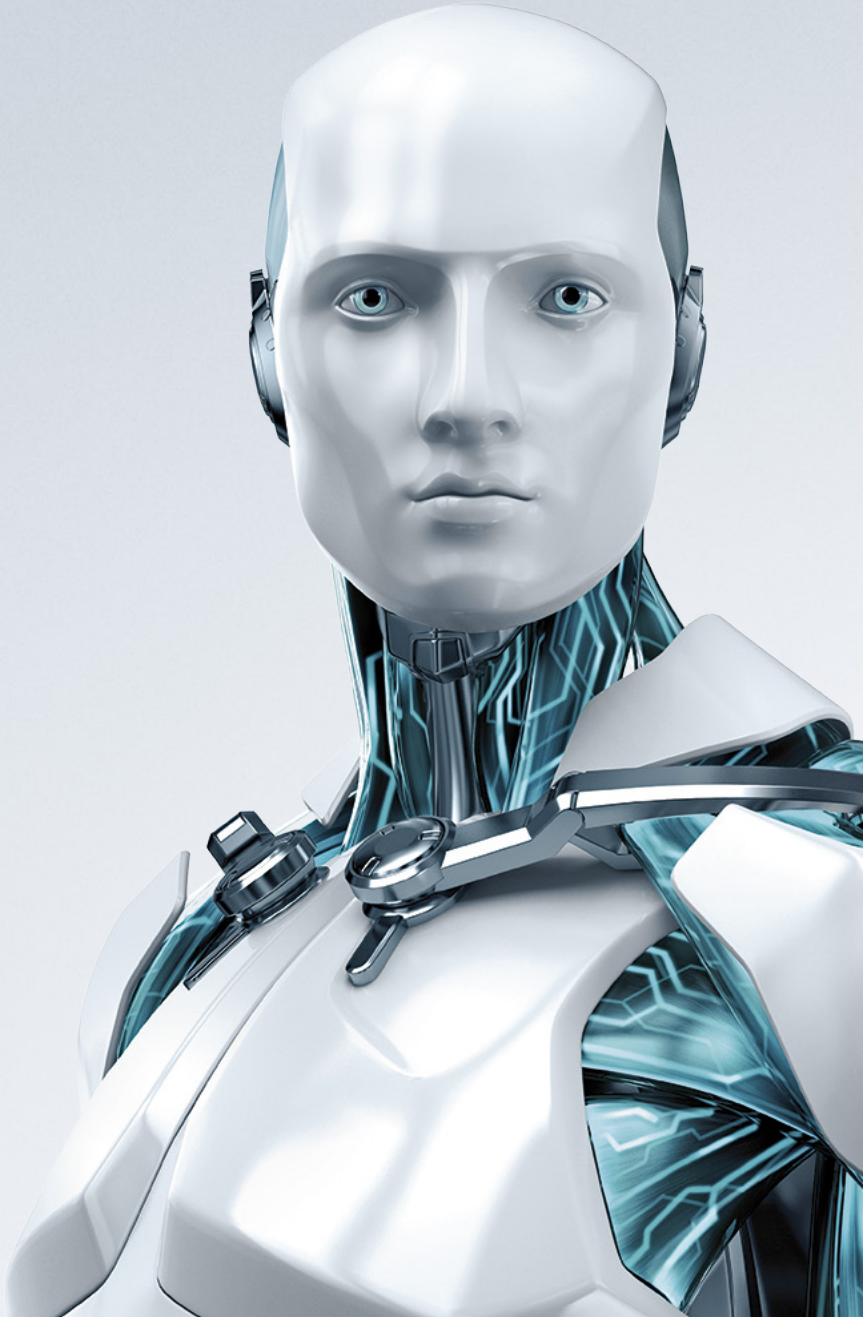
The Thoughtful Phisher Revisited



ENJOY SAFER TECHNOLOGY™

The Thoughtful Phisher Revisited

[A much shorter version of this article appeared in the October 2013 Threat Radar Report as 'The Thoughtful Phisher'. As these particular scam/spam campaigns don't seem to be diminishing, however – indeed, some of the phishing techniques seem to be getting more sophisticated – I thought perhaps it was worth updating and expanding for a wider audience. In fact, I've got so many new samples it's going to take me several blog articles to get them all in, and that's just the interesting ones.]

