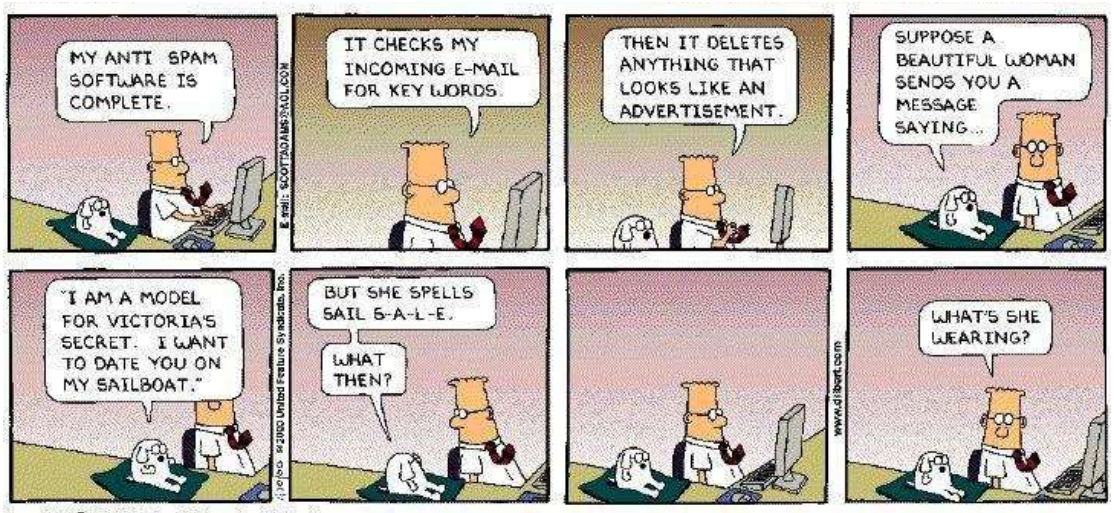
# Chapter 2 - SPAM and Phishing

## SPAM

Everybody knows SPAM or at least understands the predecessors such as junk mail. Ten years before SPAM Email became everybody's favourite pain in the butt, your parents were complaining about bulk snail mails. You know the ones from Readers Digest with "you may have already won £10,000" plastered all over the envelope.


If not that, the same concept is immersed in the stream of letters inviting you to take out health insurance that never pays out, bank loans that you can never pay off and Credit cards that cost the earth - they are the same thing.





SPAM is not an acronym although I like **S**tu**P**id- **A**dvertising e**M**ail - Actually who's to say that's not the proper derivation for the word. Definitively, SPAM is the slang name for Unsolicited Commercial Email.

Anecdotally, based on statistics from my company's spam solution, a typical person will receive from 20 to 200 SPAM emails each day. Most of these are harmless, and I genuinely find many of them rather amusing. How do they know I am overweight and need Viagra!!!!!!!!

However for those that are easily offended or for those that have young children, it can be a serious problem as most of them refer to dimensions of sexual organs, or drugs or pornography.

The growth rate is phenomenal

- 2005 - 30 billion per day
- 2006 - 55 billion per day
- 2006 – 83+ billion per day
- 2007 - 90 billion per day

Comparing the proportions of various types of email, the figure of 72.9% for spam with the corresponding figures for Viruses (around 1% of all emails) and phishing (around 0.5% of all emails) – shows the scale of the spam problem confronting business. After all, this is digital mass-marketing, purely a numbers game. According to Messagelabs in summer 2004 (the peak of spam), spam accounted for 90% of all email traffic

My biggest problem with spam is that it seems to have caused the demise of one of my childhood school days favourite school dinners – Spam Fritters.


Technically spam is illegal in many countries, many of the drugs and watches sold are fake and therefore a breach of the law. However, bulk emails are used in PHISHING – to use technical jargon, SPAM is the initiating attack vector for PHISHING - and PHISHING is incredibly serious.

