SPOTTING SUSPECT EMAILS

A COMPLETE GUIDE TO RECOGNISING LEGITIMATE EMAILS

WWW.SYSTEMAGIC.CO.UK

SYSTEMAGIC
DOING IT DIFFERENTLY

HOW DO SUSPECT EMAILS SLIP THROUGH?

As technology evolves, we're sending and receiving more emails now, than ever before. Which is why we need to be aware of what we do online. More and more bad actors are moving their illegal activity online and attempting to take advantage anyway they can.

One of their main targets are emails. Simply because both home and business users rely so heavily upon them. Today's modern user can have upwards of 5 email addresses, and anything above that can be a handful. Most of the time you need to be able to read and quickly respond to your emails without any trouble, but there may be one or two suspicious emails that can slip through. Then before you know it, you've accidentally given up your password or allowed someone access to your machine.

A great deal of suspicious emails may come from odd addresses like **yye9982@xzxx.com**, which looks really strange and are often filtered, but others could come from Jeff@outlook.com. The second address looks far more believable and it's come from a reputable source. Jeff has unknowingly had his account hacked and the bad actor is now sending out spam from his account.

HOW CAN I AVOID THIS?

In the world of emails, the best filter isn't some fancy new system, it's you!

Hackers and bad actors rely on the human element.

That slight lapse in judgement

Not fully reading an email

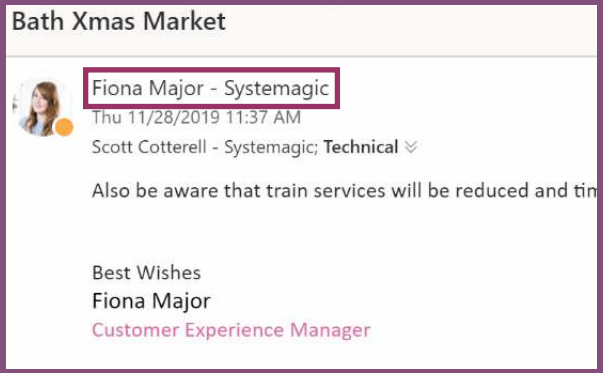
Not checking the sender

These are all things a hacker hopes for when carrying out these types of attacks.

It may seem hopeless, but we have four tips to help you keep on top of things, and to keep yourself and your business safe. Once you start looking for the signs of a suspicious email, you'll be chucking them into the junk in no time!

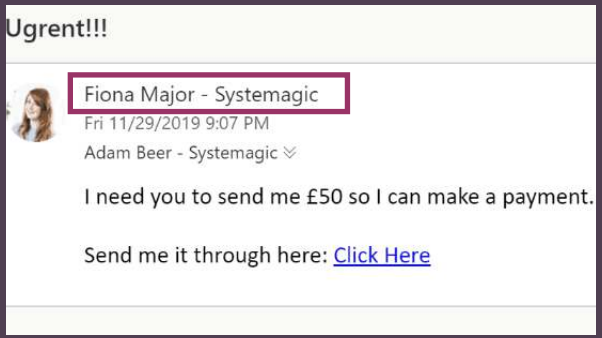
1 DISPLAY NAMES AND ADDRESSES

The biggest thing hackers hope you miss are the email address their attacks are coming from. They rely on their display name to trick you. Any email account on any email provider can change their display name to anything they wish. This is where it can get tricky to distinguish between a legitimate email and a fraudulent one.



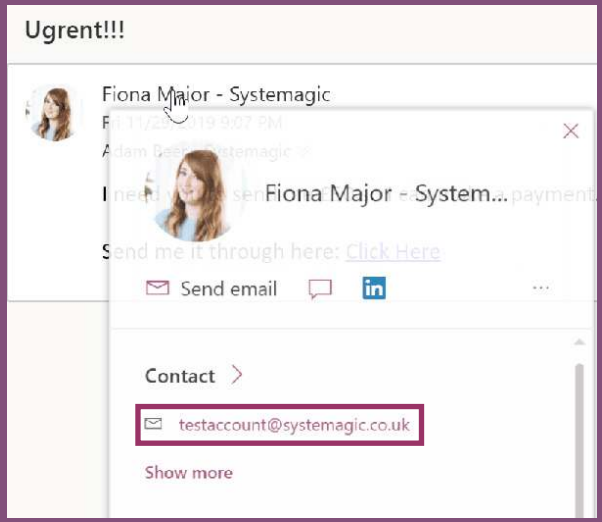
Even if the display name looks familiar, like your boss, a relative, or a company that you've worked with in the past, check the address.

While we can see our email has come from Fiona, we can't see what address it's come from.



To check, we simply click on the name to show the contact details. You can do this on OWA (Outlook Web App) on your browser, within outlook itself, and even on your phone.

Fiona wants me to send money using a suspicious link, but upon closer inspection we can see that it hasn't come from her email address but testaccount@systemagic.co.uk!



