Phishing

A practical case study

Rohas Nagpal
Asian School of Cyber Laws

Jasa dista tasa nasta mahnun jag phasta (old Marathi saying)

[things are not what they seem and that is why the world gets conned]

Table of Contents

Executive Summary

With the tremendous increase in the use of online banking, online share trading and ecommerce, there has been a corresponding growth in the incidents of phishing being used to carry out financial frauds. Phishing involves fraudulently acquiring sensitive information (e.g. passwords, credit card details etc) by masquerading as a trusted entity.

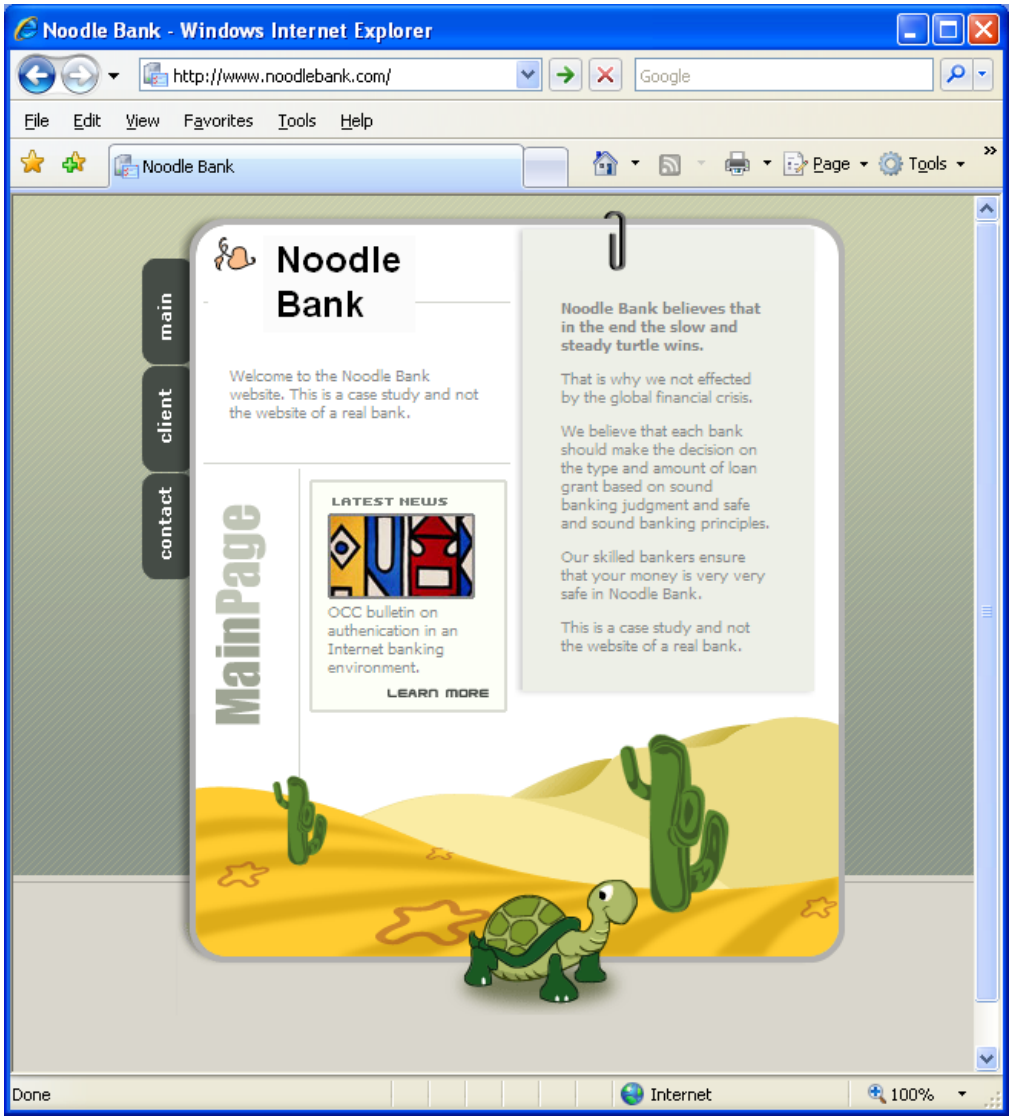
The usual scenario is that the victim receives an email that appears to have been sent from his bank. The email urges the victim to click on the link in the email. When the victim does so, he is taken to “a secure page on the bank’s website”. The victim believes the web page to be authentic and he enters his username, password and other information. In reality, the website is a fake and the victim’s information is stolen and misused.

This case study explains the above scenario in detail along with two fully functional websites, noodlebank.com and nood1ebank.com (i.e. NOOD**L**EBANK.com and NOOD**1**EBANK.com)

