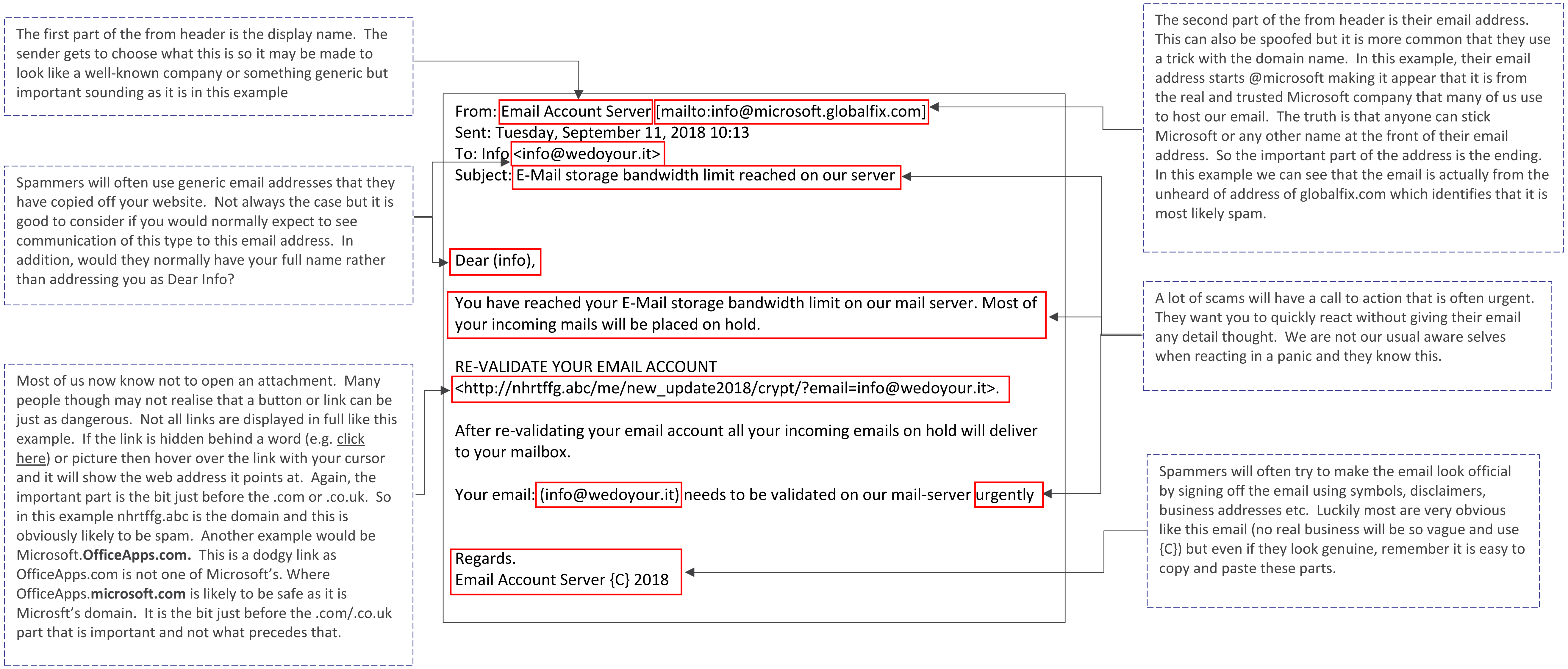
WE DO YOUR IT

# Top Tips for Spotting Spam

*It used to be easy spotting spam and fake emails when it was just Rolex watches, cheap Viagra and Nigerian princes promising you a share of their fortune. These days though, the scammers have got a little smarter and now employ a wide range of tactics to bypass filters and trick you.*

## Here are some things to look out for:



The first part of the from header is the display name. The sender gets to choose what this is so it may be made to look like a well-known company or something generic but important sounding as it is in this example

Spammers will often use generic email addresses that they have copied off your website. Not always the case but it is good to consider if you would normally expect to see communication of this type to this email address. In addition, would they normally have your full name rather than addressing you as Dear Info?

Most of us now know not to open an attachment. Many people though may not realise that a button or link can be just as dangerous. Not all links are displayed in full like this example. If the link is hidden behind a word (e.g. click here) or picture then hover over the link with your cursor and it will show the web address it points at. Again, the important part is the bit just before the .com or .co.uk. So in this example nhrtffg.abc is the domain and this is obviously likely to be spam. Another example would be Microsoft.**OfficeApps.com.** This is a dodgy link as OfficeApps.com is not one of Microsoft’s. Where OfficeApps.**microsoft.com** is likely to be safe as it is Microsft’s domain. It is the bit just before the .com/.co.uk part that is important and not what precedes that.

