**Remember these 10 golden rules to help you beat the scammers.**

1 There are no guaranteed get-rich-quick schemes.

2 Do not agree to offers or deals straight away. If you think you have spotted a great opportunity, insist on time to obtain independent/legal advice before making a decision.

3 Do not hand over money or sign anything until you have checked the credentials of the company that you are dealing with.

4 Never send money or give bank or personal details to anyone you do not know or trust. This includes sending money abroad and using methods of payment that you are not comfortable with.

5 Log directly on to a website that you are interested in rather than clicking on links provided in an email.

6 Do not rely on glowing testimonials: find solid independent evidence of a company's success.

7 Always get independent/legal advice if an offer involves money, time or commitment.

8 If you spot a scam or have been scammed, report it and get help. Contact ActionFraud on 0300 123 2040, online at actionfraud.police.uk or the Police in your area.

9 Always remember: scammers are cunning and clever. They know how to manipulate you to produce the response they want.

10 Be suspicious. If you are unsure about anything, seek independent/legal advice.

Help sheet create by

Eddie Gore
(edshelp)

enquire@edshelp.co.uk

# Help on Email and internet Fraud

## What to do if you receive a suspected Phishing Scam email

**DO NOT** click on any links in the scam email.

**DO NOT** supply any personal information of any kind as a result of the email

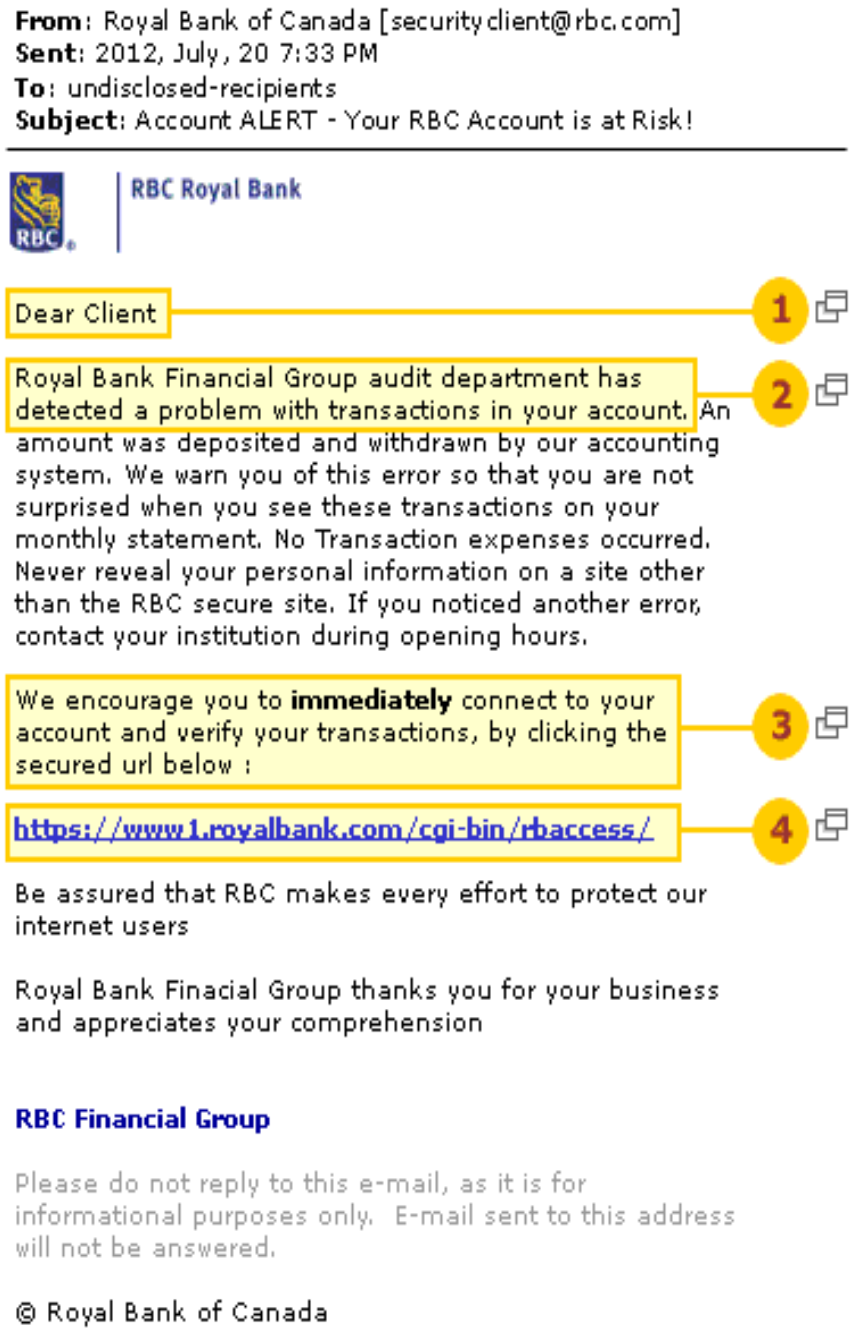
**DO NOT** reply to the email or attempt to contact the senders in any way.