Now the New Year, reviving last Year's Debt,
The Thoughtful Fisher casteth wide his Net;
So I with begging Dish and ready Tongue
Assail all Men for all that I can get.
(The Rupaiyat of Omar Kal'vin, Rudyard Kipling)

I know New Year is a little way off yet, as I write this series of blogs. However, I've been interested in recent months to see a minor avalanche of phishing scams, most of them targeting users of NatWest, Lloyds and the Halifax (all banks with huge customer-bases in the UK). There's a pronounced family resemblance between these scams. While the earlier ones mostly point to phishing sites apparently hosted in Poland (*.pl) or Niue (*.nu), the most recent include *.be (Belgium – what would Poirot say???) *.br (Brazil), *.es (Spain), *.cl and *.za (South Africa) domain names. I say "apparently" because domains used for phishing are by no means always authentic, registered domains and there's no guarantee that these regional suffixes offer any real clue as to the geographical location of the scammer. In any case phishing sites come and go all the time as they're spotted, blacklisted, and replaced.

On the other hand, if your bank or credit card provider is based in the UK, the chances are that it either has a local domain (*.co.uk) or a (*.com) domain. There may be less obvious possibilities, but an address for a UK bank apparently hosted in South America or Eastern Europe should really ring alarm bells, if only because these are regions particularly noted for phishing activity.

Nevertheless, an apparently legitimate TLD (Top Level Domain) can be spoofed in a variety of ways. That's why we always recommend that you don't click on a URL (web address) in any message that could be a phish. Instead, you should be able to navigate from a known, authentic URL. Still, if a URL looks blatantly improbable, that's a pretty good reason to ignore it immediately and completely.

One way of getting some further insight into the validity of a link is to check the Top Level Domain with a reasonably reliable source like *this one*. Not only will this tell you in some instances that 'your bank' is apparently operating a web site somewhere quite unexpected like the middle of the Pacific, but it may also tell you that there's something phishy about the email address from which a message appears to have been sent.

- Why would an English bank send you emails from Peru?
- Why would any bank send you emails from a domain called boat.com? (Must be a phishing boat...)
- ...Or from parish.net? I know nets are used by phishermen – sorry, fishermen – but clergymen? (I was wondering if it was in good taste to use a 'phisher of men' biblical reference here but *an article on the phys.org web-site* got in first, so the question is academic anyway.)

Oddly enough, while some of the apparent sender addresses in this particular kettle of phish are spoofed – as you'd expect – so as to look as if they were sent from a real domain owned by a phished bank or building society, others make less of an attempt to look like a real bank address. So as well as 'info@lloyds.com', 'onlineservice@nationwide.com', we have 'info@nbs.mobi', 'secure@lloydsbank.mobi' and 'info@lloydsbank.mobi'. These at least sound as if they have some tenuous connection with the banking industry, except that major banks don't usually sit on the.mobi domain, but 'info@services.com', and 'info@service.mobi' are almost as generic as 'info@yahoo.com' would be. (That's just an example, not a known phishing address.) Meanwhile 'info@box.com', 'review@dot.com', and 'info@be.mobi' really make no effort at all to sound like a bank.

As we always say, you shouldn't expect email to be genuine just because it seems to come from [yourbank].com, but you should be even more sceptical if the sender's address looks the least bit 'odd'. For instance, a Hotmail or Gmail address: that is, something that doesn't sound like a legitimate bank email address (like the above-mentioned boat.com). Not that Hotmail or Gmail addresses can't be legitimate in the right context, but respectable financial institutions can afford to use addresses that are clearly from their own domains.

It's also worth checking the address that the mail is sent to. If the 'To' field is empty, that means it's been blind-copied, and that suggests that it's been sent to several recipients. If it's sent to 'Recipients' or 'Customers', it's certainly been sent to many people. And if, despite that, it includes a link that sounds as if it should be personal to you (like one that's supposed to enable you to log in to fix a 'problem') that should certainly tell you that something is very wrong. But you should be suspicious if the mail includes any link, even if it doesn't look particularly odd. (I know 'odd' is rather a broad term, but there are some examples of oddity given below.)

We'd always advise that even if a login link looks OK, it's safer to go through a URL known to be legitimate, not the one that's given in an email. Unless, at any rate, you have no doubt at all that the email is genuine (like one you've verified with the sender by other means). And in general, any email apparently requiring you to click on a link in the message in order to log in to your account is either fake or sent by a bank that knows so little about phishing that you probably ought to consider banking elsewhere.

