries.

These can originate from virtually anywhere in the world despite the efforts of Governments in many countries taking steps to prevent this type of crime. In this respect, international cooperation between law enforcement agencies is very important.

In Portugal, US Homeland Security experts recently gave Portuguese law enforcement officials a five-day course on internet crime including financial fraud. This initiative came after a recent wave of hackings into computer systems of Portuguese ministries, government agencies, banks and political parties.

Phishing emails are often sent purportedly on behalf of major corporations such as *Halifax Bank*, *Lloyds Bank*, *Citibank*, *Co-operative Bank* and *PayPal*. An example of a PayPal Phishing email used at this time of year is as follows:

"Dear PayPal Member,

We here at PayPal.com are pleased to announce that we have a special New Year offer for you! If you currently have an account with PayPal then you will be eligible to receive a terrific prize from PayPal.com for the New Year. For a limited time only PayPal is offering to add 10% of the total balance in your PayPal account to your account and all you have to do is register yourself within the next five business days with our application (see attachment)!

If at this time you do not have a PayPal account of your own you can also register yourself with our secure application and get this great New Year bonus! If you fill out the secure form we have provided PayPal will create an account for you (it's free) and you will receive a confirmation e-mail that your account has been created".

The Phishing email then promises the same offer for friends and family who wish to participate. Of course, opening the attachment infects the recipient, spreads the email worm to others. Any information entered into the form is sent to the criminals.

People who launch phishing attacks are clever, educated computer users. They think very logically - but there is one ultimate failure on their part.

One of the key assumptions when it comes to phishing is that you will NOT think logically.

That is, you will take everything at face value, and never question anything which might seem suspicious.

ISECA, the Independent Security Agency, therefore provides the following guidance to help you recognize and prevent a phishing attack and therefore you avoid becoming a victim.

Ensure that your anti-virus software on your computer includes anti-phishing software.

Most governments and banks never ask you to provide confidential or personal information such as passwords, credit card or bank account details by email – so do not provide them.

Fraudsters want you to act immediately. Be wary of emails containing phrases like 'you only have three days to reply' or 'urgent action required'.

You should be aware that fraudsters sometimes include links to genuine web pages in their emails which is to try and make their emails appear genuine

Look out for a sender's email address that is similar to, but not the same as the genuine email addresses. Fraudsters often use email accounts with government or corporate names in them (such as 'refunds@hmrc.org.uk'). These email addresses are used to mislead you.

Fraudsters often send high volumes of phishing emails in one go so even though they may have your email address, they don't often have your name. Be cautious of emails sent with a generic greeting such as 'Dear Customer'.

Look out for spelling mistakes and poor grammar.