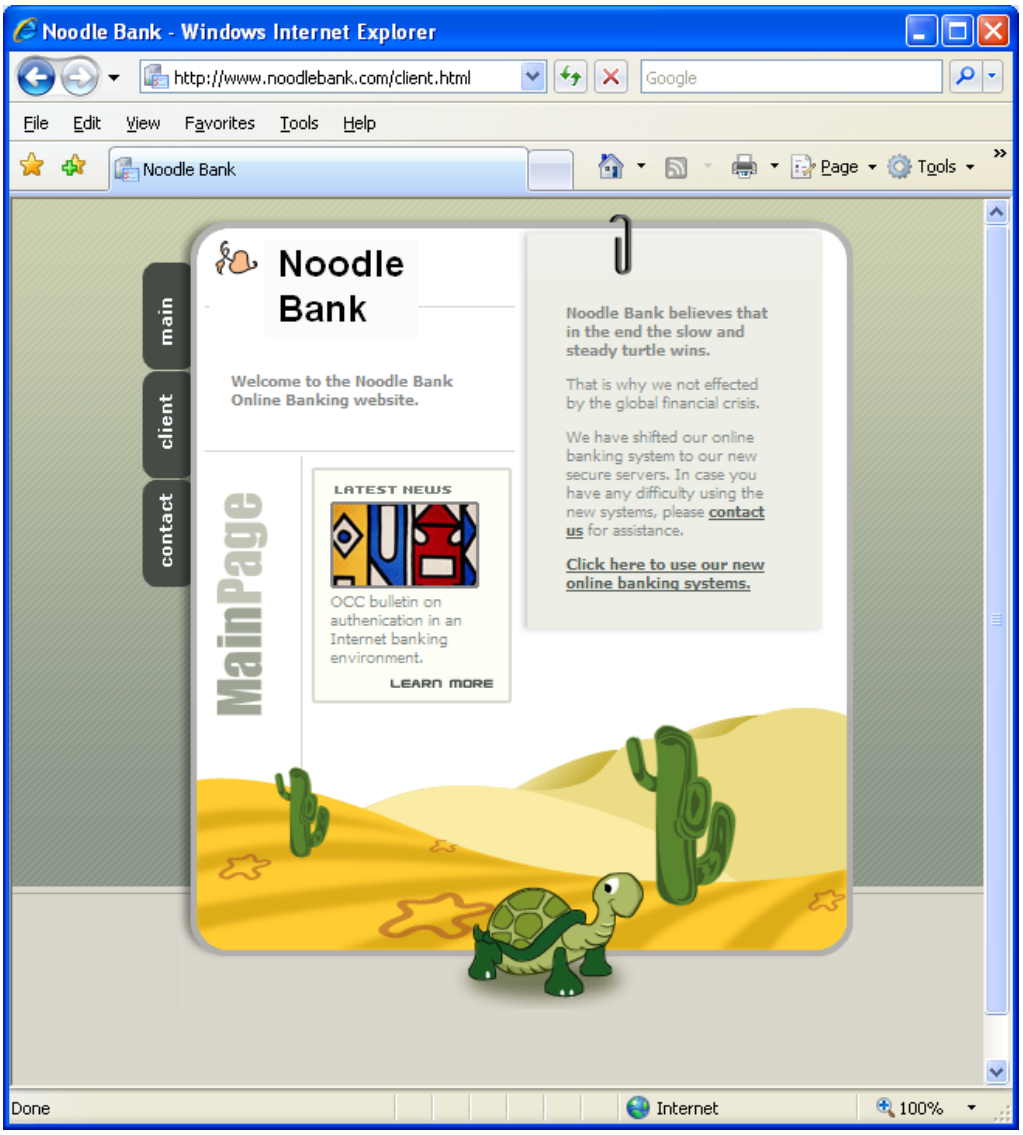
1. The genuine website

NOODLEBANK.com is the genuine website for the purposes of this case study (Note: in reality Noodle Bank is not a bank, it is just a case study).

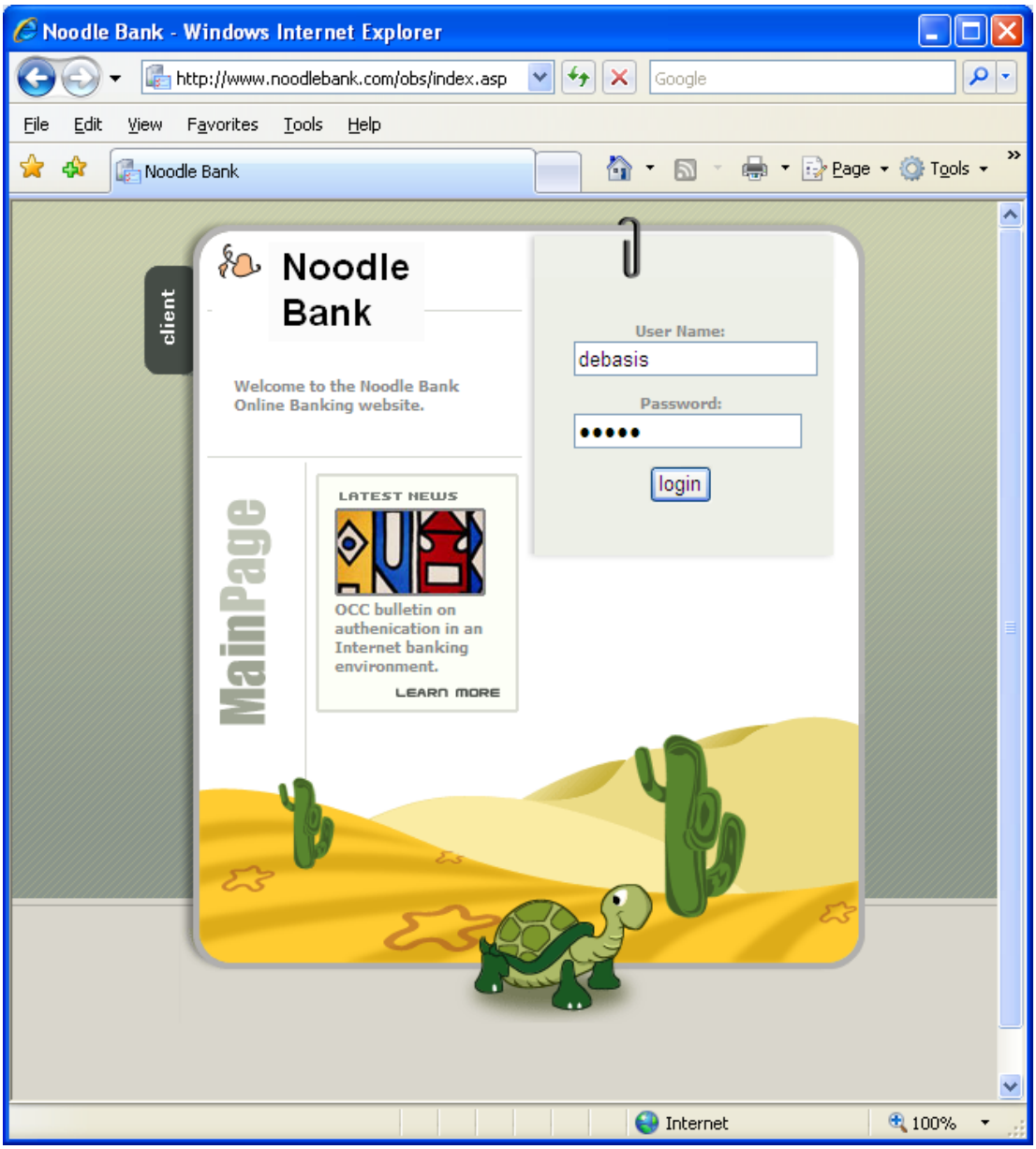
The website can be accessed at: http://www.noodlebank.com