Here are some typical (and typically odd) sender addresses along with the subject of the message they accompany. N.B. email addresses can be (and usually are) spoofed, so an address might look much more authentic than these: still, while scammers continue to use addresses that don't look genuine, they're worth noting as a potential heuristic. It's actually unlikely that any email address given here is genuine.

Address (apparently from...)	Subject
NatWest Card Services[info@service.mobi]	REFUND SLATED ON YOUR ACCOUNT
Nationwide Building Society[info@nbs.mobi]	Nationwide – Security Certificates Update
Lloyds Bank[secure@lloydsbank.mobi	Lloyds Bank - Existing Customer Notification

The Thoughtful Phisher Revisited

Address (apparently from...)	Subject
Lloyds Bank [info@lloydsbank.mobi]	Lloyds Bank – Existing Customer Notification
Nationwide [info@box.com]	Nationwide – Resolve Your Account
Nationwide [info@services.com]	Nationwide – Upgrade Notification.
Halifax [info@halifax.co.uk]	LloydsTSB – Account Upgrade Notice
NatWest Credit Card [xx@kio.com]	NatWest Credit Card Security upgrade – Must Read
NatWest Card [info@pe.mobi]	NatWest Card – Important Notification.
NatWest [server@parish.net]	Natwest Credit Card Online Services Review
NatWest [veri@cred.com]	Important Notification On Your NatWest Card
NatWest Card Services[info@bt.mobi]	Verify the Error On Your NatWest Card.
MINT [service@mn.mobi]	Your MINT Card Important Notification !
Lloyds Bank [sin@resolve.com]	New security notice on your Lloyds account
MINT [info@edi.mobi]	Fix the Error On Your MINT Card.
MINT [info@large.mobi]	Fix the Error On Your MINT Card Account

Address (apparently from...)	Subject
Lloyds Bank [i@noreply.com]	Account Notification
Lloyds Bank[noreply@lloydsonline.com]	Online Customer Identification Requirements
NatWest Card Service[card@boat.com]	NatWest Credit Card Security upgrade – Must Read
NatWest Card [info@vu.mobi]	NatWest is giving you a chance to shop for free !
NatWest Credit Card[wages@salary.com]	Your NatWest Card Important Notification
NatWest Card [info@be.mobi]	NatWest Important Security Notification.
NatWest [review@dot.com]	NatWest Card Online Service Review
Santander[onlineregistrations@santander.co.uk]	Pending Incoming Credit Notification [or]Pending Credit Alert
NatWest [info@lt.mobi	{NatWest Card Service Secure Message}

And these are some of the links: on the left is the text that it conceals unless you're the sort of professional sceptic (like me) who always passes his mouse over the link to see where it really goes, even if he has no intention of following it.

What you see	What it links to
Kindly Click here now.	hxxp://www.enocowanie.net/model/Natwest-Card/
LOG ON HERE	hxxp://rygielska.pl/wp-includes/css/txt.htm
Click here	hxxp://drukujfoto.pl/fotogaleria/formularze/xy/rrs.htm
click here to avoid services interruption	hxxp://static.teatrwybrzeze.pl/phpThumb/docs/rrs.htm
click here	hxxp://succesformule.nu/frm.htm
SECURE ACCOUNT	hxxp://www.lebenstraum-immo.de/kickers/images/fbfiles/images/gou.htm
click fraud text alert services	hxxp://www.villademerlo.gov.ar/vecino/libraries/wp.htm
Resolve Your Nationwide Account	hxxp://www.globalla.pl/views/img/prettyPhoto/default/NATIONWIDE/nationwide.co.uk.htm
Click Here to avoid services interruption	hxxp://www.quady-gorzow.pl/images/cms/Natwest-Card/
That was me.	hxxp://www.toiture-antony.lu/ps.htm
That was NOT me.	hxxp://www.toiture-antony.lu/ps.htm
Yes, I made this request.	hxxp://www.plasticadosonho.com.br/txt.htm
No, I did not make this request.	hxxp://www.plasticadosonho.com.br/rrs.htm
Resolve Here	hxxp://www.csie.ncue.edu.tw/csie/include/wp.htm
Confirm Pending Credit	hxxp://vservetech.com/files/wpThumbnails/error.php
Unlock Your NatWest Credit Card Online Services	hxxp://www.bornllibres.com/content/user_images/tiny/mcith/Natwest-Card/

Next, we'll look at some specific messages and see what we can learn from them about the kind of social engineering that scammers use.

