



Recognising Suspicious Emails

I hope you are keeping well.

Some clients have been in touch recently regarding emails they have received which they are unsure about.

The emails have stated their **Email account was closed** or their **Mailbox was full and they needed to follow a link**, or they needed to **Reactivate their Email Password** or their **Domain was expiring** and needed paying online or that another Payment was due.

I thought I would get in touch to let everyone know that these aren't real, you will not be approached for payments online for your Email or Website nor to reset your email password.

You may have received similar emails in your personal life, they tend to come in cycles, you won't have any and then in a short period several come in and then you won't receive any for a long time.

Payment Emails

I will always email you direct regarding hosting and domain renewals and **I will always include an invoice with bank details for payment**, I will not ask you to follow a link.
If I ever change this process in the future I will contact you first to explain before changing over.

Domain Renewals

All Domains are set to auto renew so you won't receive any direct request from anyone else to keep your domain, if you do that is most likely a suspicious email.

Email Passwords

You will not be sent emails telling you your Email Password has expired and you need to follow a link to reactivate it, you can change your Email Password via the Webmail portal (<https://stackmail.com/>) at anytime but they do not expire.
It is always a good idea to have a strong password and it can help to change your password now and then just to be safe.

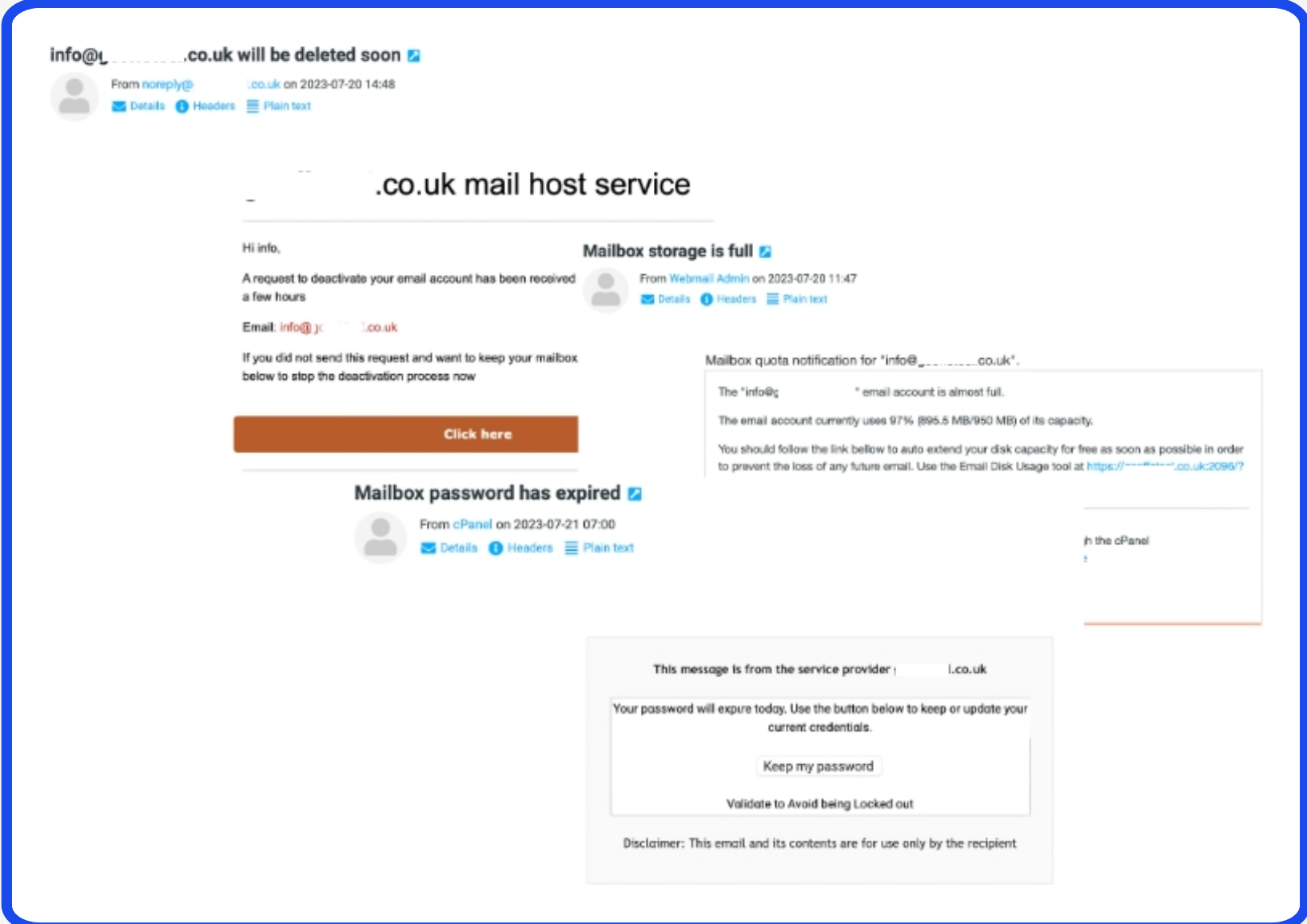
I have a tutorial on my Client Support Page **showing how to Change your Email Password**, the link is included at the end of this email.

Spam Emails

You may also receive some emails offering to get you to **No.1 in the Search Engines** or Cheap reDesign or Social Media work.
These are more spam than malicious usually but they do tend to offer an **UnSubscribe link which isn't real** and following those links or replying to the email usually means you will receive more spam emails so it's best to just delete these emails.

Suspicious Email Examples

Below I have included some examples of the type of malicious emails you may receive trying to get you to follow a link and enter details.



Dealing with Suspicious Emails

My rule of thumb for when I receive these types of email asking me to select a link or pay online is if I am not expecting it or I'm not sure I delete it, if it is real and important the sender will get in touch again.

Unfortunately it is difficult to completely stop these emails as the people involved use ever changing tactics hoping the email looks official enough.

The technical support people who look after the servers that run your website and email do take a proactive approach and once they are aware of suspicious emails they will block the IP address they come from.

Get in Touch

I am always happy to help, so if you receive an email you are not certain about please do Email me and/or forward any suspicious emails and I will check them for you.

Please do feel free to forward this email to anyone you work with who might find it useful.

Real/Official Emails

Below I have included a screenshot of an official "Mailbox alert" Email you will receive if your Email box is nearing its maximum size.
You will see it includes my Name and Logo and it only directs you to go to your email application to see if you can reduce how much space is used, no link asking you to visit a website.



Email Upgrade

If you find you are nearing the default 10GB maximum size of your Mailbox and need to keep all of your emails there is an upgrade option which doubles your mailbox size at a yearly charge of £20.
Please email me if you would like to purchase this upgrade.