2

ASSUME LINKS & ATTACHMENTS ARE BAD

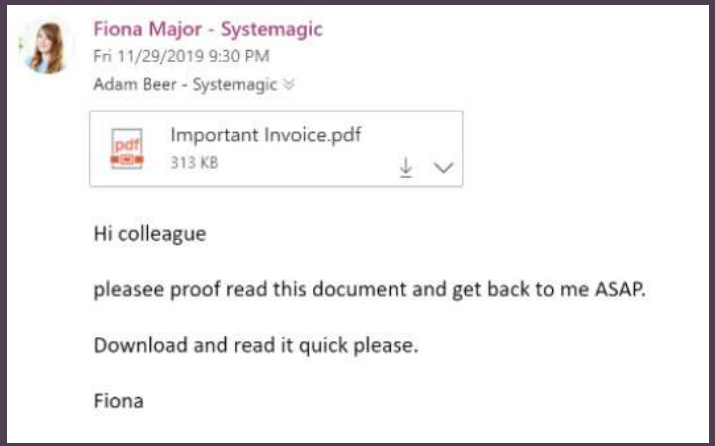
A great rule of thumb is to assume all links are bad, regardless of who they came from. Even if a link has come from a person you recognise, or an email address you recognise, doesn't mean the link is safe.

The best way to check is to hover your mouse pointer over the link. Don't click it!

Hovering over the link will display it's intended destination and if it doesn't look familiar to you, don't click it. If you've been sent a link pointing you to a YouTube video, but hovering over the link is showing Yt22898.asffg.net, it's probably taking you somewhere bad.

Sometimes everything looks legitimate. The display name checks out, the email address checks out, but something doesn't feel right.

I wasn't expecting an invoice from Fiona, and why does she want me to download it so badly?



It's possible that Fiona's account may have been compromised and the hacker may be trying to infect others. If an email just doesn't feel right, always double check. If you're in the same office, have a quick chat, or pick up the phone.

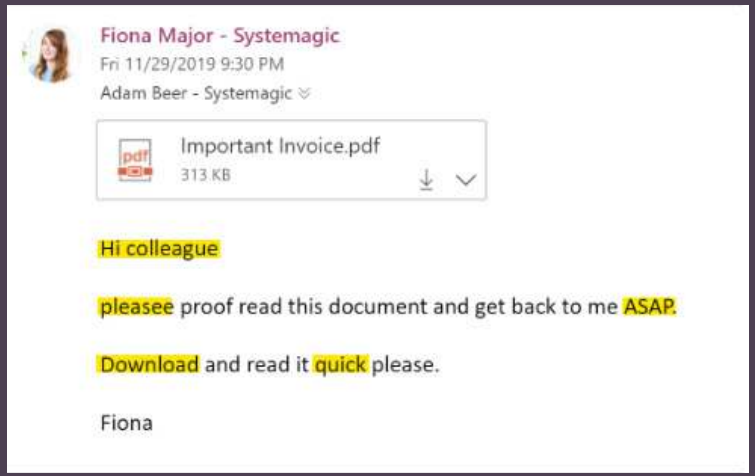
This PDF file may have some malware attached so it can't hurt to check!

3

FORMATTING ODD LANGUAGE

A good portion of attacks are launched by attackers that may speak English as a second language, or the email in question may be structured in a way that doesn't fit the person.

Let's take a closer look at that last email...



Firstly, 'Hi colleague', Fiona never says that to me, that's odd but OK. Let's read on. 'Please' is spelt incorrectly. She wouldn't forget to spell check her email before sending, strange. Hmm, this email is using language like 'ASAP' and telling me to download something. The wording is trying to rush me and ignore the previous mistakes. Lastly, I know how to download an attachment, she doesn't have to remind me.

Lots of red flags here! Enough to make me second guess if this email is legitimate, despite coming from her email address.

Time to walk across the office and ask her if she really sent this email!

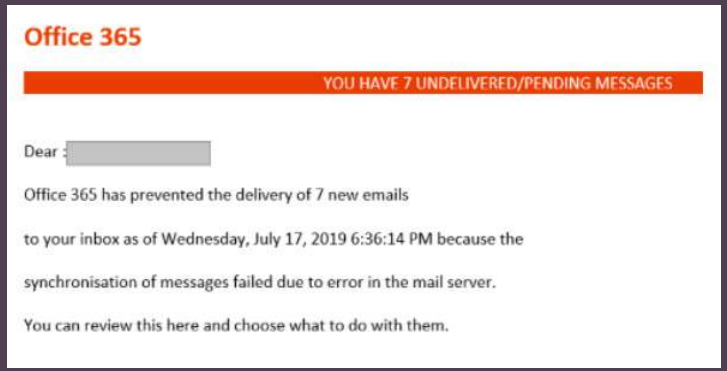
4

FAKE LOGIN SCREENS

This one can be quite sophisticated, but the key thing to remember is you don't have to log in from a link sent to you in an email. You can make your own way to the website in question and log in directly.

One attack hackers like to use is trying to 'force' you to re-authenticate your account. They try to fool you into doing this by sending an email claiming you have unsent messages, and they won't be released until you sign in. Or worse, if you don't sign in quickly, they will be deleted!

No email provider will EVER email you something like this. No emails will ever be held, waiting for a user to sign in and release them.



But what happens if you click the link in this email?

You'll be taken to a fake, but identical looking login screen for Office 365, Fusemail, Gmail, or others. When you try to sign in, this fake website will simply capture your email address and password, then redirect you to the real login screen. When you enter your credentials again, you'll log in to the real version and be left thinking perhaps it was a bug your login didn't work the first time.

IN DOUBT?
GIVE US A SHOUT..

If you're one of our lovely clients, you're ever unsure and just can't quite figure out if an email is legitimate or not, give us a call and we'll be happy to assist.

We have safe environments in place to check emails and even scan and test any links to see if they are suspicious.

We can also add specific emails or even domains to block lists that can stop emails before they even land in a user's mailbox.

Just remember, the best filter is **you.**

SYSTEMAGIC
DOING IT DIFFERENTLY