

Email: Recognise Threats and Scams

Spot Fake Email Messages and Avoid Being Tricked by Email Scammers

This article shows you how to:

- Spot fake emails immediately using practical examples
- Systematically check whether a message could be legitimate
- Avoid falling into the traps set by online criminals

The Internet's criminals use all sorts of tricks to get their hands on your private information – and ultimately your money – but their favourite method is email. An email message lands right in front of your nose, and the criminal simply has to hope you'll believe what the message tells you.

In this article, I'll show you how to spot the telltale signs of scam email messages using real-world examples, and delete them right away without the risk of falling into their traps.



Contents:

What Criminals Hope to Accomplish with Scam Emails.....	E 509/2
Step 1: Quickly Recognise Fake Senders and Multiple Recipients	E 509/6
Step 2: Spot the Common Tricks in the Subject Line	E 509/9
Step 3: The Telltale Signs in a Message's Text.....	E 509/10
Step 4: Identify Malicious Links and Attachments.....	E 509/13

What Criminals Hope to Accomplish with Scam Emails

The Internet is a gift to criminals...

Crooks and swindlers have been around for as long as there has been someone to swindle. But widespread use of the Internet has made their job an awful lot easier and far more profitable: rather than having to target one potential victim at a time, they can target hundreds of thousands of people every day. Better still, they can do so with minimal risk, since the Internet gives them almost complete anonymity.

... and email is a well-used method

One of their favourite methods is to use email. However, over recent years, their tactics have changed. Previously, scammers worked alone or in small groups – they were effectively ‘amateurs’ – and a lot of the email messages they sent were easy to spot as fraudulent.

Email scams are operated by criminal gangs

These days, email-based scams have become big business, operated by much larger criminal networks with a more professional approach. As a result, the messages they send often look much more authentic.

The risks of email scams

This means there’s an increased risk that you might take an email message at face value and fall into one of the classic traps:

- Clicking a link which looks innocent, helpful or important, but which actually leads to a website which tries to install malware on your PC.
- Clicking a link which appears to take you to a website at which you have an account, but which is designed to fool you into disclosing your username and password to the scammers.
- Opening a file attached to an email message which instantly tries to install a malicious program aimed at spying on you or extorting payment from you.

- Responding to the message (usually by emailing a reply) in such a way that you can be lured into handing over your money willingly in expectation of receiving something in return.

Those are the most typical traps laid by the scammers, but they're played out using a wide variety of tricks and stories. Let's look at a few practical examples of the scams you'll encounter to get a quick flavour of what goes on:

Common tricks and scenarios

- **The Phishing scam.** Pronounced 'fishing', this is an email message which purports to have come from a bank, PayPal, Amazon, Apple, Microsoft, or any other large company with whom you might have an account (and which usually has some sort of financial connection). The message says there's some sort of problem with your account and you need to 'click here' to confirm your details.

'Click here to verify your account'

What happens next? If you click the link, you'll arrive at a web page which looks just like that of your bank (or PayPal, or Amazon...) and which prompts you to sign in. It isn't – it's a fake page set up by the scammer to harvest the username and password you type into it, thereby giving the scammer full access to your bank account.

- **The Fake Purchase scam.** There are various scenarios, but the most common is to receive a payment confirmation from a well-known store which claims you've just purchased something. The message gives no details about what you bought or how much it cost, but encourages you to click links to visit the store, log into your account and find out. In a second scenario, you receive an anonymous-looking message which says little more than 'The receipt for your purchase is attached', clearly expecting you to open the attached file out of curiosity or concern.

'Click here to find out what you've just bought'

'Contact us to receive a large sum of money'

What happens next? The first scenario is a slightly more artful version of the classic phishing scam explained above, designed to steal your account and payment details for the online store. In the second scenario, the attachment tries to install malicious software on your PC as soon as you open it.

- **The Windfall scam.** There are many types of this scam, all designed to convince you that you're about to receive something for nothing. For example: you've won a fortune in a lottery you didn't enter; a foreign bank official will pay you to help him embezzle funds from an account he manages; a solicitor has a huge inheritance for you from a deceased distant relative; a courier company is trying to ship a large parcel of cash to you.

What happens next? In each case, you're requested to reply, giving brief contact details, to start the process of getting all this money to you. Before long, you'll discover there are costs involved, and you'll be asked to pay ever-larger sums to the scammer until you realise you've been had.