When an online banking customer visits the website, he clicks on "**client**". The following webpage opens up:

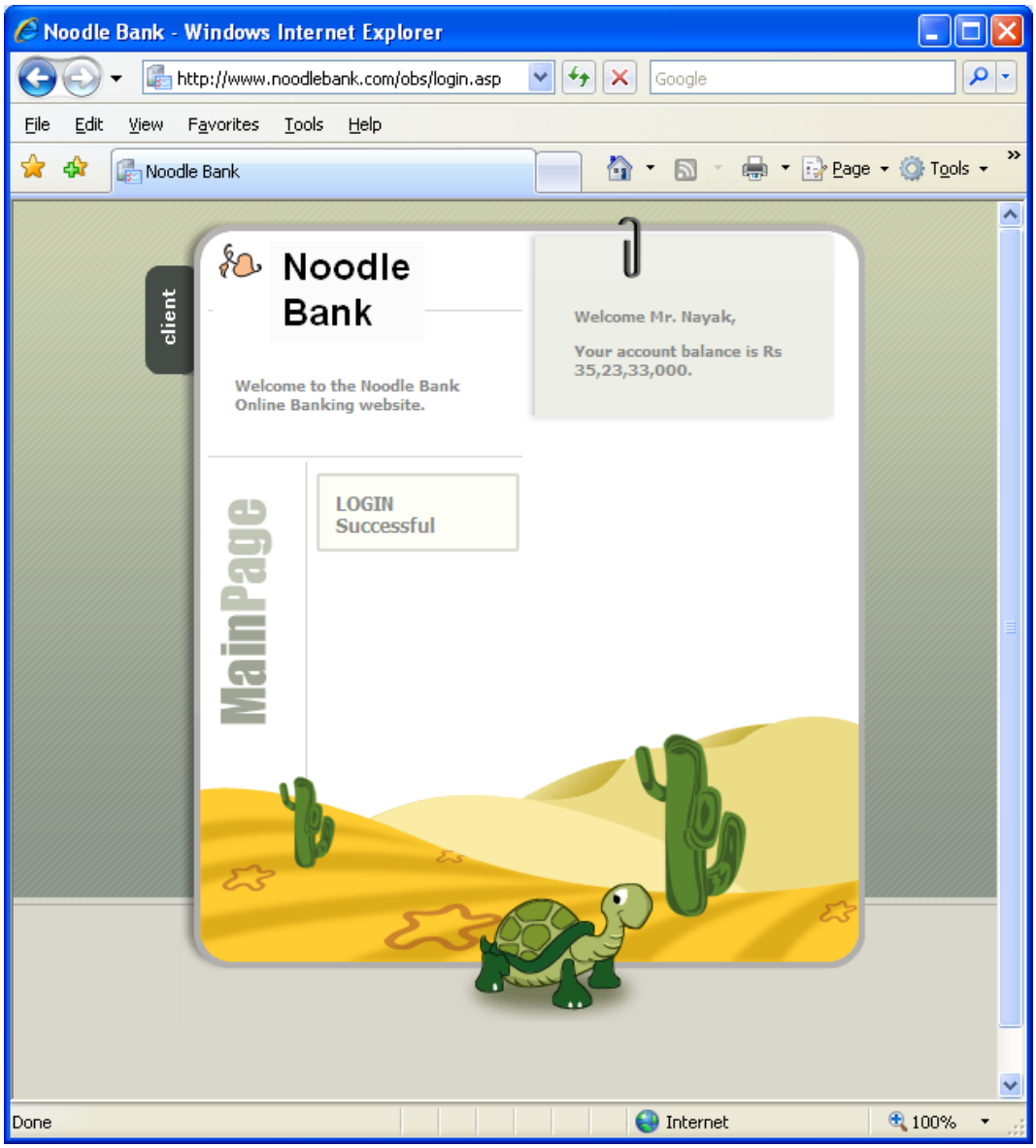


He then clicks on the "**Click here to use our new online banking systems**" link. The following page opens up:



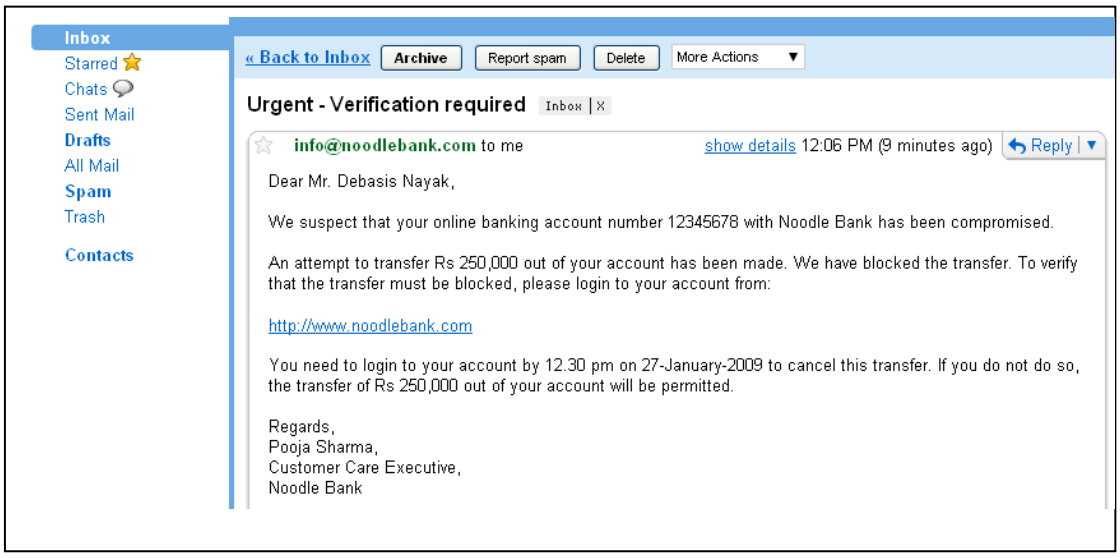
He then enters his usernme (debases) and password (nayak) and clicks on the "**Login**" button.