From: Email Account Server [mailto:info@microsoft.globalfix.com]
Sent: Tuesday, September 11, 2018 10:13
To: Info <info@wedoyour.it>
Subject: E-Mail storage bandwidth limit reached on our server

Dear (info),

You have reached your E-Mail storage bandwidth limit on our mail server. Most of your incoming mails will be placed on hold.

RE-VALIDATE YOUR EMAIL ACCOUNT
<http://nhrtffg.abc/me/new_update2018/crypt/?email=info@wedoyour.it>.

After re-validating your email account all your incoming emails on hold will deliver to your mailbox.

Your email: (info@wedoyour.it) needs to be validated on our mail-server urgently

Regards.
Email Account Server {C} 2018

The second part of the from header is their email address. This can also be spoofed but it is more common that they use a trick with the domain name. In this example, their email address starts @microsoft making it appear that it is from the real and trusted Microsoft company that many of us use to host our email. The truth is that anyone can stick Microsoft or any other name at the front of their email address. So the important part of the address is the ending. In this example we can see that the email is actually from the unheard of address of globalfix.com which identifies that it is most likely spam.

A lot of scams will have a call to action that is often urgent. They want you to quickly react without giving their email any detail thought. We are not our usual aware selves when reacting in a panic and they know this.

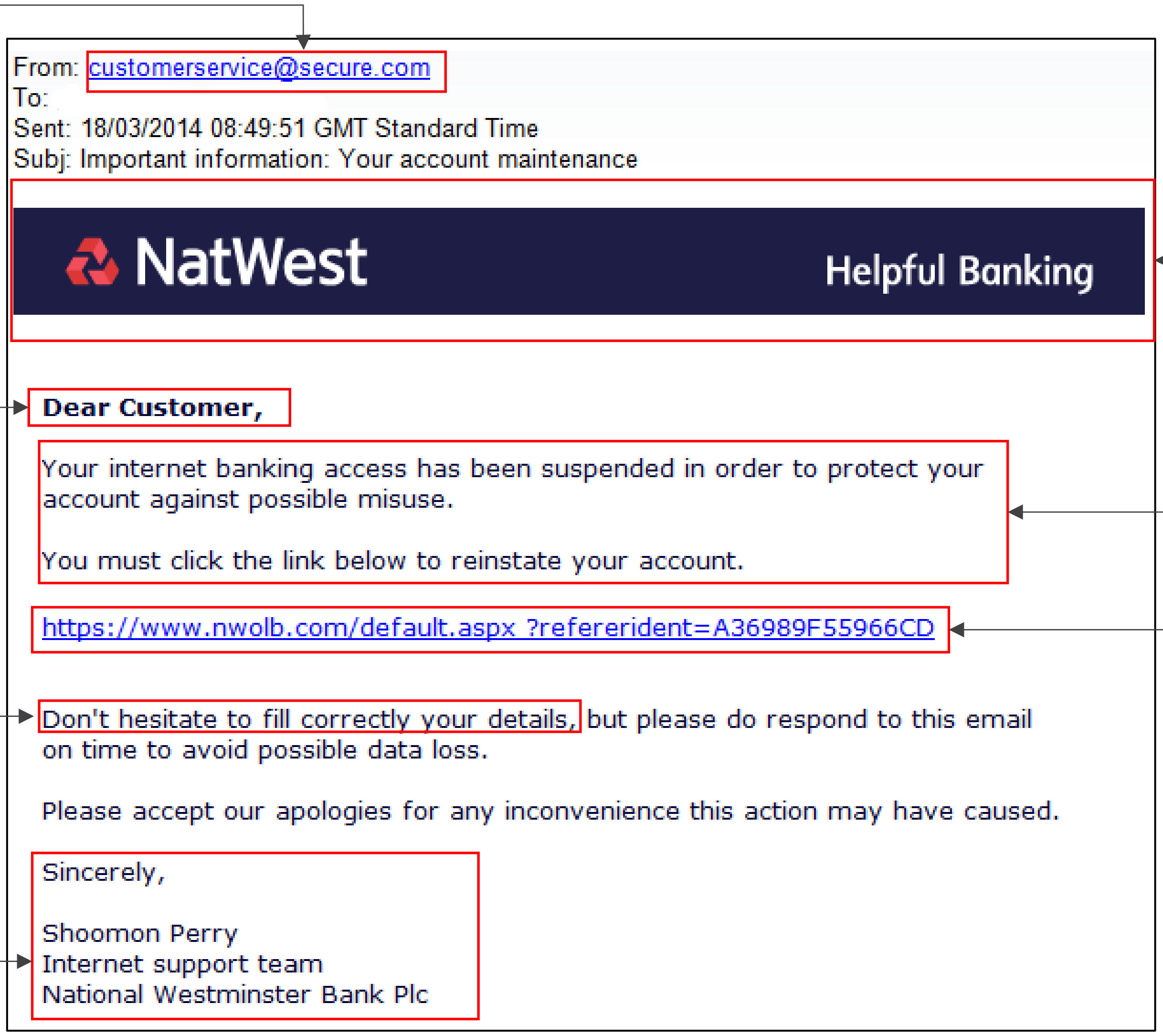
Spammers will often try to make the email look official by signing off the email using symbols, disclaimers, business addresses etc. Luckily most are very obvious like this email (no real business will be so vague and use {C}) but even if they look genuine, remember it is easy to copy and paste these parts.