A sly variation on the Windfall scam is the Lonely Heart scam – a message from someone who wants to befriend you. Assuming you reply, and a few messages are exchanged to cement the relationship, you'll learn that the 'lonely heart' needs help with financial difficulties, or would love to meet you but can't afford the plane fare, or has an illness for which the cure is very expensive.

Incidentally, a common point about Windfall scams is that they often ask you to keep your good fortune secret and not to share this wonderful news with your family and friends. They can't offer any good reason why you should do this, but there is one: the scammer doesn't want anyone telling you it's a scam!

- **The Legal Trouble scam.** This is a new and suddenly-popular scenario – a threat of legal problems. It may be a message stating that you’ve been summoned to a court appearance, or a message from a debt-collection company claiming you owe a large sum of money. In either case, the attachment supposedly contains the details.

‘Contact us or you’ll be in trouble’

What happens next? Here again, the attachment would try to install malicious software on your computer if you were to try to open it.

- **The Tax Rebate scam.** An email message from HM Revenue & Customs (HMRC) which says you’re entitled to claim a tax rebate of several hundred pounds. All you have to do is complete the attached form and email it back.

‘Fill in this form for a tax rebate’

What happens next? In the examples I’ve seen, the attachment really is a form. However, it’s a form that insists you provide the kind of personal and financial details you probably wouldn’t share with your best friend, right down to the PIN numbers and available balances on your credit cards. If you were to send back this form, money would soon be leaving your account, not entering it!

That’s just a taste of the most common email scams currently doing the rounds, but it by no means covers them all. In addition, scammers are inventive and sneaky (it’s part of their job description), and they’re dreaming up new scams all the time.

New scams appear all the time

Unless you immediately recognise a message you’ve received as being one of the common scams outlined above, there’s only one way to avoid falling for the criminals’ tricks. That’s to examine the message carefully yourself and work out whether or not it’s authentic. Over the following pages, I’ll show you what to look for in the various elements of an email message.

You have to learn what to look for

Step 1: Quickly Recognise Fake Senders and Multiple Recipients

Two important points about email

We'll start by looking at two similar elements of an email message: who sent it, and who it was addressed to. Just before we do, there are two vital points to be aware of about email-based scams (and indeed all other types of junk email):

Sender's details are easily faked

- **Point 1:** a drawback to email is that it has no verification system – you can't tell who really sent the message you've received. Scammers use this shortcoming to make their messages appear to have been sent by anyone they choose.

One message, many recipients

- **Point 2:** scammers use automated software to send out messages in huge quantities. Rather than setting their software to send out 5000 individual messages (for example), they speed up the process by addressing a single message to 50 people. This way, their software can reach 5000 people by sending only 100 messages, vastly speeding-up the operation. We'll return to this point a little later.

Check the sender's name and email address

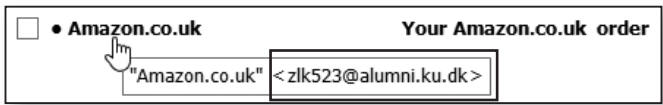
Don't trust the name or address!

As you'll realise from Point 1 above, you can't trust the name or email address displayed in the 'From:' column of your email program: the scammer can make the message appear to be sent by anyone he chooses.

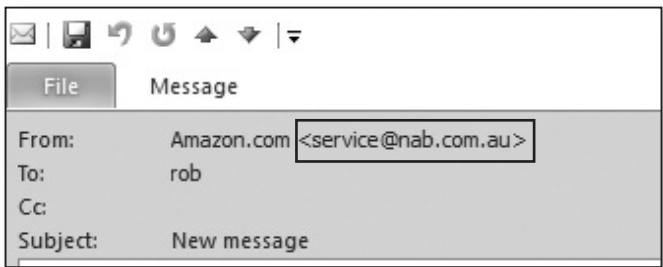
That leads to the most important rule to remember when you look at the sender of any email message: just because it appears to have been sent by your bank, or Amazon, or HMRC, that doesn't mean it was. Never take the sender's name or email address at face value!

Check the email address

In some email programs and webmail services, holding the mouse over the sender's name displays the sender's email address:



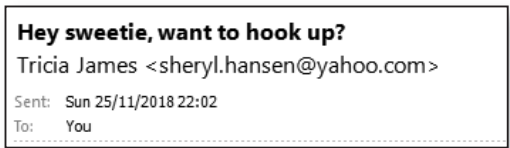
In others, you can click (or double-click) the message to display it either in the preview pane or in a separate window, where you'll see the sender's email address above the text of the message:



The two examples above were apparently sent by Amazon, so you'd expect the sender's address to end with **@amazon.co.uk** or **@amazon.com**. They don't: the first is a Danish email address (it ends **.dk**) and the second is Australian (**.au**). Quite why the scammers didn't specify a real Amazon email address is a mystery, but it doesn't matter: it tells us at a glance that the message couldn't possibly be from Amazon.