### *What do I do about spam*

Don't worry And Don't buy anything. You should install decent virus protection software which will come with a spam killer. But please remember to two check your spam folder regularly for emails incorrectly marked as spam

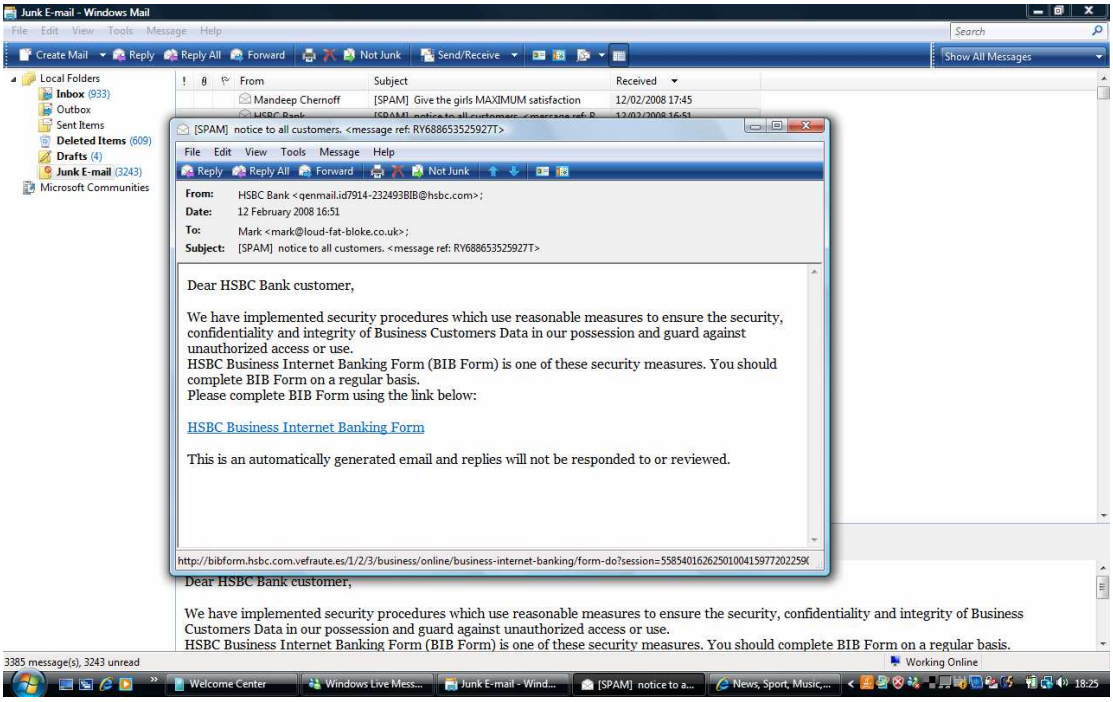
## Phishing

The first real volume of PHISHING emails started with the Nigerian emails. In these e-mails you were almost certainly the recipient of a variable legacy, a true fortune.

The only impediment to you receiving this vast wealth was the requirements for a small payment to cover postage of some valuable documents. If you are foolish enough to provide your bank details in short order you would find your banking cupboard bare.

There is an incredibly funny but sometimes sad website where people publish the interaction with the Nigerian the fraudsters whilst they string them a long. http://www.nigeriamasterweb.com/

Now-a-days, PHISHING attacks always consists of an email and a website. These more advanced PHISHING attempts have become more credible yet they all attempt to steal your Internet banking or auctions site passwords. Just like the one below.




## *The modus operandi*

The attacker will send you a link to a website in an email. The email will relate a story inferring that your account has a problem. Typically,

- Your internet bank has had a security problem
- A customer on an auction site is complaining that you have taken his money and not sent the items you sold him
- A portal claiming to debit your account with 10 days unless you login and cancel.

The email will insist that you need to log on and correct the situation. It will helpfully provide a link. The link in your e-mail will look valid but should you click on it, it will take you to a PHISHING website. This dummy website will look exactly like the real thing but when you log on-it will tell you that your account is locked or that there is the temporary problem with the site. If you leave it a couple of days, you will find that your credentials have been used and you will have definitely lost money.