The Thoughtful Phisher II

In the previous section, we looked at some visual clues that should tip you off that a email from a 'bank' is not to be trusted. Just as interesting here, though, is the variety of social engineering gambits used by this wave of phish campaigns. It's worth taking a closer look at some of the messages just because they include quite a few standard phishing techniques, but some of the others are even more interesting because they're a little more inventive, and those are ones I'm focusing on in this article. the actual text of each message is italicized to distinguish it from the comments I've added.

The Thoughtful Phisher Revisited

What a bargain!

Here is one of the most interesting, in that it moves away from the standard "this is something you must read for your own security" gambit to "here's your chance to get something for nothing". Here's a tip: in these days of economic meltdown, banks aren't giving too much away. (Heck, they can barely be persuaded to pay you interest on the money you entrust to them...)

> ***NatWest is giving you a chance to shop for free !***
>
> *[The unnecessary space before the exclamation mark is the scammer's error, not mine!]*
>
> *Dear Valued Customer,*
>
> *NatWest is giving out free shopping vouchers for your favorites stores for Christmas.*
>
> *This offer is only for NatWest Credit Card Online Services users and it will be valid to use until the 31st of December, 2013*
>
> *To Qualify for this opportunity, Kindly Click here now.*
>
> *After validation your voucher will be sent via text message or posted to your Mailbox.*
>
> *Yours Sincerely,*
> *NatWest Credit Card Services.*

You may notice one glaring Americanism in the spelling (which shouldn't have been a plural either), even though it's sent to a UK email address. Tsk, tsk: whatever happened to knowing your market?

Apart from that, it's a little short on circumstantial information, maybe. Which stores would that be? Well, I suppose my card provider might know something about my shopping patterns, but not very much. Especially as I live in an area not noted for a multiplicity of chain stores. (And not that I have a NatWest card anyway.) What's really interesting and fairly novel, though, is that it uses a carrot rather than a stick, a marketing technique rather than a threat. Note, though, that there's still pressure on you to take action as soon as possible (i.e. before 31st December).

Of course, legitimate marketing is also limited by time or availability: a commercial organization doesn't want to be giving away items it no longer has a budget for, years after the marketing campaign finished. Ask the British division of Hoover, which lost around £50m when it underestimated the demand for giveaway air tickets. Well, you could have asked if it hadn't been *sold off*. Moral: scammers do marketing too. And some of them are better at it than some legit marketers.

Can I have my money back?

Here's another phish with a 'something for nothing' angle: in this instance, you're supposed to believe that:

- You are entitled to a refund – well, banks certainly make mistakes
- Your bank is hurrying to correct its error – not so likely
- Your bank is so incompetent that it can't fix the error without your help.

REFUND SLATED ON YOUR ACCOUNT.

Our record shows that you have a refund slated on your card account due to charges made against your card account by us.

We do apologies for this mistake which was caused by errors from our system. This transaction cannot be completed due to the errors present in your account information.

You are required to click on the LOGON below to fix this problem immediately. Please note, it will take 3 working days to credit your account with the refund.

LOG ON HERE

Thanks
NatWest Card Services

Well, maybe the last point is the most believable: bankers haven't covered themselves in glory in recent years in almost any respect but the ability to draw huge bonuses.

Well, who can resist a refund? Certainly phishers and other scammers are convinced you can't, because they often use this gambit to get you to click on a malicious link or attachment.

Interestingly, there is no 'Dear Valued Customer' (nor any similar generic salutation) here. We've been pointing out for a long, long time, that this sort of generic (non-personalized) salutation just means that the scammer doesn't know your name, because he's mailing the message out en masse to hordes of potential victims. Perhaps scammers have noticed our saying this, and are hoping that having no salutation is less conspicuous than having a generic salutation, and that the recipient will not notice the omission. the moral: the complete absence of a salutation should be considered just as suspicious as a generic salutation. But don't forget that it's also possible – though not so common – to derive a name automatically from an email address. Though that name may or may not be convincing. As far as I'm concerned, 'dear dharley3467'or 'dear dharley@myISP.com' is not a personalized salutation...

Note also that the scammer tells you that it will take three days for the credit to go through. More to the point, it gives him plenty of time to plunder your account. Good to see that phishers still have problems with their English, though, since it's often an indication that all isn't right ... (Sometimes it just means the office junior can't spell, though.)

