SYSTEMAGIC
DOING IT DIFFERENTLY

IT Support Connectivity Cloud

HOW TO

SPOT SUSPICIOUS & SPAMMY EMAILS

A SIMPLE GUIDE



Introduction

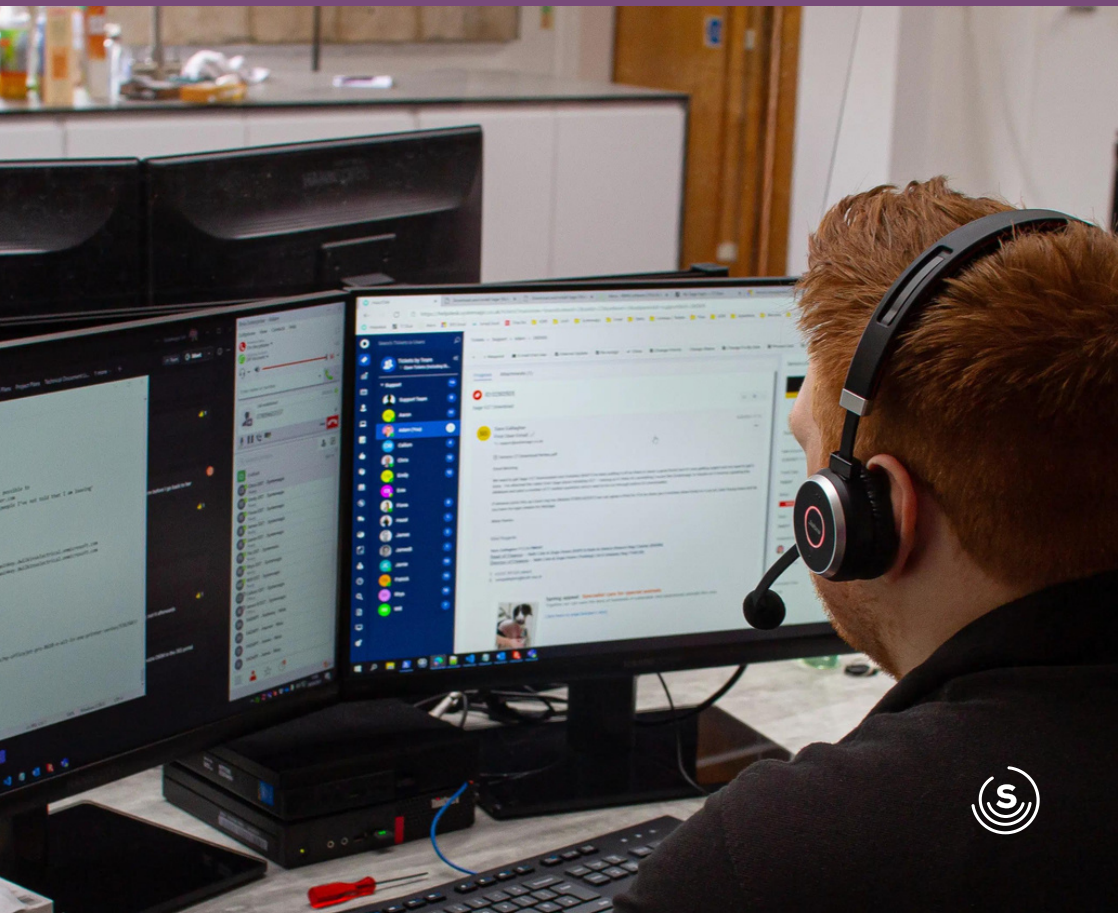
Recent data suggests that nearly **350 billion** emails are sent every day, and that number is only growing.

As busy professionals, reading and responding to emails often feels like a chore, and it's not something we put much thought into. It's something we're all guilty of!

However, cybercriminals are leveraging this to catch us off guard and steal sensitive data.

About This Guide

In this guide, you will learn how to spot a suspicious email, why they sometimes slip through security and what to do if you receive one.



What Do Cybercriminals Want?

You might not think it, but your business and customer data is incredibly valuable to cybercriminals. Especially if you collect, process or store sensitive and confidential information, such as IDs, health records, business documents and bank details.