**DO NOT** supply any information on the bogus website that may appear in your browser if you have clicked a link in the email.

**DO NOT** open any attachments that arrive with the email

**DELETE** the email from your computer as soon as possible.





**From:** Royal Bank of Canada [securityclient@rbc.com]
**Sent:** 2012, July, 20 7:33 PM
**To:** undisclosed-recipients
**Subject:** Account ALERT - Your RBC Account is at Risk!

RBC Royal Bank

Dear Client

Royal Bank Financial Group audit department has detected a problem with transactions in your account. An amount was deposited and withdrawn by our accounting system. We warn you of this error so that you are not surprised when you see these transactions on your monthly statement. No Transaction expenses occurred. Never reveal your personal information on a site other than the RBC secure site. If you noticed another error, contact your institution during opening hours.

We encourage you to **immediately** connect to your account and verify your transactions, by clicking the secured url below :

https://www1.royalbank.com/cgi-bin/rbaccess/

Be assured that RBC makes every effort to protect our internet users

Royal Bank Finacial Group thanks you for your business and appreciates your comprehension

**RBC Financial Group**

Please do not reply to this e-mail, as it is for informational purposes only. E-mail sent to this address will not be answered.

© Royal Bank of Canada

Subj: Inadequate security enrollment

NatWest Helpful Banking

**Dear NatWest Customer,**

Personal details of your NatWest account has encountered an error which made your online banking disabled.

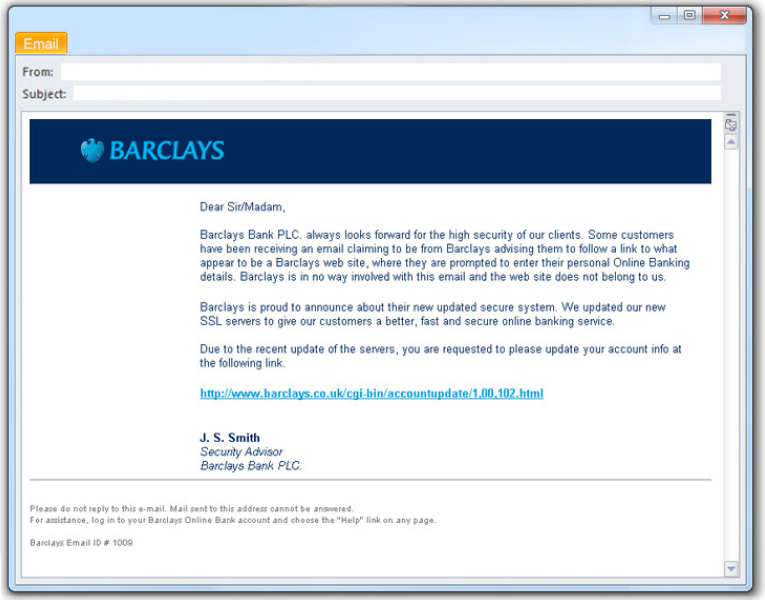
The cause may be:

* Inadequate security enrollment
* Your account has been logged in from a different location
* Invalid attempt login

As a bank we strongly recommend you to re-activate your account by clicking on the link below and follow the required steps

Click here to Sign in

Yours sincerely
National Westminster Bank






**This is a example of an email that would seem to come from one of you friends or family member.**

Dear **(Your Name)** I Hope you get this on time, sorry I didn't inform you about my trip in Cyprus for a program, I'm presently in Nicosia and am having some difficulties here because i misplaced my wallet on my way to the hotel where my money and other valuable things were kept.