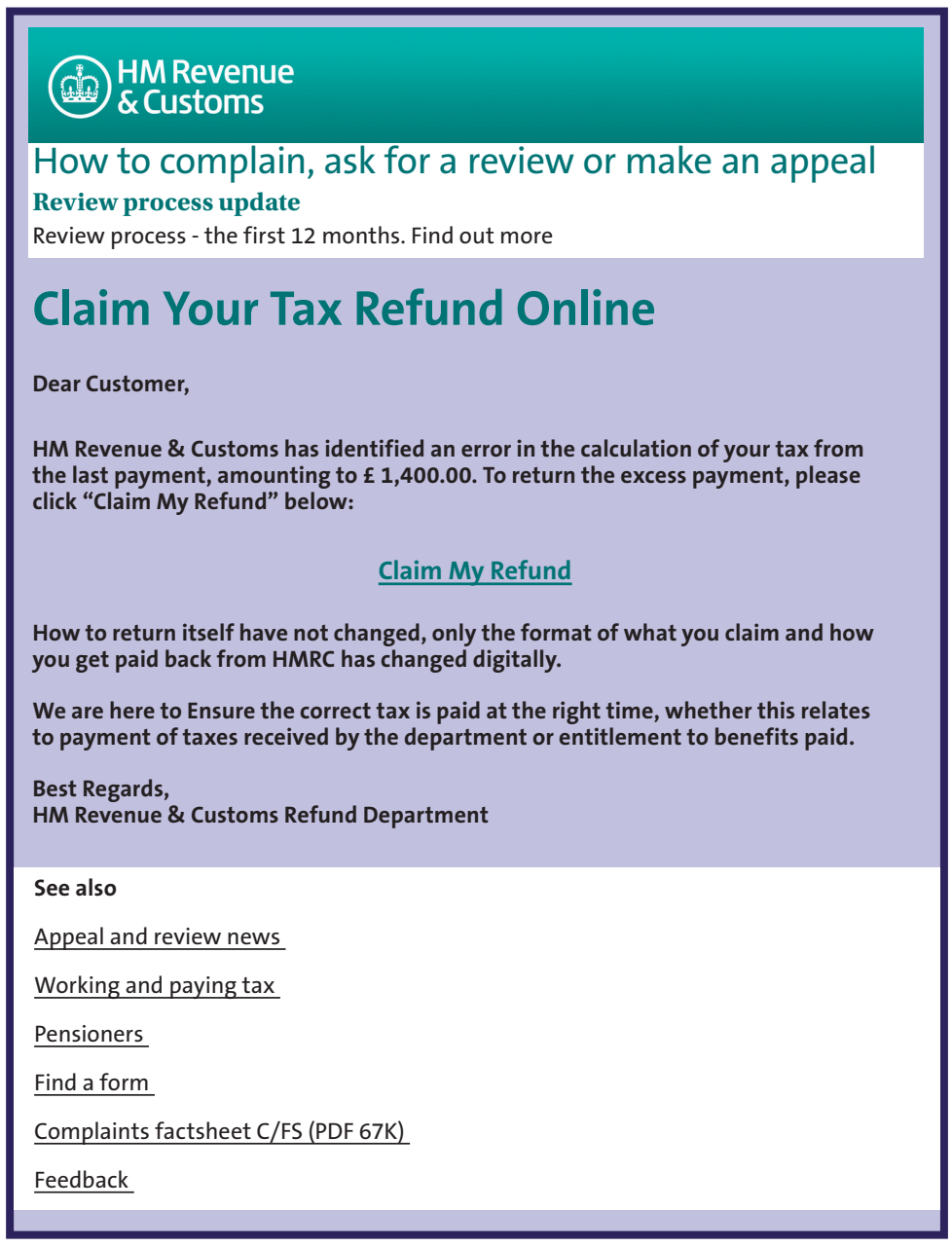
Be cautious of attachments as these could contain viruses designed to steal your personal information.

If you suspect that the offer is too good to be true or it is requesting you to divulge sensitive information the best advice is not to open it.

Most major corporations such as those stated above have security departments which investigate phishing emails and it is good practice to bring this to their attention so they can be kept up to date with the latest scams.

These corporations also provide advice on how to recognize phishing emails. Contact them if in doubt.

Have a safe and enjoyable New Year.



HM Revenue & Customs

How to complain, ask for a review or make an appeal

Review process update

Review process - the first 12 months. Find out more

Claim Your Tax Refund Online

Dear Customer,

HM Revenue & Customs has identified an error in the calculation of your tax from the last payment, amounting to £ 1,400.00. To return the excess payment, please click "Claim My Refund" below:

Claim My Refund

How to return itself have not changed, only the format of what you claim and how you get paid back from HMRC has changed digitally.

We are here to Ensure the correct tax is paid at the right time, whether this relates to payment of taxes received by the department or entitlement to benefits paid.

Best Regards,
HM Revenue & Customs Refund Department

See also

Appeal and review news

Working and paying tax

Pensioners

Find a form

Complaints factsheet C/FS (PDF 67K)

Feedback

- **Be cautious of emails sent with a generic greeting such as 'Dear Customer"**

- *David Thomas, Director of ISECA – the Independent Security Agency can be contacted at 913045093 or by email at info@iseca.net. More about ISECA is available on its website www.iseca.net and on Safe Communities Algarve website www.safecommunitiesalgarve.com.*