**Email: Support@wedoyour.it**
**Tel: +44 (0) 117 9118 808**

# Top Tips for Spotting Spam

*Not all emails are as obvious as the first example, but they will share some common traits. Here is a fake NatWest email. These types of emails that spoof a genuine email are known as phishing emails.*

**Here is a helpful example:**



From: customerservice@secure.com
To:
Sent: 18/03/2014 08:49:51 GMT Standard Time
Subj: Important information: Your account maintenance

**Dear Customer,**

Your internet banking access has been suspended in order to protect your account against possible misuse.

You must click the link below to reinstate your account.

https://www.nwolb.com/default.aspx ?refererident=A36989F55966CD

Don't hesitate to fill correctly your details, but please do respond to this email on time to avoid possible data loss.

Please accept our apologies for any inconvenience this action may have caused.

Sincerely,

Shoomon Perry
Internet support team
National Westminster Bank Plc

The email is not from the Natwest.co.uk domain we would expect even though it starts with the genuine looking customerservice@.

The layout of the email is almost identical to any Natwest email. Keep in mind that it is easy for anyone to copy and paste the content of an email so even if it has the correct logo and layout, it doesn't automatically make it genuine.

The email is not addressed to you personally. NatWest would have your name…the spammer obviously doesn't.

There is a call to action trying to make you panic and click on the link. Take your time to check the email for clues to confirm if it is genuine or not.

The important part of the domain (before the .com ending) is not what we would expect for NatWest. Typically, we would expect to see natwest.co.uk. Even though NWOLB.com could stand for **N**at**W**est **O**n**L**ine **B**anking, it is not the common publicly known address for NatWest and so should be treated with suspicion.

The language used is not correct. Spelling or grammar mistakes are clear signs that the email is spam

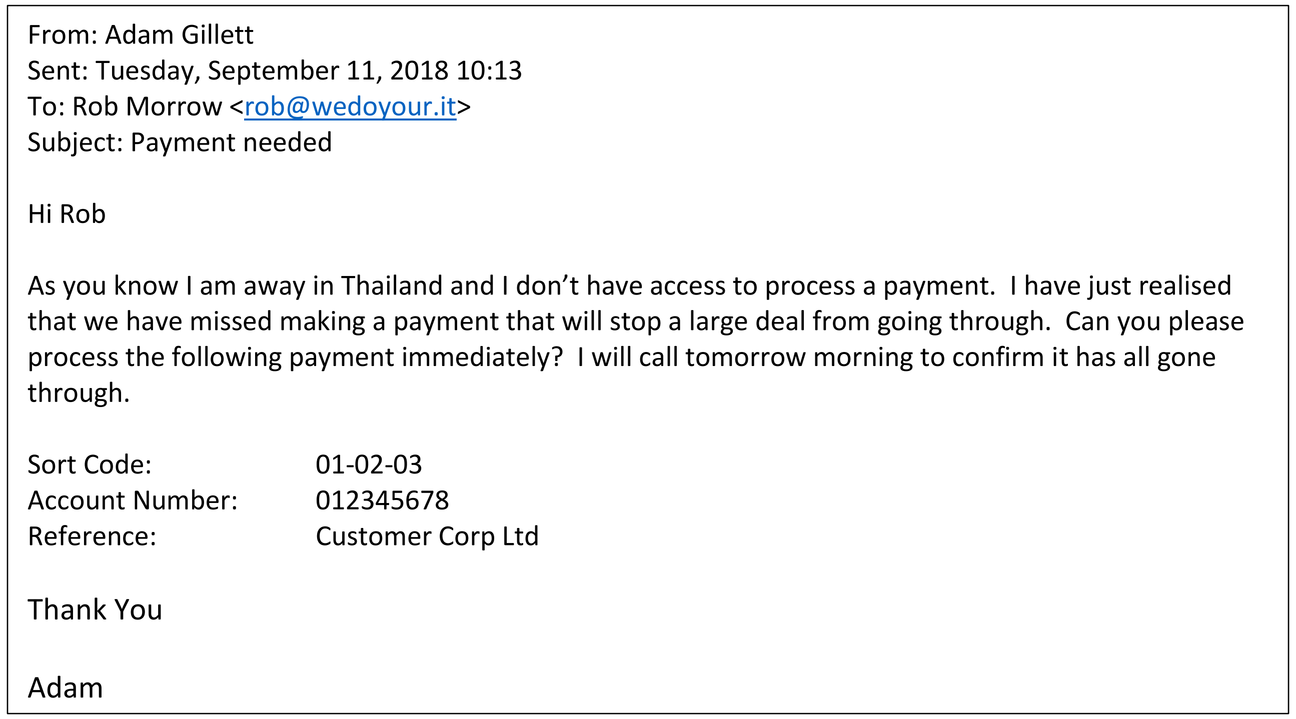
Remember that anyone can sign off an email as anyone they want. Do not be fooled by official looking email signatures or sign offs.