Is it what you'd expect?

Here's another example: apparently you've received an unexpected approach from someone named **Tricia James**. Or have you?



Why has Tricia James created an email address in the name **sheryl.hansen**? Don't put it down to confusion or forgetfulness on her part; it's because the scammers'

Scammers often skip on the details

software is pairing random female names with random email addresses the scammers have set up.



As the examples above illustrate, scammers may be inventive and sneaky, but they often don't pay attention to detail. That's a point that works in your favour, as long as you remember to look at those details yourself!

A large company using a free email account?

Another thing to look for is the use of free email accounts. The most popular are Gmail (with addresses ending **@gmail.com**), Yahoo (**@yahoo.com**) and Microsoft's Live .com (**@live.com**). Ask yourself why a bank official, a solicitor, a courier company or a lottery administrator would write to you from one of these free email accounts. These types of businesses and organisations would have their own domain name – it's an important part of any company's branding and credibility – and since the sender claims to be writing to you on company business, you'd expect him to be using the company's email account to do it.

Was the message sent to you – and only you?

Who is the message addressed to?

After looking at who sent the message, look at whom it was sent to. Picking up on Point 2 on page 6, do you see your own name and/or email address beside the 'To' at the top of the message?

Was it sent to multiple recipients?

If you see the words **undisclosed recipients**, or **recipients**, or **you**, or **Customer**, or something similarly general, you can be fairly sure the same message has been sent to others besides yourself. Likewise, you may see that the email address is similar to yours (it starts with the same few letters), which is another indication that the message was sent to other people at the same time.

In many of the scenarios used by scammers, you'd expect to receive a personal message, sent only to you. For example, if you've won a lottery, been informed of an

inheritance, received a payment confirmation, or been told your online account has been suspended, why would the company send identical messages to a bunch of other people too?

Do you even have an account with this company?

This is quick and easy. If the message appears to have come from a company you've never dealt with, you know straight away it must be a scam. You can't have been billed by Amazon or PayPal if you don't have an account with them; you can't have had your Barclays account blocked if you bank with HSBC.

No account? An obvious scam!

On a similar topic, consider whether this purported sender would contact you by email, and whether they would even have your email address. For example:

Are they likely to have (or use) your email address?











- Courts, debt-collection agencies and HMRC would contact you by post, not by email.
- If a courier company were trying to deliver something to you, they would know your postal address, but why would anyone have given them your email address when handing over the parcel?
- If a solicitor were trying to contact you about an inheritance from a distant relative, is it really credible that the solicitor is able to email you, but not to telephone you or send you a letter?

Step 2: Spot the Common Tricks in the Subject Line

If a look at the 'From' and 'To' details of a message hasn't already tipped you off that it's a scam, have a look at the message's subject line. Many phishing scams, in particular, can be spotted easily. Any suggestion in the subject line that you're being asked to 'update' or 'verify' or 'confirm' your account details, or that

Telltale signs of a phishing scam

your account or subscription has been 'blocked' or 'limited', should tell you immediately that there's something fishy going on:

!  	From	Subject
	Amazon.co.uk	Amazon.co.uk : Online Account Update
	Apple	Verify your Apple ID.
	Amazon.co.uk	Amazon.co.uk : Update Your Online Account
	Netflix	Important information regarding your Netflix subscription
	PayPal	Reminder: Update your details for PayPal
	Barclaycard	Card usage interrupted
	Apple Support	Please update your Apple account now
	Amazon.co.uk	Account Confirmation

Look out for these tricks too Beyond this, there are several other common tricks used in the subject line by scammers:

- **A sense of urgency:** watch out for words and phrases like 'Urgent', 'Important', 'Alert', 'Must Read'.
- **Good fortune:** telltale words and phrases include 'Congratulations!', 'You won!', 'Overpaid tax return', 'A financial support donation to you', 'Jackpot winner, Good News!'
- **Reference numbers:** scammers like to quote fictitious 'reference numbers' in the subject line to make the message look official and important. Whenever you see 'Order info: 31116928466' or 'Reminder: 299196245', it's a safe bet you're looking at a scam.