## What should I do if I get a PHISHING email

Ignore it. No respectable bank will ever inform you of a security problem via email. And if you have reliable antivirus and anti spam solutions on your computer you will only find these e-mails in your junk folder as they will already have been flagged as SPAM or a Phishing attack. If you have a genuine concern, please call the bank on the telephone. Never enter your details into a link provided in an email unless you are absolutely sure that it is valid.

## How does the attack work

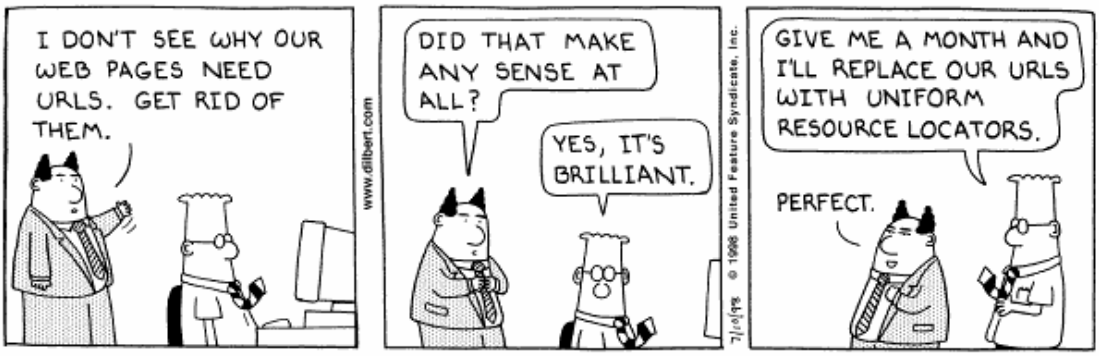
Phishing attacks are simple. All you have to do is craft a cleverly worded email as shown below. However, the first clue to it being a fake is that the Email will not refer to you personally (i.e. “Dear Customer – we have noticed a problem on your account”) and the English is often hard to decipher.

The e-mail will commend you to click on the link. Most of you, except the Pointee haired manager, will know that links are made up of URLs or UNIFORM RESOURCE LOCATORS. These look like this

**http://www.loud-fat-bloke.co.uk/cv.html**

And consist of a:

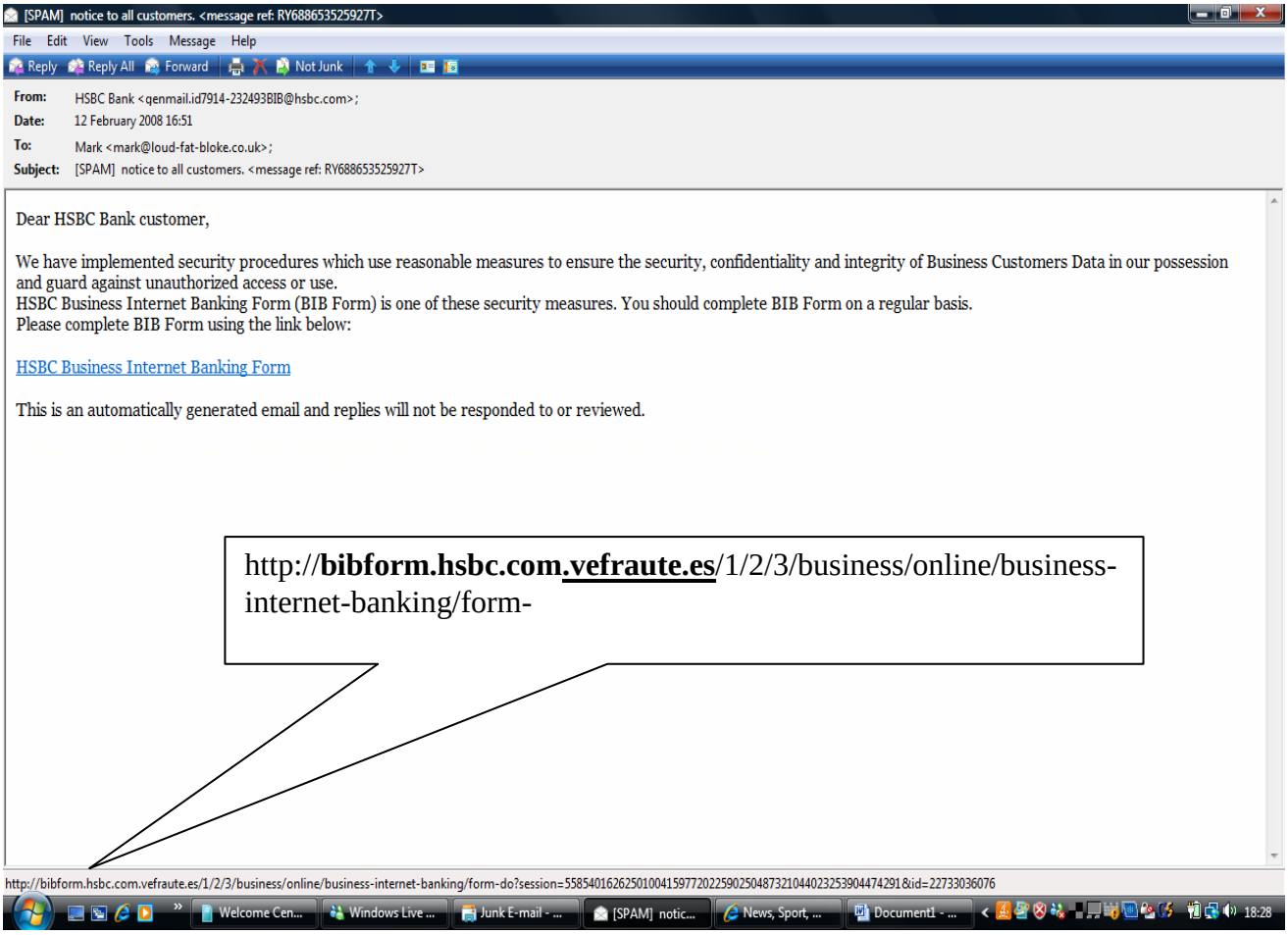
- Protocol bit – for web stuff http
- A server name - www.loud-fat-bloke.co.uk
- And a page name - /cv.html



