

FRAUDULENT EMAILS & INTERNET BANKING

WHITE PAPER

The use of email is rising exponentially and it will do so for the foreseeable future.

With this rise, we see an increase in the amount of spam and scam email we receive. This happens for many reasons.

The first is that the email owner has registered to some websites which in turn put them in mailing lists that were sold again and again to virtually anyone in the world.

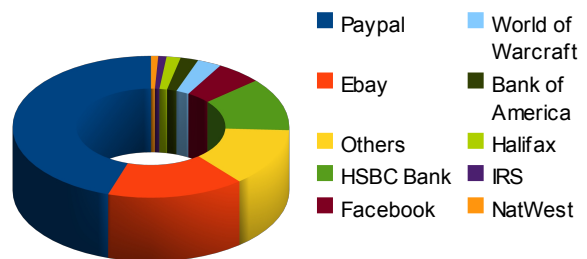
The second reason is that some of the owners friends may have had their computers compromised with malware that accessed their address books and provided new email addresses to spammers and fraudsters.

The third possible reason is that your computer itself has been compromised and has the information in your address-book disseminated online.

There is a variety of scam emails that are around, some very old and boring for those in the know, some a bit more adapted to new situations and circumstances.

One of the most widespread categories is that of "phishing". Phishing is a social engineering process, where people are made to believe they got an email from a legitimate source (i.e. their bank) and they respond as if the message was genuine.

Phishing Statistics
By Brand targeted (May 2010)



Paypal, Ebay, and banks are according to statistics the most target businesses.


Internet Banking messages are targeting everybody, and not specific bank account owners. They are sent to anyone on a list (sometimes 5-6 emails from "different banks" to the same person one after the other) and they usually bring up a security issue to prompt people to take action. A link is provided and the person who clicks goes to a website that looks almost exactly as that of the real bank. Then after putting their log in (user ID, password and secret question) they are redirected (usually) to the real bank website.


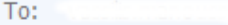
How does an email like this look like? The screenshots in the following pages show exactly how the scam works.


Halifax e-Alert: Important Security Alert

Back to messages |  

Halifax Online Banking [Add to contacts](#)
To vassilis.manoussos@hotmail.com

01:58
Reply 

From: **Halifax Online Banking** (helpdesk@halifax.com) 
Sent: 03 February 2011 01:58:45
To: @hotmail.com

 Microsoft SmartScreen marked this message as junk and we'll delete it after ten days.
Wait, it's safe!



Access Suspended !

Our Valued Customer,

Your access to Online Banking Service has been suspended. Due to a miss-match access code between your Security information. To enable you continue accessing your online account it will only take you few minutes to verify your Identity. Follow the reference below and you will be guided to where you can gain an instant verification process.

https://www.halifax-online.co.uk/_mem_bin/formslogin.asp/

IMPORTANT - You are strictly advised to match your **Sensitive Details** correctly to avoid service denial.

Thank you for helping us to protect you.

Security Advisor,
Halifax Online Banking Helpdesk

Photo 1. The scam email claiming to be from HALIFAX.

The logo is there and a link that seems to be from the bank is also obvious. However not all is how it looks.

The link in the message looks like this:

https://www.halifax-online.co.uk/_mem_bin/formslogin.asp/

However the real address that you will visit if you click on it, is this:

www.oycd.es.kr/rg4_data/members/.halifax-online.co.uk/_mem_bin/formslogin.asp/

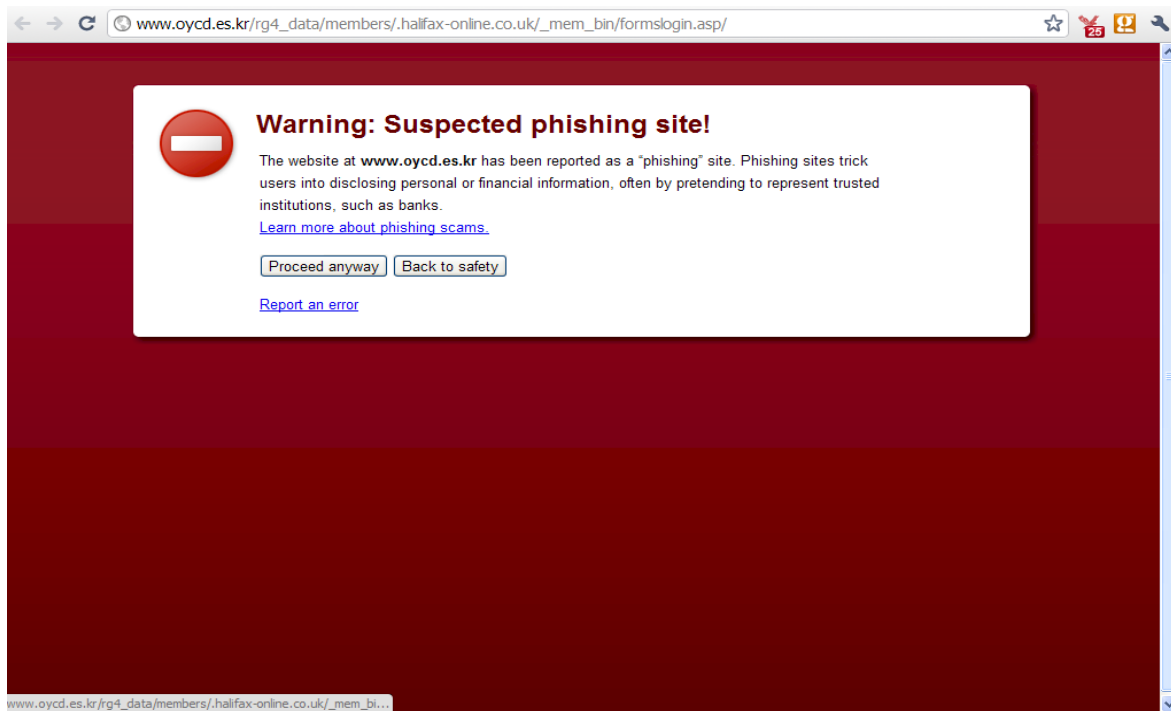


Photo 2. Warning from Virgin Media Security.