The next page shows that the login has been successful and displays the account balance etc. (Note: in reality my friend Debasis does not have such a huge bank balance, so please don't abduct him for ransom ☺)



2. The spoofed email

Mr. Nayak receives the following email.



A clever criminal can easily obtain your bank account number and the name in which the account is operated (every cheque that you issue has your name and bank account number !!).

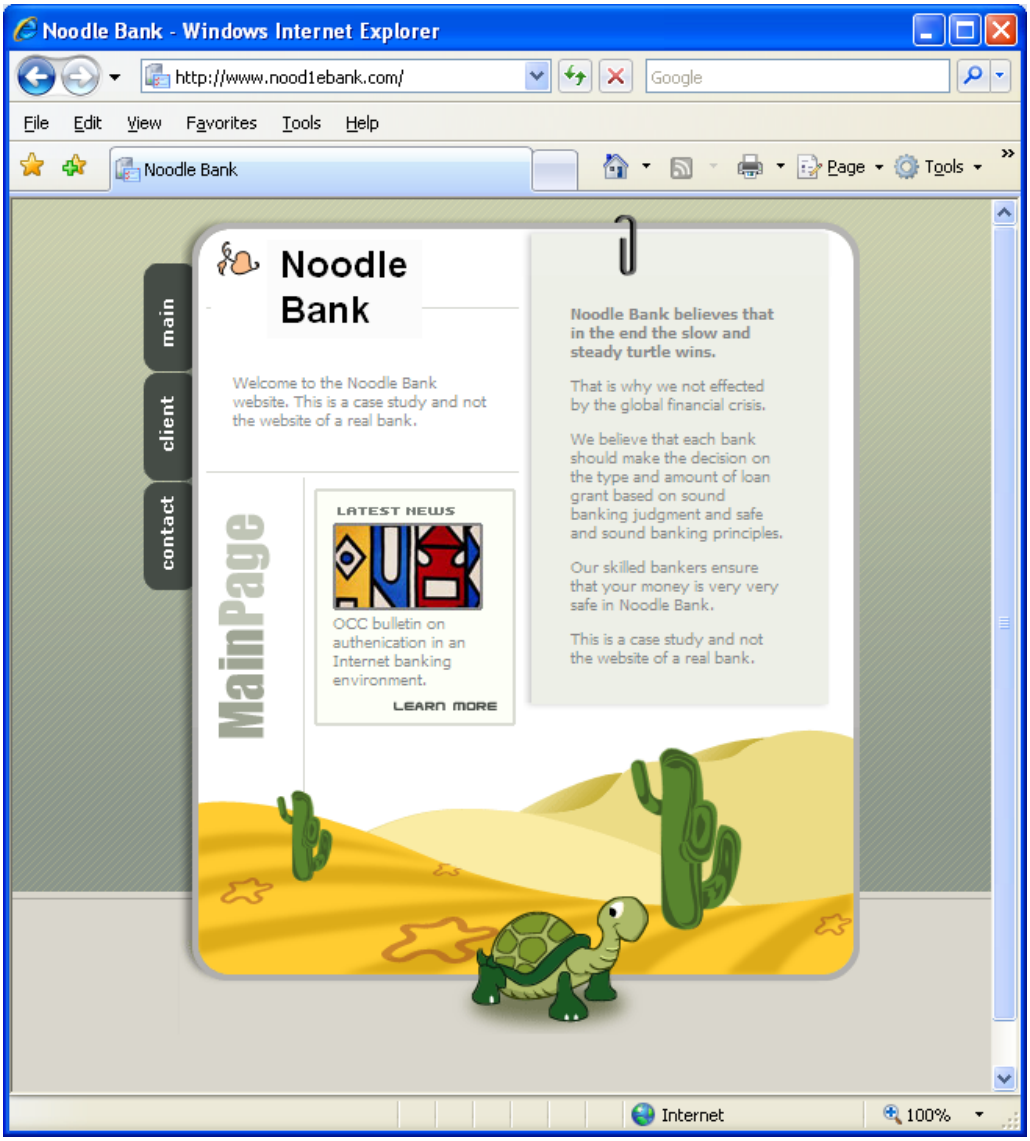
Most users would be scared by an email like this and would click on the URL. On clicking the URL, the site that opens would look exactly like the genuine www.noodlebank.com website but in reality would be a spoofed or fake site.