The life of Riley

Here's another example with a very similar message, but the presentation is much more sophisticated (not to mention looooooonnnnnggggggg...). I have several examples of these that all have more stereotyped subject lines than the previous example: 'Your MINT Card Important Notification !', or 'Fix the Error On Your MINT Card.' So the subject line is alarming enough to catch your attention, though the content is more reassuring. Is that deliberate, so that relief will incline you to lower your defences? I don't know, but it could have that effect.

The Thoughtful Phisher Revisited

Dear Valued Customer,

Our record shows that you have a refund slated on your MINT Credit Card account due to charges made against your MINT Credit Card account by us.

We do apologies for this mistake which was caused by errors from our system. This transaction cannot be completed due to the errors present in your account information.

You are required to click on the LOGON below to fix this problem immediately. Please note, it will take 3 working days to credit your account with the refund.

LOG ON HERE

We hope you find our Online Credit Card service easy and convenient to use.

Yours sincerely,

Paul Riley
Head of Credit Cards

About this email

This email is confidential and intended for the addressee only. Please delete if that is not you.

This is a service message designed to keep you informed of important information associated with your account.

Please do not reply to this email as the address is not monitored. Visit our Support Centre if you have any queries and we'll be happy to help.

Important Security Information

To help you identify our email and as an extra security measure the second half of your postcode is shown at the top. If you have not provided us with this information or you have changed address please contact your local branch to update your details.

MINT will ***NEVER*** *ask for your full PIN or Password when identifying you on the phone or online, and will* ***NEVER*** *ask for Card Reader codes on the phone or when logging in.*

Fraudsters may claim to be the bank to try and access security information. If you receive a call or email from MINT that you are suspicious about, cease the call immediately, or forward the email tophishing@rbs.co.uk. Visit mint.co.uk/security for more information and advice.

MINT is a business name of the Royal Bank of Scotland plc registered in Scotland No 90312. Registered Office: 36 St Andrew Square, Edinburgh EH2 2YB.

First of all, the salutation is non-specific. 'Dear Valued Customer' doesn't mean that your custom is valued but not so much that we can be bothered to personalize this letter by including your name. It means we have no idea who you are, but we're hoping you're a Mint customer gullible enough to fall for a fake login and give us access to your money, which we certainly do value.

Interestingly, the acres of boilerplate verbiage at the end of the pseudo-letter (which may well be lifted from genuine RBS material – the occasional missing space character suggests a cut and paste from PDF to me, but that's just a guess) claims that To help you identify our email and as an extra security measure the second half of

your postcode is shown at the top. Of course, that would have been miraculous, as RBS has no reason to know my address: I'm not one of their customers and the message isn't from RBS at all, so there is no postcode in the message. Clearly, the scammers don't expect you to read the small print. But then, nor do many legitimate financial providers, insurance companies, pensions providers...

Once again, they want you to give them three days to plunder your account and move on. the scanned signature is a nice touch (but proves absolutely nothing, of course). Interestingly, all of the scam messages that appear to be signed by an individual rather than by the name of the bank are claimed to be signed by 'Paul Riley', who appears to be 'Head of Credit Card(s)' for two credit card providers. Well, that's just greedy. We'll get back to the versatile Mr Riley shortly.

(As far as I can tell, there is no Paul Riley who holds a genuine role like this in RBS or its associated financial institutions: if there is, I apologise for any confusion, but I'm sure he is not in any way responsible for the very common misuse of his name in this type of phishing scam.)

The Less Thoughtful Phisher

Less innovatively than the scam mails described in my previous articles (*Phish to phry* and *the Thoughtful Phisher II*), there are those phish messagesthat suggest a problem with your account that you have to log in to fix.

New Year's resolution

Mostly their appeal is to fear and paranoia – I'll look at some of those in due course – but this one is interesting, in that it suggests a technical/administrative error, or maybe a mistake on the victim's part.

> ***Nationwide – Resolve Your Account***
>
> *We are sorry to inform you that your account in NATIONWIDE Internet Banking System is not fully available.*
>
> *During the last update of your account details, our security system reported many required fields not filled.*
>
> *To finish the activation process please follow the link below.*
>
> *Click here to complete your account*
>
> *Thank you for banking with us.*
> *Nationwide Building Society.*

We've probably all had the experience of being unable to complete a transaction because a form isn't constructed to meet the conditions that we find ourselves in: for instance, it might include some fields that are too restrictive in format, such as a postcode format that assumes you have an American zipcode. Or it simply hangs or crashes out for no obvious reason, perhaps a browser with collywobbles. So this approach could be quite convincing for an incautious potential victim.