Photo 3. The actual phishing website.

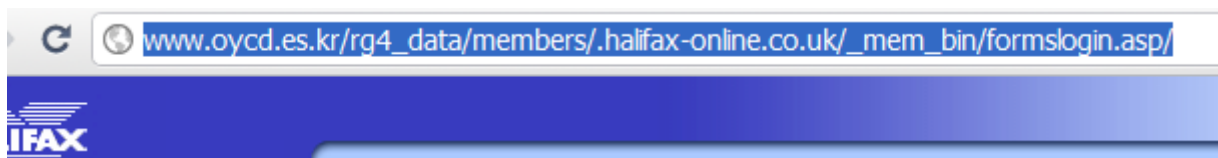
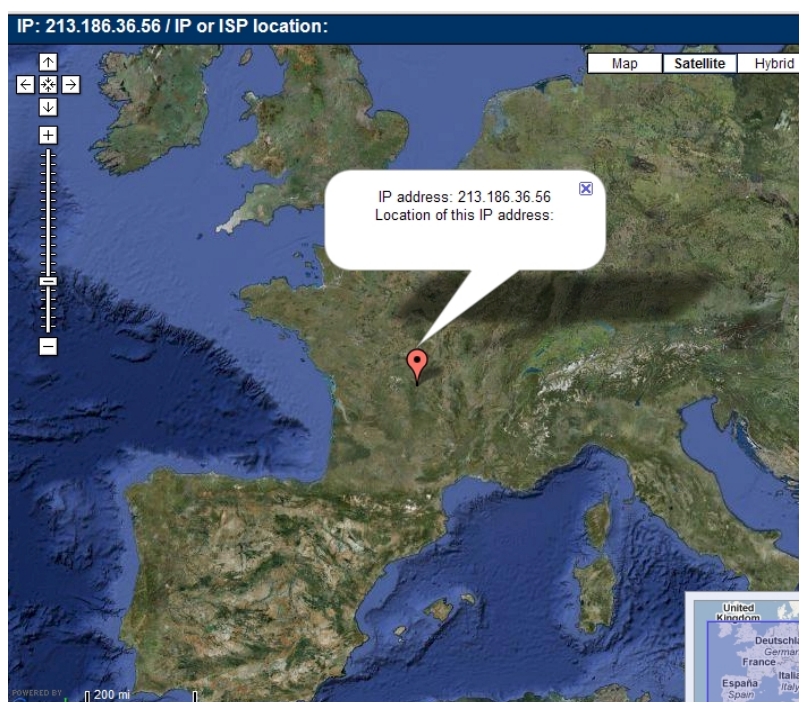


Photo 4. The real URL (address) is revealed at the top of the browser.

The use of the words **halifax-online.co.uk** in the address, is there to confuse the user.

As it is obvious, the fraudulent website looks exactly like the HALIFAX website. To add to the problem, apart from the log in section, all other links are directing you to the genuine web page on the Halifax website, making the distinction between the two even harder.



The domain name of the fraudulent website is a Korean one (.kr) however this does not mean the email came from Korea or that the website is hosted in Korea.

Further investigation of the email's header (hidden information in the email) proved that it originated from the following IP address: 213.186.36.56 (IP address is the unique address of the website that your browser needs in order to connect with the website).

Photo 5. The origin of the email (left)

It came as no surprise that the email did not originate from Korea. It was actually from central France.

The website however was located in Korea, and the address of the host was located at Seoul.

This is not the address of the perpetrator, but of the Internet Provider.

Photo 6. The website's origin (right)



Why should you consider a forensic investigation of a phishing scam?

- ✓ Your client deserves to know the truth if they are a victim
- ✓ If the perpetrator is within the UK you can use the evidence for a successful prosecution
- ✓ Even if the investigation may not reveal the address of the perpetrator, it will provide information about the IT provider that was used to send the email. This can be used in court to get the records associated with that specific incident.
- ✓ Most perpetrators they will prefer to target bank accounts of their own country, because there is no language barrier and they would know first hand how the system works.
- ✓ By locating a perpetrator, you may be able to attract more phishing victims (from the same or different source) as clients.

Host Info

Host: www.oycd.es.kr
Host IP: 125.251.158.226
IP country: 🇰🇷 Korea, Republic of
IP Address state: Seoul-t'ukpyolsi
IP Address city: Seoul
IP latitude: 37.5664
IP longitude: 126.9997
ISP: DACOM-PUBNETPLUS
Organization: DACOM-PUBNETPLUS

Modern digital forensics is the answer to dealing with electronic crime. If you are dealing with e-crime, you need to seek advice from a specialist, and use what technology has to offer as part of your litigation efforts.

Modern day crimes need modern day investigations, and people who are following developments closely.

For more information about digital forensics services and how you can integrate them into your litigation processes, please visit the [Strathclyde Forensics website](http://www.StrathclydeForensics.co.uk).

www.StrathclydeForensics.co.uk

Find out what other forensic services you can incorporate to your litigation processes. Read about our previous cases and discover new opportunities for your future cases.

For more information about forensic investigation of Blackberry and Nokia mobile phones, please visit our two sister sites:

www.BlackberryForensics.co.uk or www.NokiaForensics.co.uk



Copyright 2010-2011 Strathclyde Forensics