# Top Tips for Spotting Spam

## CEO Spam

*Spammers are now using even more personal tactics.  They will use Linked In to see who works in the accounts department and who the top bosses are (the CEO for larger companies hence the name for this type of spam).  They may then use Facebook to work out when and where these bosses are on holiday.  They will use blogs and hijacked emails to learn how the bosses sign off their emails.*

**Gathering all this information you may receive an email similar to the below:**



From: Adam Gillett
Sent: Tuesday, September 11, 2018 10:13
To: Rob Morrow <rob@wedoyour.it>
Subject: Payment needed

Hi Rob

As you know I am away in Thailand and I don't have access to process a payment.  I have just realised that we have missed making a payment that will stop a large deal from going through.  Can you please process the following payment immediately?  I will call tomorrow morning to confirm it has all gone through.

Sort Code: 01-02-03
Account Number: 012345678
Reference: Customer Corp Ltd

Thank You

Adam

This email looks genuine, has the correct information in the from header, addresses you specifically and uses information about the persons holiday that you wouldn't expect anyone to know.  To be able to spot these types of emails comes down to the fact if it seems odd or out of character then its most likely is fake.  If you were to click on reply, it will also change the reply address to a non genuine one.  This is a instant clue the email is fake but does require users to click on reply to check so not always the easiest. Therefore we advise it is best to have a strong process in place for making payments.  This may include that new payees are only added when they are confirmed verbally.  Communication by email to confirm a payee could be compromised so shouldn't be used as a way of checkin.  We advise training for any member of staff that has access to make payments to help spot these scams too.

## What to do if you fall victim to a spam email?

It is likely that at some point you won't spot an email scam until it is too late.  We have all done it, especially if when we are frantically busy and overlook some of the obvious signs.  In these moments, it is important to understand that even if you have let a virus in, it is unlikely that you will see any symptoms.  So it is natural for many to think they haven't done any harm and so no need to report it.

Truth is, the scammers know that time is of the essence so purposely make their actions hidden.  So even if it looks like your actions haven't resulted in any issues, the damage will be happening incredibly fast behind the scenes.  That is why it is imperative that you contact We Do Your IT as soon as you realise you may have accidentally clicked or open something you shouldn't have.  The sooner we know the sooner we can stop the damage from occurring.

A common threat today is ransomware.  This type of virus puts a special password on all your files and holds you ransom for that password.  These viruses can password protect an entire server within 30 minutes or less. So a quick response is vital to being able to limit their damage.

We Do Your IT are keen advocates for ensuring that staff do not get in to trouble when reporting any mistakes opening or clicking on nasty links. We will always support the end user if they report a mistake as soon as possible.  It is easily done and is likely to happen to all of us at least once.  After all, we need to remember we are all on the same side…trying to combat these bad guys together!

If it is still difficult to identify whether an email is genuine or not, please do get in touch with one of our help desk team.  We are always happy to help confirm if an email is safe or not.  Its always quicker and easier to check the email first than try and deal with the fallout from one you get wrong.

Please do pass this on to anyone you think it could benefit.  The more people it helps avoid falling victim to malicious emails, the better!

Thank you!

We Do Your IT Limited