Step 3: The Telltale Signs in a Message's Text

Check the body of the message I mentioned earlier that most scammers often don't give enough attention to the details. If you haven't noticed anything suspicious in the other details, a scammer will often give the game away in the body of the message.

Don't be fooled by logos and other artwork in the message! It's very simple for a scammer to copy the logo from Amazon, PayPal, HMRC, Barclays or anyone else (it takes literally a few seconds) and include it in the message to add an air of credibility. Likewise, scammers like to include 'small print' and disclaimers at the bottom of the message to give a similar effect. Never believe that these are signs of authenticity.



Here are the most important things to look for in any email message.

Does it address you by name?

This is always the first thing to check. If the message starts with **Dear customer**, **Dear valued client**, **Good morning** or simply **Hello**, the sender clearly has no idea what your name is. In addition, of course, this vagueness allows the scammer's software to send identical messages to thousands of people. If they began with 'Dear James' or 'Hello Shirley', they'd immediately lose a large proportion of their prospective victims.

If you deal with them, they know your name!

Don't be swayed by a message that greets you by email address. If it starts **Dear rob.young@example.com**, that's no indication they know who you are. Neither does simply copying the beginning of the email address in the hope that it contains a name, as some scammers' software does, leading to **Dear rob.young** or **Dear rob** (but also, depending on your email address, possibly leading to **Dear zen14786** or **Dear jsmith41** or **Dear sales**).

Does it contain your account number?

At your bank, you have an account number; with HMRC you have a tax reference number; at online stores and at payment services like PayPal, you probably have a customer number. In addition to referring to you by name, you'd expect this number to be quoted too. If it

Do they quote an account number you recognise?

isn't, there's only one possible conclusion: the sender of the message doesn't know what it is!



Remember, though, that scammers have a fondness for including official-looking reference numbers in their messages. We can all drum up random numbers, so don't be impressed unless you know the number being quoted really is your own!

Look for typing mistakes and bad grammar

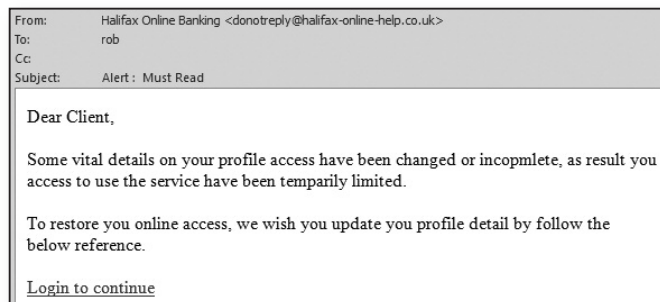
Most scammers are not English speakers

Most scammers have barely a nodding acquaintance with English, so they piece their messages together from a combination of copying, guesswork, dictionaries and online translation tools. This can result in some very peculiar spelling, grammar and sentence structures.

Poor spelling and grammar is a giveaway

You might be inclined to think that the odd mistake is acceptable in an email message, but always keep in mind the supposed sender of the message. It's usually a well-known company (a bank, an online store, a large multinational, a courier company), or someone else you'd assume could cope with basic spelling and grammar (a solicitor, a court, a tax inspector). These senders would take care to look professional at all times.

The example below, supposedly from Halifax Online Banking, does some very cruel things to the English language, but it's far from unique in that:



Fear or greed, and a sense of urgency?

These are the common hallmarks of a scam: it tries to frighten you into believing something bad is about to happen, or to convince you that something wonderful could happen, combined with a clear sense that you must take a certain action quickly. That action is to click a link, open an attachment, or send some sort of reply.

Three hallmarks of a scam message

Step 4: Identify Malicious Links and Attachments

Major companies and organisations are well aware of the email scams perpetrated in their name. As a result, many of them do all they can to make it clear that the messages they send you are genuine. It doesn't need much: they address you by name, and they include your account number, your postal address, or some other detail that demonstrates that they really do know you.

Genuine messages often provide reassurance

They also do one other important thing. They don't insist that you click a link or open an attachment. Yes, they may include links or (much less frequently) attachments, but they know we may be wary of them. Therefore, they'll often say something like: 'You can click the link below, or use your usual method to visit our website and log into your account'.