I want you to assist me with a loan of 2500Euro to sort-out my hotel bills and to get myself back home. I have spoken to the embassy here but they are not responding to the matter effectively, I will appreciate whatever you can afford to assist me with,

I'll Refund the money back to you as soon as i return, let me know if you can be of any help. I don't have a phone where i can be reached. Please let me know immediately. Archie -
See more at:

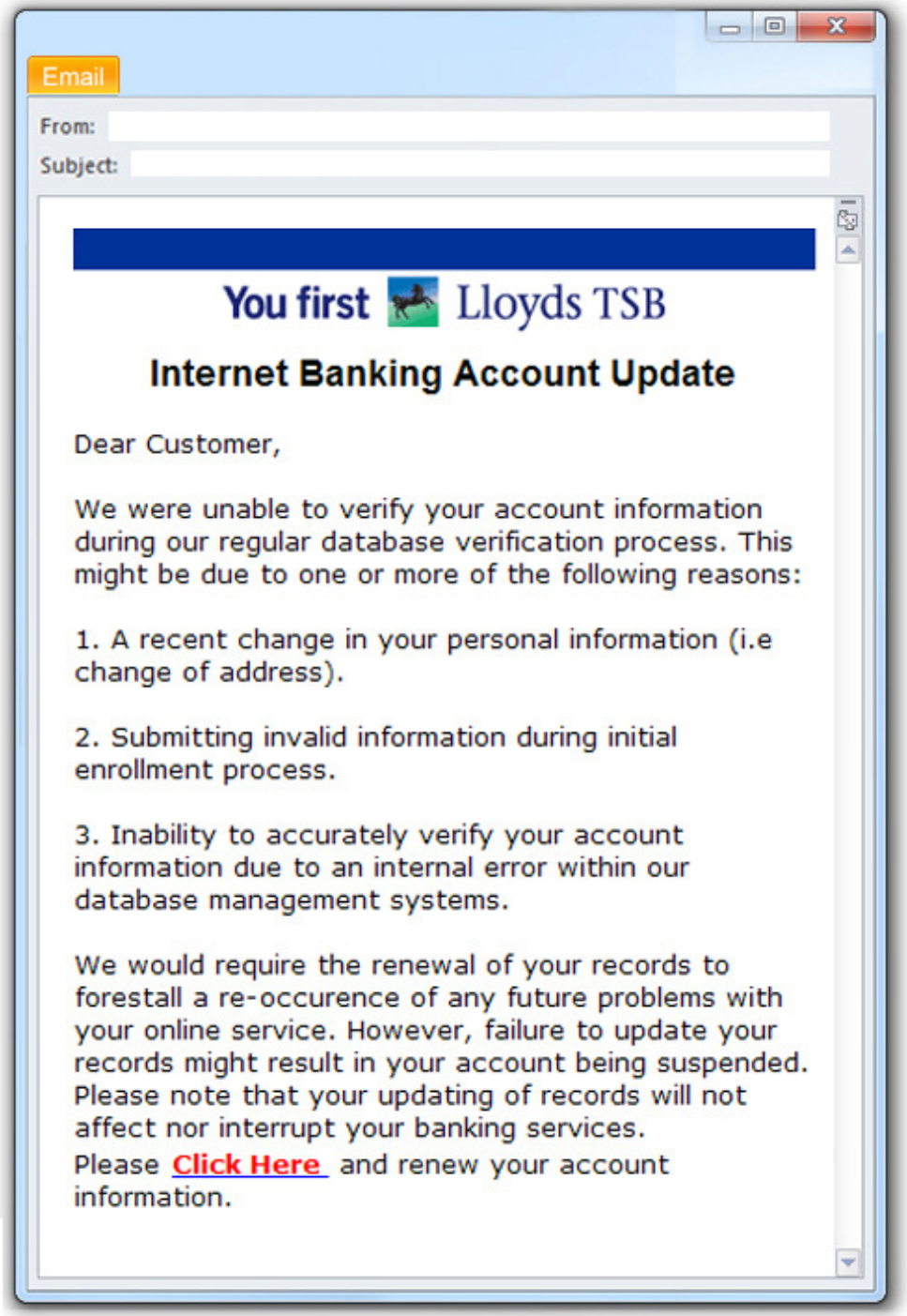
http://netprofitstoday.com/blog/email-scam-urgent-request-from-a-friend/#sthash.O3nQcFA9.dpuf