The fake site in this example is: www.nood1ebank.com

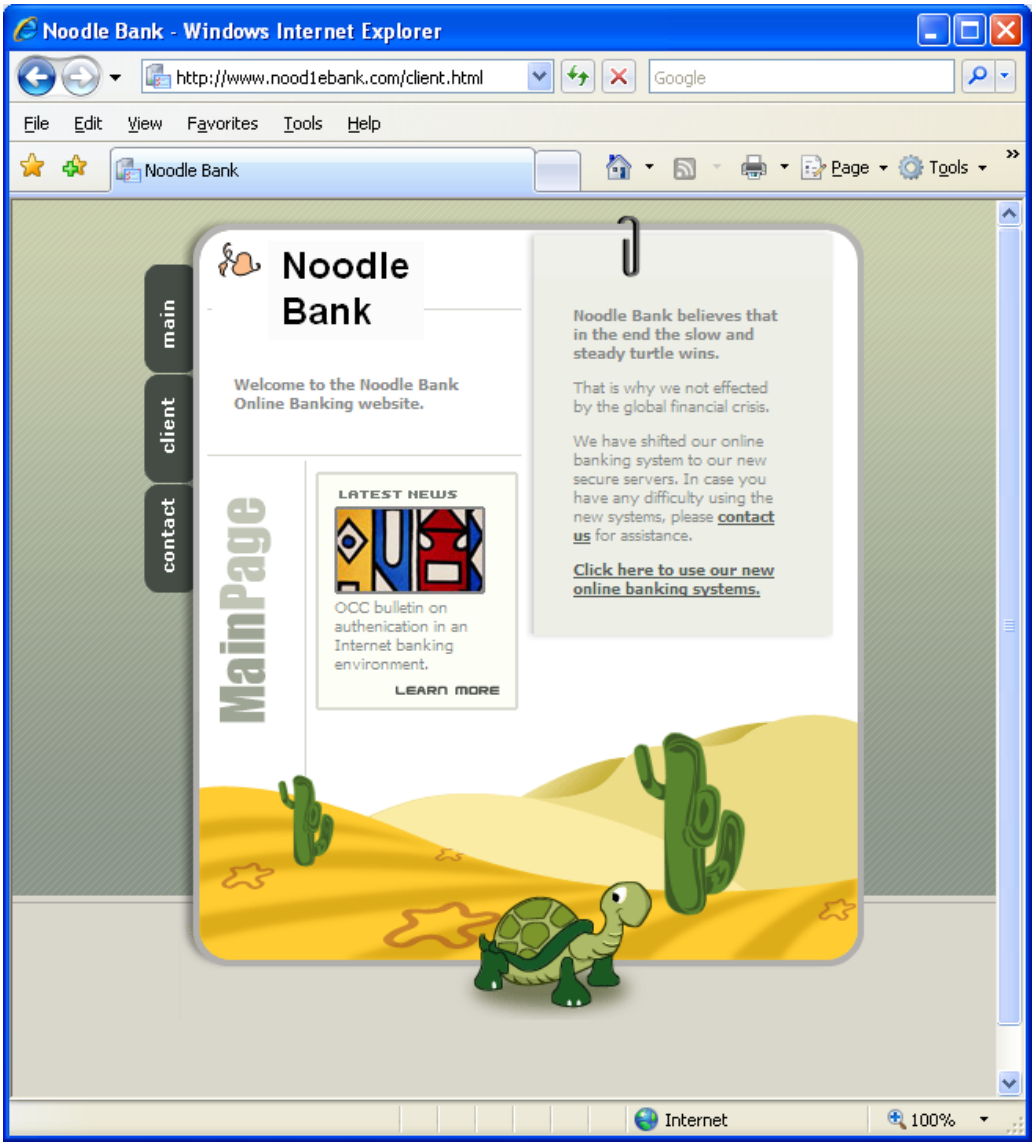
The difference in the name is that the "**L**" is replaced by "**1**" so NOODLEBANK.com becomes NOOD1EBANK.com but when written as nood1ebank.com the difference is very difficult to notice, especially by a scared customer who feels he is about to lose a huge amount of money!

So, effectively, when Mr. Nayak clicks on the link in the email above, he is taken to the NOOD1EBANK.com website and not the NOODLEBANK.com

3. The fake website

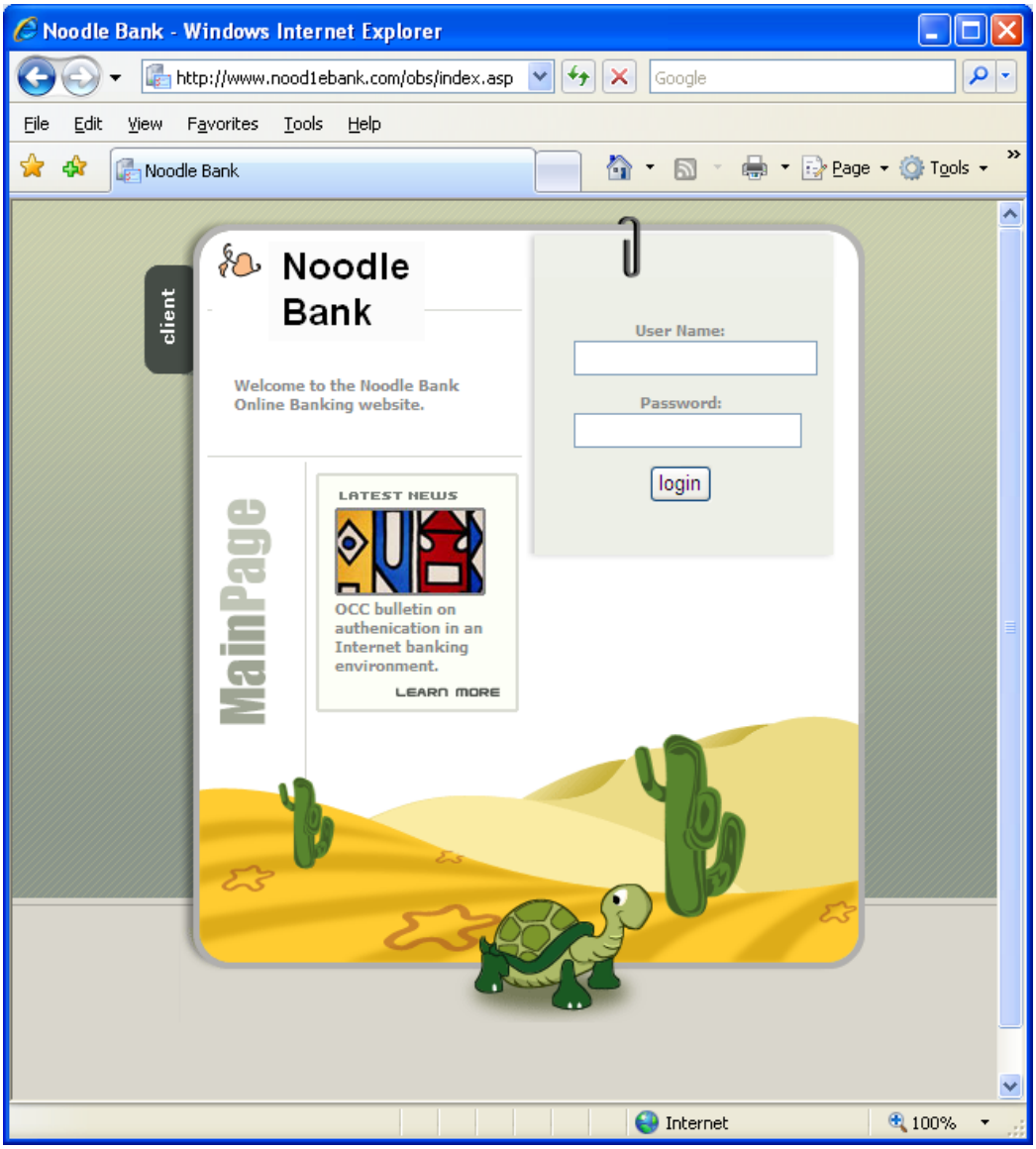


Since the website looks like the original, Mr. Nayak does not suspect anything. He clicks on the "**client**" button.