The English is slightly better on this one than it is on many others, though it still sounds a little 'foreign'. I'm not sure how many potential

victims would be put off by that, though poor English is certainly a viable heuristic for detecting likely phish messages. People who write emails on behalf of a bank in a given region are likely to be native speakers of the language primarily spoken in that region. I'm not sure if 'fully available' is deliberately vague, but it might reassure someone who tried to access the phishing site and tried to access services to which it didn't include valid links.

Here's one that could almost belong to the previous article, since it describes something desirable (an incoming credit), though it also describes an imaginary problem.

It does you credit

> ***Dear Santander Account Holder,***
>
> *At Santander We take our internet banking security seriously. When using our internet banking you automatically benefits from our internet banking promises.*
>
> ***SECURITY NOTIFICATION***
>
> *There is a pending Credit payment into you account from our account department for security reasons invalid records and your 4 digits Security Pin we require you to confirm your account status and profile on file with us before this transfer can be completed.*
>
> *This can be done in 2 simple steps using the reference provided below.*
>
> ***Confirm Pending Credit***
>
> *Please accept our apologies for any inconvenience this action may have caused*
>
> *Yours sincerely,*
> *Online Customer Service*
> *Santander*

As usual, there is no personalization. the English is abysmally bad. And why on earth would they need your PIN in order to facilitate a credit?

Jump to it!

Now we move to a class of phishing message that appeals to your fear of insecurity, if not downright paranoia. This set of messages is characterized by subject lines such as '[your bank] Important Security Notification' or 'Credit Card Security upgrade – Must Read' to create a sense of importance and urgency.

> *Starting from September 25 2013, Lloyds bank introduces new authentication procedures in order to better protect private information of our account holders.*
>
> *Please note that accounts that are not reviewed within 48 hrs are subject to termination.*
>
> *To avoid service interruption click here to avoid services interruption*
>
> *Thank You.*
>
> *Lloyds Banking Group.*

Again, the English isn't bizarrely wrong, but is slightly odd. Note the further use of a common phishing technique: the scammer tries to frighten you into complying before you've had time to consider it properly, by threatening to terminate your account if you don't react immediately.

The Thoughtful Phisher Revisited

It's good for you

And here's another. Short and not particularly sweet, but it doesn't contain an overt threat.

> *Dear Valued Customer:*
>
> *We have upgraded our system security service bringing significant performance improvements and new features, which all Nationwide Building Society customers will enjoy.*
>
> *Due to this upgrade we urge you to please upgrade to this service now for security purpose.*
>
> *Please kindly click here now to upgrade your Nationwide Building Society account to the latest security feature.*
>
> *Thanks.*
> *Nationwide Building Society*

Welcome to Halifax. Errr, Lloyds. Um, Halifax....

The next one is interesting in that it's more than usually sloppy: it can't quite decide which part of the Lloyds banking empire it was sent from. the apparent sender is Halifax [info@halifax.co.uk] but the subject is LloydsTSB - Account Upgrade Notice.

> *Dear Valued Customer,*
>
> *We recently reviewed your account and noticed that your Halifax account details needs to be updated and verified.*
>
> *Due to this, you are requested to follow the provided steps to confirm your Online Banking details for the safety of your accounts.*
>
> *Simply click on secure account to update your Internet Banking details.*
>
> ***SECURE ACCOUNT***
>
> *Thank you for banking with us.*
>
> *Yours sincerely,*
> *Customer Service Department.*
> *Halifax Online Banking*

Scams like this are very much less effective if you bear in mind that the last thing a responsible financial institution is likely to do is to ask you to upgrade your security by going to a dubious link in an unexpected email.

You might also bear in mind that your bank probably knows whether it's called the Halifax or Lloyds TSB. Of course, banks and building societies do merge – Lloyds TSB is itself the result of the merging of Lloyds Bank and what was once the Trustee Savings Bank, and the Halifax is nowadays part of the Lloyds Banking Group – but where both names are used randomly like this, it just means that the scammer has used a standard template and forgotten to change one of the name references to fit the current phishing target.

We'll Text you when we've robbed you

The next one is kind of interesting because it offers a service. But not the one you might think that it's offering.

