Emma receives emails every day, but today she also received what's known as a phishing email - a malicious email sent by scammers. Let's look at what would have happened if she'd done what the criminals had wanted her to do.

Had she clicked on the link to the help desk, she would have been taken to a fake website and been asked to update her personal information. The website was set up by criminals to gather personal details which they would then use to hack into Emma's accounts and commit fraud.

If she'd clicked on the other link, or opened the attachment, malicious software, known as malware would have tried to install itself on Emma's computer. It would have then collected details such as her usernames and passwords and sent them back to the criminals.

As Emma's on a network, the malware could have got into the system and stolen, corrupted, or deleted other stored data.

Fortunately, Emma recognised this email for what it was, and deleted it immediately. Many aren't so lucky, so this is spotting phishing emails by what you need to know.

It's estimated that 156 million phishing emails are sent every day, and of these 16 million get through the protection software, 8 million are opened, 800,000 links are clicked and 80,000 people fall for scams and give away their personal details.

Knowing how to recognise phishing emails can lessen your chances of getting caught, so let's have a look at some of the signs.

Perhaps the first thing to look at is the email address of the sender. If you can't see the address, try moving your cursor over the name to reveal it.

Criminals use two tricks here: one is to put a real company name before the @ sign to make it look credible.

The other is to use a web address which is similar to the genuine one.

For example, let's say there's a company called Floyd's Skis and they have a website at http://www.floydsskis.com which has email addresses like this one: info@floydsskis.com

Here's how scammers could create web and email addresses that look similar to the genuine one. By

using an 'i' instead of an 'l'
adding or removing a letter
using a zero instead of an 'o'
or
changing a letter like an 's' to a 'z'

These slight changes are only a sample of the tricks that criminals use, so it's worth taking a moment to inspect the underlying links and addresses carefully, to make sure they are the same as the genuine web address.

Be wary of emails with generic greetings such as 'Dear Valued Customer' and ones with poor spelling, punctuation or grammar.

However, you can't always rely on these obvious signs as sometimes scammers go to great lengths to make their phishing emails look as authentic as possible. They'll use the company's real logo and sometimes even the names of people who work there.

Another trick they use is to create a sense of urgency for example, by saying that there's a time limit, or using a threat like you'll be fined if you don't act now.

They might suggest that you'll miss out on something, raise your curiosity, or tap straight into your fears in order to push you into making an instant response.

If you feel you're being pressured in any way, or that something just doesn't seem right, be especially careful.

If there's a link, just as with email addresses, roll your cursor over it to see the underlying address, in other words, where the link would take you to if you clicked it.

On some touch devices you can use a long press to see this – but there’s an obvious danger - press too hard, and you’ll follow the link.

Lastly, look to see whose name is at the end of the message. If it’s from a department or team, do they actually exist?

If it’s from a person, is their name in the email address, and is the email address real?

So far we’ve looked at generic emails which are sent out to large groups of people knowing that it only takes a few to click to make it worthwhile for the scammers.

However, criminals sometimes target individuals. These are called spear fishing attacks, and are on the increase as the criminals know that many more people are fooled by them.

Spear fishing emails use personal information, often obtained from social media pages, to make the emails look more credible.

For example, criminals might make use your name, or tailor the email to reflect things you like, your hobbies, interests, where you live or what’s happening locally, or even make it appear to have come from the organisation you work for.

People are sometimes targeted because of their position within the company or because they have access to sensitive data. But criminals also go for softer targets, people who are perhaps less aware of the risks and are easier to trick, but who then allow the criminals to gain access to their real targets.

It can often feel like we’re bombarded with emails both at home and at work, and many of them have genuine links and attachments.

So look for the signs of phishing emails and think before you follow any links, or open any attachments.