Security Awareness Memo - Phishing Advisory

Phishing is an attack used by the computer hacking and fraud community to lure people to websites that they would normally use. They do this by creating e-mails that look very much like they are being sent by a legitimate company. However, when you click on a link in the e-mail it takes you to a mock-up of the legitimate company's website where you are asked for your logon credentials and potentially credit card or other information. When you supply this information, it is harvested by the hackers/fraudsters. Once they have it they can re-sell the information or use it to commit fraud or other illegal acts. This is a significant problem and even large security savvy organizations like RSA have recently been successfully targeted. Phishing is real and will be with us for the foreseeable future. Understanding this threat has never been more important. Consumers need to be able to identify Phishing attacks to avoid Internet fraud and identity theft.

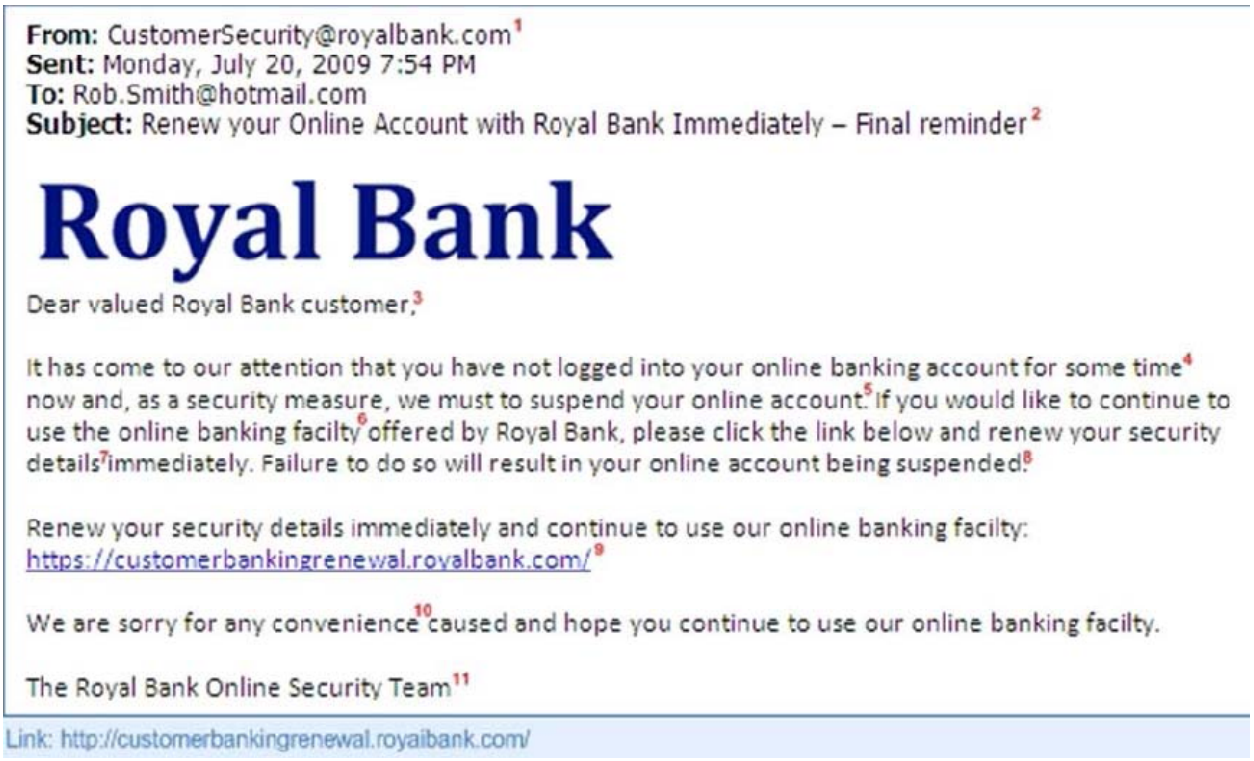
Take Action

The simplest way to protect yourself from Phishers is to avoid clicking on any unexpected link in an e-mail message. *Do not* reply to e-mails soliciting personal information. Having safely ignored the suspicious e-mail, report it.

A significant portion of on-line fraud goes unreported. Some people are too embarrassed to admit they've been taken in. Others simply don't know what to do.

WARNING SIGN #1: Soliciting Personal Information by E-Mail

Financial institutions and reputable online retailers do not send e-mails asking for personal information. Any e-mail that claims to be from a reputable source, but asks for such data is most likely a Phishing expedition.



From: CustomerSecurity@royalbank.com[1]
Sent: Monday, July 20, 2009 7:54 PM
To: Rob.Smith@hotmail.com
Subject: Renew your Online Account with Royal Bank Immediately – Final reminder[2]

Royal Bank

Dear valued Royal Bank customer,[3]

It has come to our attention that you have not logged into your online banking account for some time[4] now and, as a security measure, we must to suspend your online account.[5] If you would like to continue to use the online banking facilty[6] offered by Royal Bank, please click the link below and renew your security details[7] immediately. Failure to do so will result in your online account being suspended.[8]

Renew your security details immediately and continue to use our online banking facilty:
https://customerbankingrenewal.royalbank.com/[9]

We are sorry for any convenience[10] caused and hope you continue to use our online banking facilty.