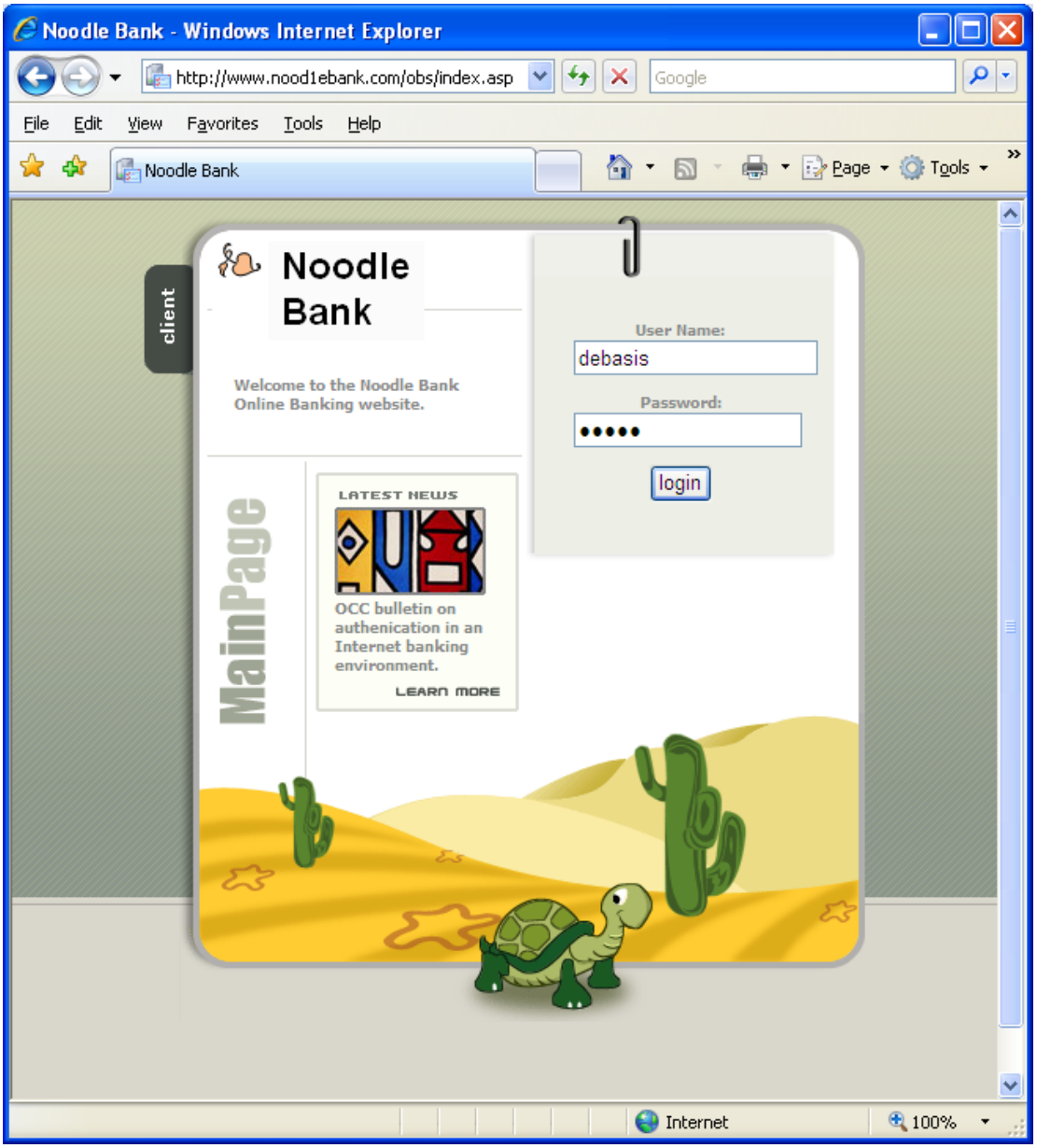


He then clicks on the "**Click here to use our new online banking systems**" link. The following page opens up:

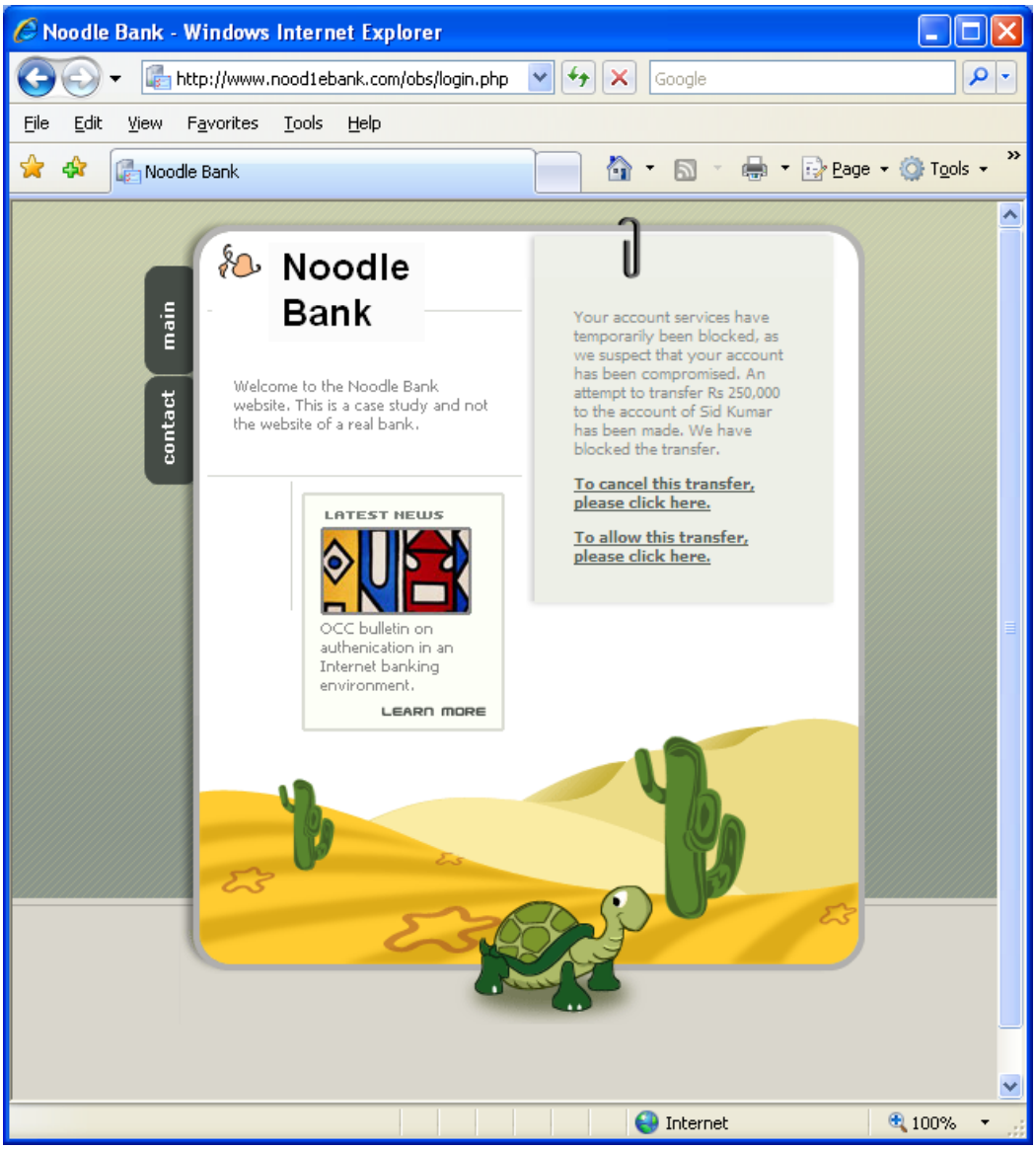
Now the login page opens up.