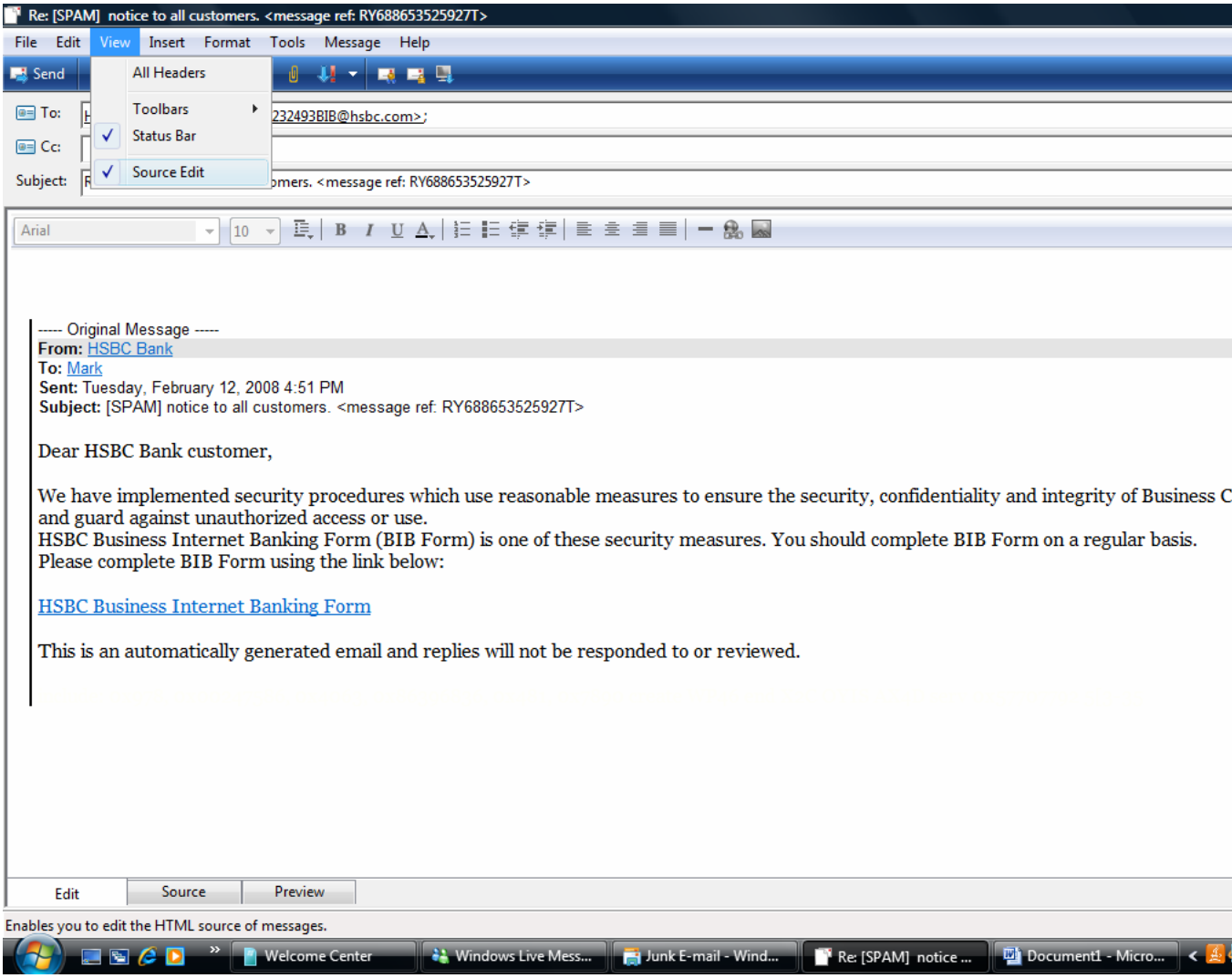



If you hover your mouse pointer over this link, it will display the real web address “behind” the link . If this is a Phishing attack, this will never be a commercial website – These URLS will often have a completely different company name in it or have lost of strange characters –far too difficult for anyone to type in.

If you look at the example below, the webserver isn't within a HSBC domain i.e. somewebserver.hsbc.com. It is actually a Spanish domain (.es ) named **vefraute.es** – they attacker has created a webserver called "**bibform.hsbc.com".**




In Microsoft Outlook, you can explore this further. If you clink reply., You can then go to the toolbar and select Source Edit. This will enable you to see the raw HTML that was used in the email.




<P><FONT face="Georgia, Times New Roman, Times, serif">We have implemented □ security procedures which use reasonable measures to ensure the security, □ confidentiality and integrity of Business Customers Data in our possession and □ guard against unauthorized access or use.<BR>HSBC Business Internet Banking □ Form (BIB Form) is one of these security measures. You should complete BIB □ Form on a regular basis.<BR>Please complete BIB Form using the link □ below:<BR></FONT></P>□ <P><FONT face="Georgia, Times New Roman, Times, serif"><A □ href="http://**bibform.hsbc.com.vefraute.es**/1/2/3/business/online/business-internet-banking/form-do?session=5585401626250100415977202259025048732104402325390447429 1&id=22733036076">HSBC □ Business Internet Banking Form</A></FONT></P>□

If you click on the source tab you will see the text above. Clearly the hacker has tried to hide the true identity of the web site and disguise it as a real banking website.

All the hacker now needs to do is create a website and copy many of the screens from the proper legitimate commercial application. Anyone entering details into the screens will have them recorded for later misuse.

Hopefully you can now see the relationship between the spam and Phishing-when you received a spam email that induces you to buy a fake Rolex, you might not only end up with a lousy watch, you may also find by the time the bad guys have emptied your bank account, that it cost you more than the genuine article. It could cost you everything.

----------end of chapter ----------