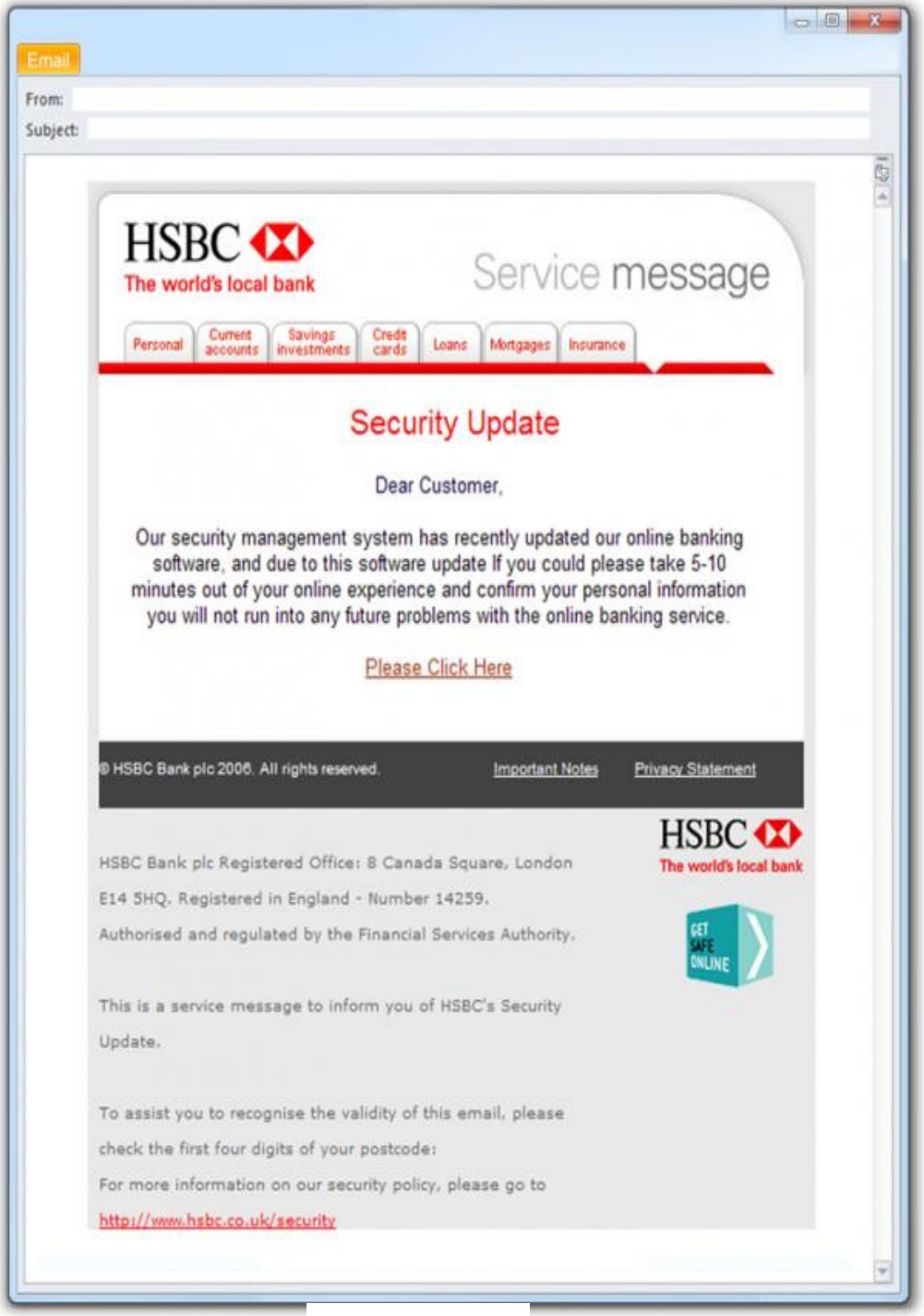
# Email Attachments
# And rules on sending emails