No insistence that you click a link

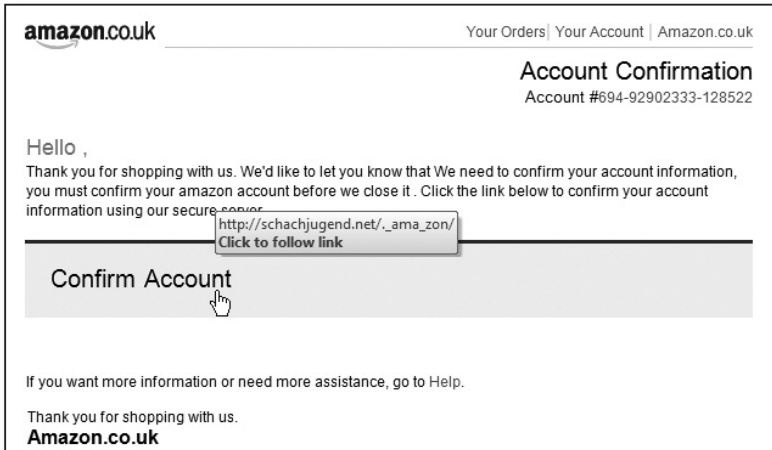
You won't see that in a scam. No ifs or buts, the scammer wants you to click that link!

Scammers offer no other option

The reason is simple: the link doesn't lead to the web page you think it does! It leads to a web page created by the scammer, either to fool you into giving away your login details or to foist malicious software on you.

Before you ever consider clicking a link, simply hold your mouse pointer over it. You'll see the address it leads to in a tooltip or in a bar at the bottom of the window.

Find out where the link really leads



Would it take you where you expect?

The message above looks reasonably believable apart from a few details (no capital 'A' in 'your amazon account', for example – would Amazon be likely to do that?). However, you can see that the link doesn't lead to **amazon.co.uk** but to a website with the address **schachjugend.net**. That's clearly not Amazon's website, so there's no knowing what would happen if you went there!

Avoid two common tricks with links

Trick 1: a cunningly-named folder

In the example below, you can see where the link leads in the message I showed earlier from the Halifax. You might notice that it contains **halifax-online.co.uk** – does that mean it leads where you'd expect?



No, it leads to a website at **floresscorpio.com**. The website address is always at the beginning of the link, straight after 'http://'. After that vital part of the address (the 'domain name') comes a slash, and everything after that slash is irrelevant: it's just the names of folders and files on that website. The scammer has created a folder named **halifax-online.co.uk** on his website in the hope you'll be fooled when you see it in the link.

Only look at the domain name!

Here's a second trick. The blue text of the link can say anything the scammers choose. Often they'll choose a so-called 'call to action' such as Click Here, Login To Continue, or Proceed To Account Verification. Sometimes, though, the blue text shows the address of the website you'd be expecting to visit.

Trick 2: the blue link shows a genuine address...

In the example below, which was purportedly sent by HM Revenue & Customs, the link says **https://www.hmrc.gov.uk**. That is indeed the address of the HMRC website, but it's not where this link actually leads. As you can see, holding the mouse over the link reveals that it really leads to a website at **doesseals.com**.

... but that's not where the link really leads!



The best advice for links in email messages is to ignore them, however. If the message really does purport to have come from a company you deal with, you obviously know a reliable way to reach its website – either typing its address into your web browser or choosing it from your browser's Favourites/Bookmarks. Use that method and you're guaranteed to end up in the right place!

The best option: ignore the link!

Dealing with email attachments

Are you sure the attachment is safe to open?

The only time you should ever consider opening an attachment is if you're entirely convinced the sender is genuine and the message has passed all the tests above. In particular, ask yourself several questions first:

- Have you dealt with the company or organisation which sent the message? If not, it's probably a scam.
- Are you tempted to open the attachment because there's a suggestion something bad could be happening, and this file supposedly contains the details? If so, it's probably a scam.
- Is the message itself very short on information and the attachment has aroused your curiosity? If so, it's probably a scam.

It's vital to remember too that certain types of files can be more dangerous than you think they are. For instance, you might assume that a Word document or a PDF attached to an email message could only contain text, so it must be safe to open and read, but that's not the case at all.

Likewise, be very suspicious of a zip file (whose name ends with the extension .zip), for which you'd have to open the zip file to find the file(s) stored inside it. If the email message says you've been sent a single document such as a receipt or invoice, as it almost certainly does, why wouldn't they simply attach that document rather than going to the trouble of putting it inside a zip file? Quite simply, because they're trying to disguise it!