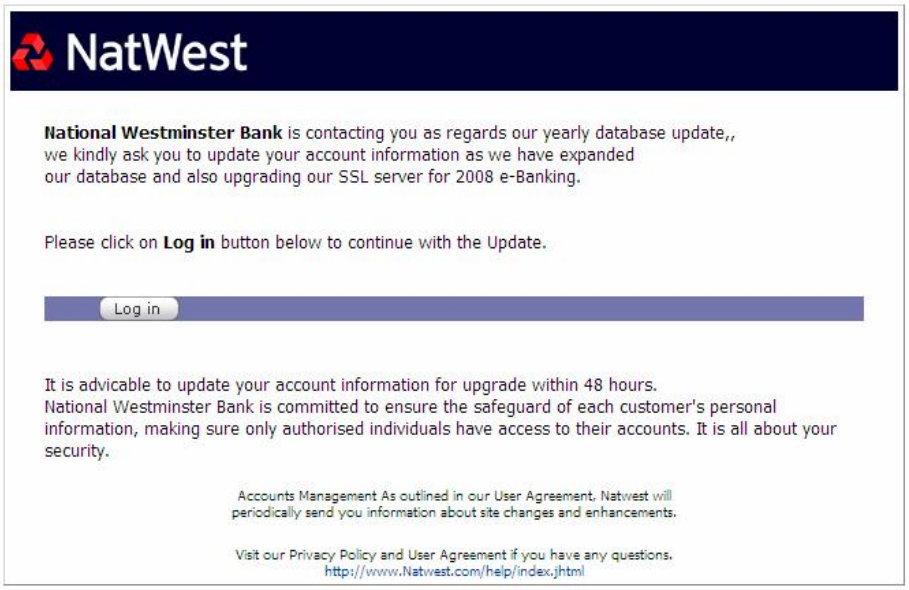
Phishing emails

A couple of weeks ago, I received the following in an email:


NatWest

National Westminster Bank is contacting you as regards our yearly database update,,
we kindly ask you to update your account information as we have expanded
our database and also upgrading our SSL server for 2008 e-Banking.

Please click on **Log in** button below to continue with the Update.

Log in

It is advicable to update your account information for upgrade within 48 hours.
National Westminster Bank is committed to ensure the safeguard of each customer's personal information, making sure only authorised individuals have access to their accounts. It is all about your security.

Accounts Management As outlined in our User Agreement, Natwest will periodically send you information about site changes and enhancements.

Visit our Privacy Policy and User Agreement if you have any questions.
http://www.Natwest.com/help/index.jhtml

However, despite the sender address (Natwest Bank [alert@natwest.com]), this email was not from the NatWest Bank; it was a relatively amateurish attempt to obtain my bank account details. The log in button actually takes you to a website in California that is set up to look like a NatWest login screen. Once your bank information has been entered, the criminal will have full access to your bank account!

I say that this was an amateurish attempt as in the first instance, it has numerous punctuation, spelling and grammatical errors which in the main you would not expect in an email from your bank (Although that's no guarantee!) and the link was obviously to a non-NatWest website.

It is an example of an increasingly used criminal, social engineering technique, known as phishing. Any of us can be targeted by it and so we should all be making efforts to avoid becoming a victim. This example targets NatWest Bank customers, but customers of any other bank or building society are just as likely to be singled out.

The key thing to remember is that you should never, that is NEVER, click on a link in an email to go to your bank's website. You should always type the bank's normal web site address in the address bar at the top of your internet browser and then follow links from there. If at anytime you are suspicious or unhappy about the information that you are being asked for, stop and either email or phone your bank. Never use the phone number or email address from the email; ALWAYS use your bank's normal details either from their website or from the back of your bank statement, etc.

If you ever suspect you have become a victim, contact your bank/building society immediately to inform them, check out the links below for more details.

Most bank websites have further details on how to protect yourself from this kind of crime and some even have email addresses to which you can forward the phishing email.

A few days after receiving this email, I received one claiming to be from eBay, asking me to revalidate my logon details as it was concerned that someone else was using my account. Again, the link button directed me to a non-eBay website. If successful, this would have allowed the criminal to hijack my eBay account, giving them the ability to change banking details and sell non-existent items under my name and this may also have put them a step closer to my credit card payment details.

As you can see, it is not just banking websites that can be mimicked for the benefit of these criminals. Any email that you receive asking for personal information, should in the first instance, be treated suspiciously. In fact the majority of financial institutions will not send you email with these kinds of links and recommend that you always go through their main webpage to login.

Phishing emails are an increasing menace. Security and email software can provide some protection (more on this next time) though as with anything in life you will never be 100% safe. Hopefully knowing the risks will help you to minimise the chances of becoming a victim.

If you have any ideas for future computer related articles, then please email chris@c2s2.co.uk. This article and additional links can be found at www.c2s2.co.uk/VP

Further Info:

http://www.banksafeonline.org.uk/

UK banking initiative to help users stay safe online.

http://www.antiphishing.org/consumer_recs.html

How to avoid phishing scams.

http://www.antiphishing.org/consumer_recs2.html

What to do if you fall victim.

Chris Simon