- If an attachment comes in and you do not recognise it do not try to open it
  Always send an email back to the person that has sent you the email.
- If an email comes in and you do not know who it is do not try to open it
- If you are sending an email to many people always use the BCC command ( Blind Carbon Copy) do not put any name in the TO: box or the CC: box. The purpose of this is to hide the email addresses from all the people you send the email to.
- Imagine that you have sent the email to many people and from one of those people in their email address is a bogus or another person sending Jokes etc, and someone on the third party computer is looking at bad things POR**** you could end up getting nasty emails. Remember we would not give out our personal address book.
- If you get an email from someone from the bank asking for you details to update their details on their computer. Do not do it if the bank wishes you to do this they will arrange for you to visit the bank. This is also the same for any other type of online shopping, Paypal etc. In these cases you will need to log on to your account and change where necessary.

Also look at the icon of the attachment if it has an arrow shortcut on it.


**Note this is not the same as the icons on your desktop only applies to email.**








# How to try and spot a virus on an email

When an email arrives if it has an attachment, things to look out for before you open it.

Check who it has come from, are you excepting the email.

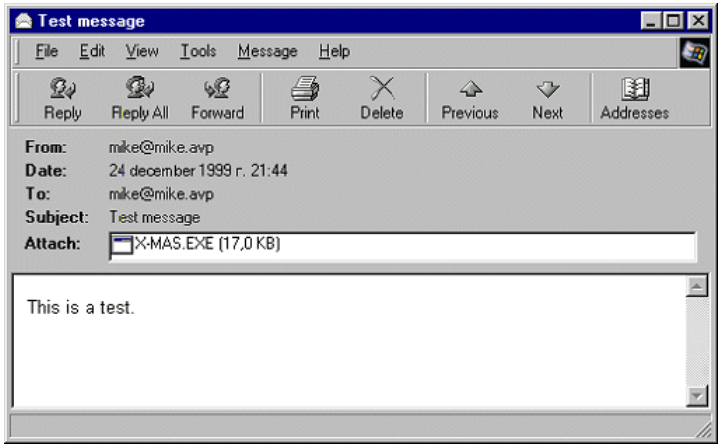
Does the attachment have the correct extension at the end.

Example.
A Picture. Would have - **.jpg or .gif**

A document would have - **.doc or .docx or .pdf**

**These are bad examples and are virus**

1. **name.doc.pdf**
2. **name.pdf.jpg**
3. **Name.exe**



# Internet Safety

- When browsing the internet do not leave too many pages open at one time.
- When looking at your bank account always make sure there is an HTTPS://www this s mean secure.
- Try not to download anything that is not really needed.
- I.E Music, Films, Games, anything that is free means there could be spyware attached.
- When doing online banking you are always asked to put in your Security details. This is the information you are asked for certain letters and numbers from this.
- If you type the wrong letters then it will ask you for the SAME Letters or Numbers again. THEY WILL NOT CHANGE until you logout then login again if this happens close the internet down then do a spyware scan and a virus scan this is called **phishing**
- Clear you Cookie and Tempary Internet files once a week more if you wish.
- If you are looking up medical information never give out your real email address make an hotmail email address for this purpose. Then clear you cookie and Tempary internet files
- If a pop up comes up on the screen saying they are chcking you computer for virus do not click on it.
- If a pop up comes on the screen and you need to close it try going to the bottom of the screen and click on the right mouse button and close on the tab near the stat button
- Always use yor credit card or Paypal where you can as they proctect you from **fraud**



This is an example of a secure website address.