Valued Customer,

Your NatWest Credit Card is designed to help keep you safe

Receive alerts when we spot a suspicious transaction

Sometimes we spot what looks like a fraudulent transaction on your credit card – so to make sure, we'll call you and check. Better still, why not join our free fraud text alert service?

It's just another way we're working to keep your card and your money safe.

To sign-up for this service, simply click fraud text alert services.

And we'll simply steal your credentials.

And finally one that bolsters the notification of 'service update' with a threat to terminate the account, if the victim doesn't respond immediately:

At NatWest Card Services, we take the job of protecting our customers seriously,

So for your protection we are proactively notifying you of this activity.

Starting from November 13 2013, NatWest Card Services introduces new authentication procedures in order to better protect private information of our account holders.

Please note that accounts that are not reviewed within 48 hrs are subject to termination.

To avoid service interruption Click Here to avoid services interruption

Thank You.
NatWest Card Services.

So. No pressure then. Now things are starting to get much more overtly threatening, as we'll see in the final section.

Phear of Phishing

From the sort of 'visit this link and update or we'll cancel your account' message that we saw in the previous blog in this series (The Less Thoughtful Phisher), it's a short step to trying to frighten you into logging into a malicious URL by telling you there's already suspicious activity on your account.

Dear Valued Customer,

Your Nationwide Account has been limited due to the unusual login attempt to your online banking.

Resolve Your Nationwide Account

Thanks,
Nationwide Building Society.

Well, fall for this and suspicious activity will certainly happen, though it may take a while before you realize it has taken place.

Yes, it's me. No, it's me.

And here's a short example of a type I've been seeing a lot of recently. the potential victim might think that simply confirming or denying that they requested a change is safer than linking to an obvious login link – after all, we keep telling you not to go directly to a link in a message you can't trust – but the scammer isn't going to be content with a simple yes or no. At some point in the process you're going to

have to share your login details, and the scammer will have got what he wants. And you may not be surprised to note that – as with most examples of this type of message I've seen so far – the 'yes' and 'no' links are exactly the same. It seems to have started to occur to them sooner or later, though, that the social engineering might be a little more convincing if they went to a different page.

> *Dear Valued Customer,*
>
> *This is a short email to let you know that your NatWest Credit Card Online Services security details was recently changed on Monday, November 11, 2013 at 9:32:48 AM. Please confirm that this request was made by you.*
>
> *Yes, I made this request.*
>
> *No, I did not make this request.*
>
> *Best wishes*
>
> *Paul Riley*
> *Head of Credit Card*

What an interesting coincidence that the Head of Credit Cards at MINT has, according to the message of which I generated a screenshot in an earlier blog in this series, exactly the same name as the Head of Credit Card(s) at NatWest. At least, so the number of NatWest phishing messages I've seen with that signature would seem to indicate. Unless he's changed jobs. Or, more likely, some phishing phreak thought that Paul Riley was a name likely to inspire confidence in UK readers. Just as I always feel reassured when I get offers from various dictator's widows to share millions of dollars. :)

We don't know why, but we know exactly when...

Here 'he' is again with a more comprehensive message. I love the precision with which they report the date and time of this imaginary breach.

> *Dear Valued Customer,*
>
> *An attempt to access your NatWest Credit Card Online Services was denied on: Thursday, 07 November 2013 at 7:03:55 GMT*
>
> *Access was denied for one of two reasons:*
>
> *The response to your personal logon details did not match our records*
>
> *A recent change in your contact information.*
>
> *If you remember trying to access NatWest Credit Card Online Services on the above date and time, please select "That was me."*
>
> *If you do not remember trying to access NatWest Credit Card Online Services on the above date and time, please select "That was NOT me." You will then be prompted to Confirm your account profile on file with us.*
>
> *That was me.*
>
> *That was NOT me.*
>
> *Best wishes*
>
> *Paul Riley*
> *Head of Credit Cards*
>
> *P.S...don't forget that you can make a payment online using the payments and transfers link once you have logged on.*

Please do not reply to this email. It is for notification only as this mailbox cannot accept incoming mail. If you need to contact us then use the Contact Us link at www.natwest.com.

National Westminster Bank plc. Registered in England and Wales (Registered Number 929027)

Registered Office: 135 Bishopsgate, London EC2M 3UR.

Authorised and regulated by the Financial Services Authority.