Since Debasis has nothing to suspect, he enters his username and password and clicks on the "**login**" button.

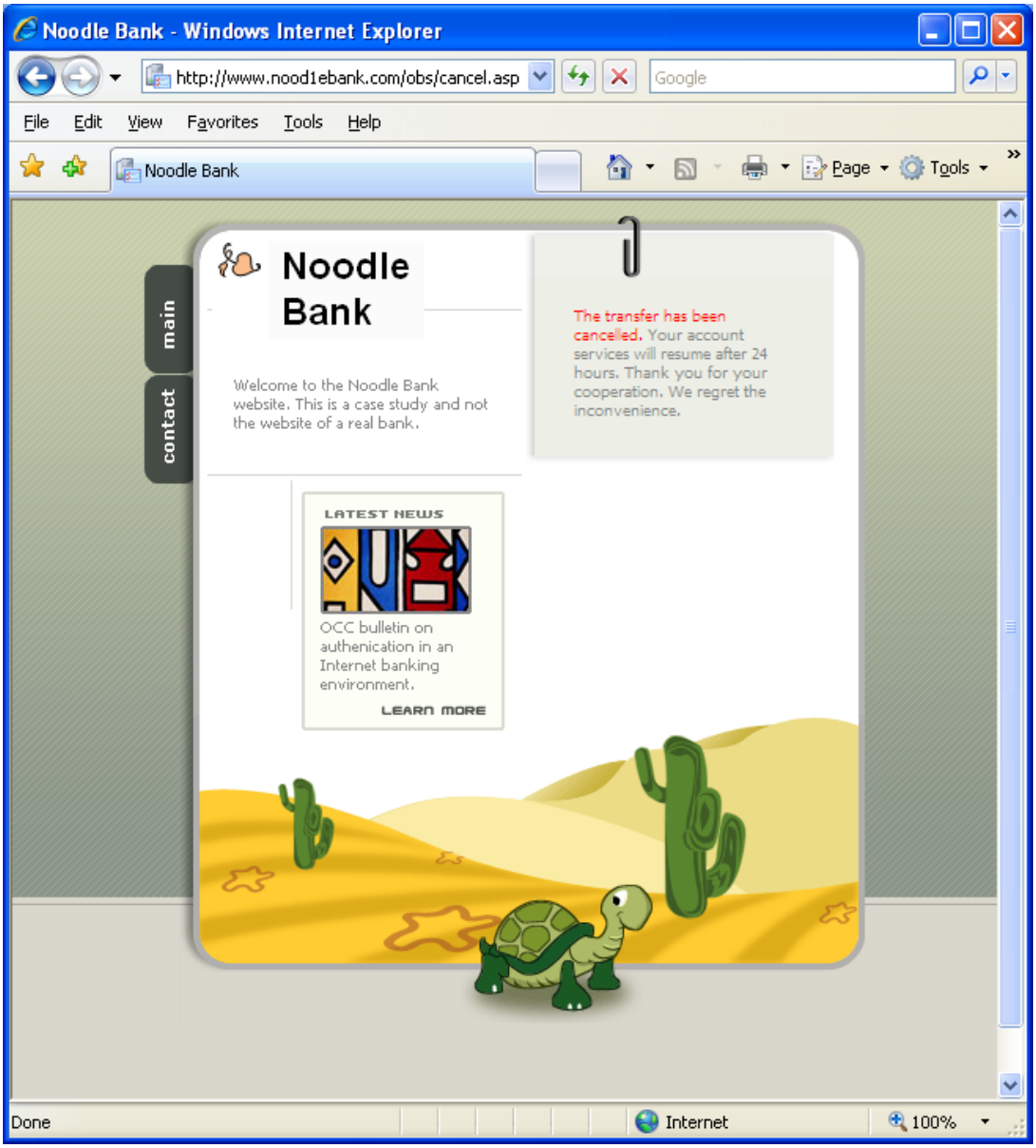


The next page displays a warning notice similar to the email received by Debasis.



He immediately clicks on the first link to cancel the transfer.