The Royal Bank Online Security Team[11]

Link: http://customerbankingrenewal.royaibank.com/

1. This sender sounds official, but how can you be sure? Emails can appear to be sent from any address, so it is easy to fake something that looks official.

2. Notice the sense of urgency expressed in the subject. Apparently, it's a final reminder. Do you remember receiving any previous emails on this subject?

3. This is rather generically and impersonally addressed for such an important subject. Why didn't they explicitly address you by name?

4. The statement about not logging in for a while could well be true, lending to the legitimate appearance of the email. Do not be fooled by this tactic.

5. "We must to suspend your online account" – notice the grammatical error here

6. Facilty – spelling mistake. They likely mean facility. The same mistake is made throughout the email.

7. Request for sensitive information. Reputable banks or financial institutions will never request sensitive information by email.

8. Threat of account suspension adds weight to the sense of urgency and importance.

9. The URL in the email appears legitimate, but when you hold the mouse or "hover" over it, you see that the actual hyperlink ends in 'royaibank.com' not 'royalbank.com' as stated

10. Another grammatical error. Likely they meant to say 'inconvenience' rather than 'convenience'.

11. Stating that the email has come from the security team is yet another tactic to appear legitimate.

WARNING SIGN #2: Badly Written E-Mail

Read the message closely. A professional company such as e-Bay or Amazon will not issue any communication containing basic grammatical and spelling errors. A high proportion of phishing e-mails contain such fundamental errors. For example:

Date: Mon, 05 Oct 2009 09:36:32 GMT
From: Webmail Technical Support Team
<masterweboffice04@gmail.com>
Subject: Dear Account User,

Dear Account User,

We are currently upgrading our data base and e-mail account center i.e homepage view. We shall be deleting old email accounts which are no longer active to create more space for new accounts users.we have also investigated a system wide security audit to improve and enhance our current security.

In order to continue using our services you are require to update and re-confirmed your email account details as requested below.

To complete your account re-comfirmation,you must reply to this email immediately and enter your account details as requested below.

Username : .....
E-mail Login ID.....
Password : .....
Confirm password:.....
Date of Birth :.....
Future Password :.....

Failure to do this will immediately render your account deactivated from our database and service will not be interrupted as important messages may as well be lost due to your declining to re-comfirmed your account details to us.

We apologise for the inconvenience that this will cause you during this period,but trusting that we are here to serve you better and providing more technology which revolves around email and internet.

It is also pertinent,you understand that our primary concern is for our customers, and for the security of their files and data.

COMFIRMATION CODE: -/93-1A388-480 Webmail Technical Support Team.

WARNING SIGN #3: Hidden Addresses & Sources

Phishing attacks redirect you somewhere other than where they claim to be going. Check to see if the link in the e-mail is legitimate by resting or hovering over the link. The output will be displayed differently in different browsers but should be the same web address as the displayed link and be the web address of the company allegedly sending the e-mail. (See below) If it is not, again this likely is a Phishing e-mail.

> *Sometimes phishing e-mails direct you to spoofed web sites. Here's an example of the kind of phrase you might see in an e-mail message that directs you to a phishing Web site:*
>
> ***"Click the link below to gain access to your account."***
>
> *HTML-formatted messages can contain links or forms that you can fill out just as you'd fill out a form on a website.*
>
> *Phishing links that you are urged to click in e-mail messages, on websites or even in instant messages may contain all or part of a real company's name and are usually masked, meaning that the link you see does not take you to that address but somewhere different, usually an illegitimate website.*
>
> *Notice in the following example that resting or "hovering" (but not clicking) the mouse pointer on the link reveals the real web address, as shown in the box with the yellow background. The string of cryptic numbers is a generic Internet Protocol address and looks nothing like the company's web address, which is a suspicious sign.*

Example of a masked web address

> *Con artists also use web addresses that resemble the name of a well-known company but are slightly altered by adding, omitting or transposing letters. For example, the address "www.microsoft.com" could appear instead as:*
>
> *www.micosoft.com*
> *www.mircosoft.com*
> *www.verify-microsoft.com*
>
> *This is called "typo-squatting" or "cybersquatting.*

WARNING SIGN #4: Threatening Legal Sounding Messages

Consider the source. From a customer service perspective, no reputable company would send their customers a threatening e-mail. If you receive a threatening e-mail, it almost certainly isn't legitimate. If you think it may be, telephone or send a new e-mail to the legitimate company. Under no circumstances should you respond directly with a return e-mail to the message you just received.

For more Phishing examples, please go to www.google.com and search for "Phishing Examples".