This email message is confidential and for use by the addressee only. If the message is received by anyone other than the addressee, please return the message to the sender by replying to it and then delete the message from your computer. Internet emails are not necessarily secure. the Royal Bank of Scotland plc does not accept responsibility for changes made to this message after it was sent.

Whilst all reasonable care has been taken to avoid the transmission of viruses, it is the responsibility of the recipient to ensure that the onward transmission, opening or use of this message and any attachments will not adversely affect its systems or data. No responsibility is accepted by the Royal Bank of Scotland plc in this regard and the recipient should carry out such virus and other checks as it considers appropriate.

Talk about adding value. Two possible reasons for the 'problem' you have to log on to resolve, an opportunity to make a payment while you're at it (more money? Bring it on!), and a lengthy disclaimer that looks like it was scraped from a real site or document.

Newly MINTed

And here is Mr Riley, again, apparently moonlighting back with MINT. I wonder if he's getting paid by both divisions.

And yes, this time the scammers used different links for yes and no. Apart from the change of provider, the value-added disclaimer is almost identical to the previous message.

Dear Valued Customer,

Our records shows that your MINT Credit Card Online Services security details was recently changed on Tuesday, November 05, 2013 at 06:09:42 PM. Please confirm that this request was made by you.

Yes, I made this request.

No, I did not make this request.

Best wishes

Paul Riley
Head of Credit Cards

Again, much of the detail like the address for the Registered Office indicates scraping from a real site. I haven't reproduced it as it was very similar to the wording in previous example.

The Thoughtful Phisher Revisited

Implore-sible...

Dear Account Holder,

We noticed a violation of our services on your account and for this reason, your account will be closed if you fail to resolve the issue within the next 48 hours.

This will only take a moment, We implore you to resolve the issues on your account immediately to restore access.

Resolve Here to complete the process.

Sincerely,
Lloyds Bank

I like it. Short and to the point. Log on and give us your money or we'll close your account. Even though, as usual, we don't know anything about you or your account... I really like 'we implore you': it's always comforting when a scammer asks nicely.

Doomed!

At Lloyds, we take your security very seriously indeed. In fact we've invested in a host of measures that help protect you and your money

Recent transactions involving your designated accounts was revoked.

Follow the provided steps to restore your online access and to review your account status

Online banking Log on

Sincerely,
Lloyds Bank

Eek! Revoked! I'm doomed. (I've been seeing a lot of these, but this one is enough to give you the idea...)

Browserbeaten

And one last shot across the browser from 'Paul Riley'.

Dear Valued Customer

Thank you for choosing NatWest Online Credit Card Services.

At NatWest Credit Card Services we are continually making improvements to protect our customers from fraud, but there are also things you should do to ensure that your details are kept safe when using your card online. We ask that you always have the latest anti-virus software protection on whichever device you use to access NatWest Online Credit Card whether that be your laptop, pc or mobile. We also offer free 'Rapport' security software protection that works alongside your anti-virus software to give added online protection.

At NatWest Credit Card Services we have introduced new additional security measures and updated our software to protect our Online Credit Card Account users. the security update will be effective immediately and requires our NatWest Credit Card customers to update their access. Please click on "Continue" below to update yours today.

CONTINUE

Find out more

If you have any questions about using your card online, we're happy to help. Simply visit our Help 24/7 service.

Yours sincerely,

Paul Riley
Head of Credit Cards

The Thoughtful Phisher Revisited

Rapport, of course, is Trusteer's security software, which has been genuinely recommended and made available by various banks to their customers. Nice touch of circumstantial suggestion of good intent, and perhaps an indication of content scraping, but the real intent here is far from benevolent.

And finally...

At least for this series.

> *Dear Valued NatWest Card Customer*
>
> *Due to too many errors on your NatWest Credit Card account.*
>
> *Your access to NatWest Credit Card Online Services has been locked out. Please use the link below to unlock.*
>
> *Unlock Your NatWest Credit Card Online Services*
>
> *Please do not reply to this message. For questions, please call Customer Service at the number on the back of your card. We are available 24 hours a day, 7 days a week.*

Happily, this has some major weaknesses that should alert most people immediately to what they're looking at here.

1. There is no personalization to prove they're addressing a known customer
2. There's an inline link to a very dodgy-looking URL
3. If you were in any doubt about this, you could check it instantly by going to a known genuine URL to log in, where hopefully you would be able to log in without a problem.

David Harley CITP FBCS CISSP
ESET Senior Research Fellow