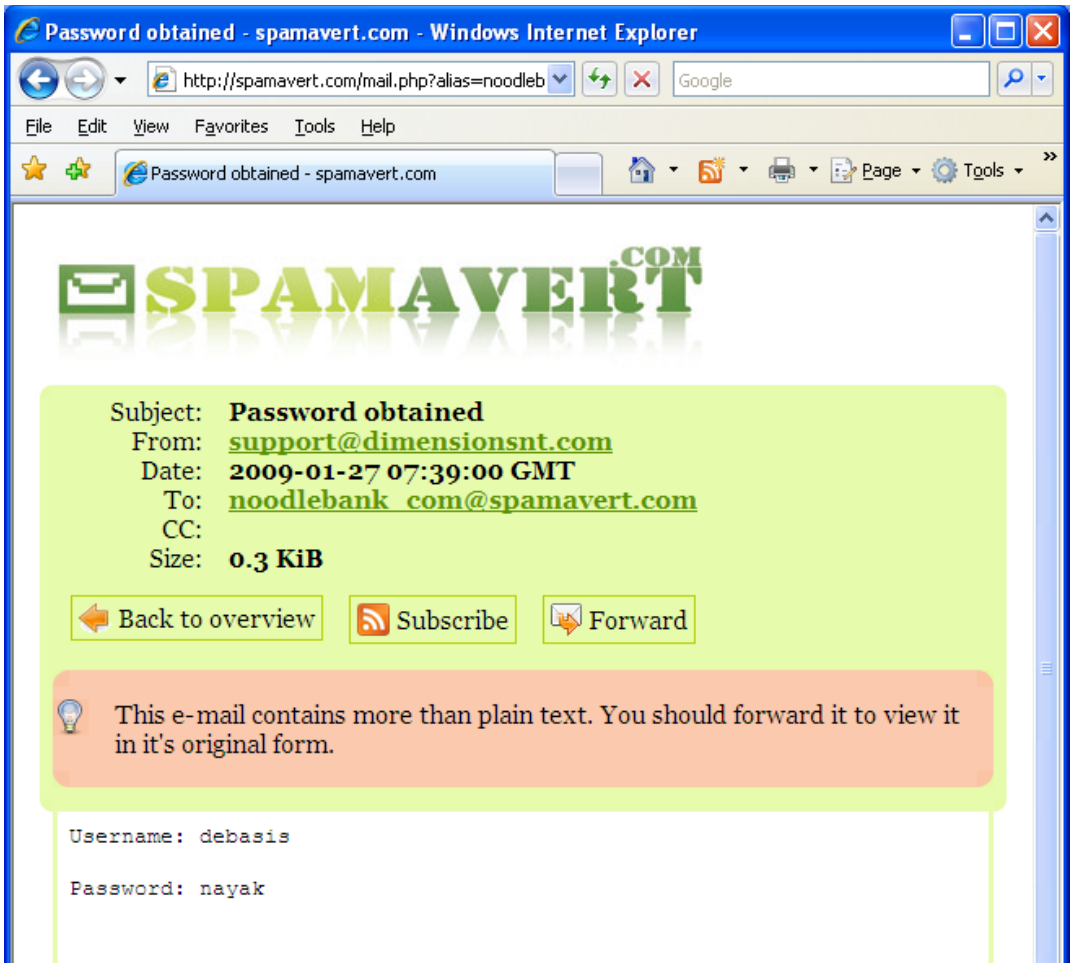
The final page confirms that the transfer has been cancelled.



4. The “steal”

When Debasis entered his username-password at the spoofed website, the username-password was sent across to the criminal carrying out the phishing attack.

In this case study the username-password is sent across to a spamavert email address so that it can be seen by everyone trying out this case study.



So if you are trying out this case study and have entered some username-password at the spoofed website, please visit http://spamavert.com/mail.php?alias=noodlebank_com to view the same.

5. More examples of phishing

In this case study, the user was enticed with a misleading URL. Such urls can be created easily using simple html code such as:

```
<a href=http://www.nood1ebank.com>http://www.noodlebank.com</a>
```

This creates a link such as http://www.noodlebank.com

This link displays the correct url but on clicking takes the user to the spoofed url.

Other methods used by criminals for that phishing include:

1. Using a url with an ip address e.g.

   http://www.NOODLEBANK.com@67.19.217.53

   This url does not lead to noodlebank.com, it leads to the website on the IP address 67.19.217.53

2. Using a split domain name e.g.

   http://www.NOODLEBANK.com.securitycheck.secure-login.nood1ebank.com/login.asp

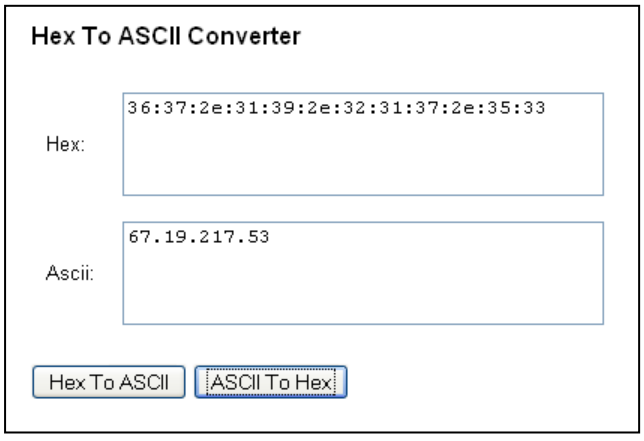
   This url does not lead to noodlebank.com, it leads to the spoofed website.

3. Using an obfuscated url e.g.

   http://www.NOODLEBANK.com%00@%36%37%2e%31%39%2e%32%31%37%2e%35%33

   This url does not lead to noodlebank.com, it leads to the website on the IP address 67.19.217.53

   Use the Hex / Ascii converter at http://www.dolcevie.com/js/converter.html to see how 67.19.217.53 gets converted to %36%37%2e%31%39%2e%32%31%37%2e%35%33



5. Useful URLs

To try out the genuine website:
http://www.noodlebank.com

To try out the spoofed website:
http://www.nood1ebank.com

To see the usernames-passwords being “stolen”
http://spamavert.com/mail.php?alias=noodlebank_com

To learn more about phishing
http://en.wikipedia.org/wiki/Phishing

The Fight Against Phishing: 44 Ways to Protect Yourself
http://www.networksecurityjournal.com/features/44-ways-protect-phishing/

Hex / Ascii converter
http://www.dolcevie.com/js/converter.html