If cybercriminals get hold of this data, they can commit a variety of crimes, including fraud, identity theft, blackmail and extortion.

Cybercriminals typically use one of two methods to do this, phishing attacks and malware-infected emails.

A phishing attack is when a cybercriminal sends an email to you, posing as a trusted contact, such as a service provider, colleague or your boss. The email will prompt you to click a link to a replica sign-in page (phishing page) of the account they want access to. Typically this will be your bank, Microsoft 365 or Google. Once you 'sign-in', your username and password is sent to the scammer and you will be redirected to the real sign-in page, making it look like a login error. Now the cybercriminal has your details, they can easily log into your account and access your files.

A malware-infected email will contain a virus or malicious code, disguised as an attachment (such as a PDF or Word document). Once you open the attachment, the malware will infect your computer and network and can perform any action a criminal wants, such as infect other computers, explore files, and steal data.

Learn more about phishing

How Do These Emails Slip Through?

Email clients such as Outlook and Google are incredibly sophisticated and can often filter spam emails.

But, what if the scammer used a legitimate email?

As we just mentioned, hackers will try and gain access to someone's Microsoft 365 account, they also have access to their emails and send from them, enabling them to pass through firewalls.

Because of this, it's important that you remain vigilant and know how to spot a suspicious email.

Signs of a Suspicious Email

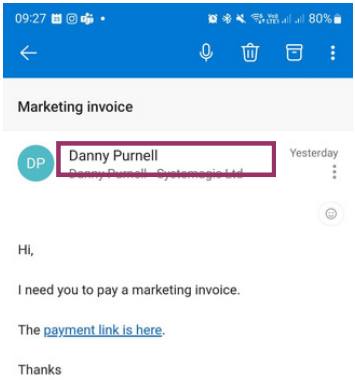
1 Display Name and Email Address

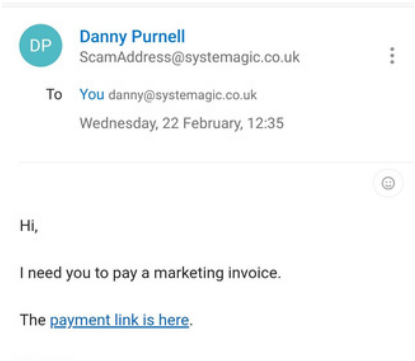
The biggest thing hackers hope you miss is the email address their attacks are coming from. They rely on their display name to trick you.

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 Danny, we can't see what address it's come from.

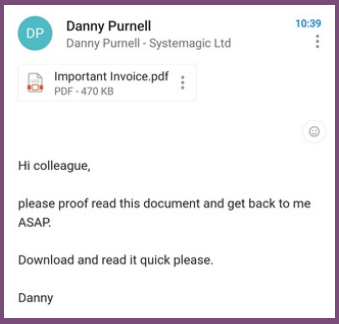




To check, we simply click on the name to show the contact details. You can do this on OWA (Outlook Web App) on your browser, within outlook itself, and even on your phone. Danny wants me to send money using a suspicious link, but upon closer inspection we can see that it hasn't come from his email address but spamaccount@systemagic.co.uk!

2 Assume Links and 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 its 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 Danny, and why does he want me to download it so badly?

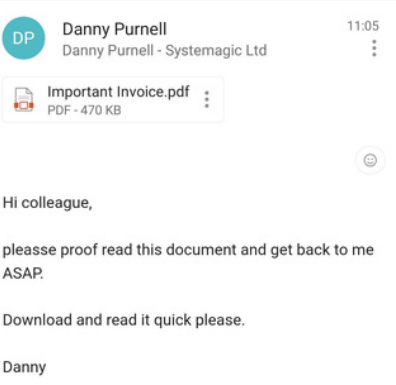
It's possible that Danny's account may have been compromised and the hacker may be trying to infect others. If an email just doesn't feel right, always double check. If you're in the same office, have a quick chat, or pick up the phone.

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

3 Formatting and 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', Danny never says that to me, that's odd but OK. Let's read on.

'Please' is spelt incorrectly. He wouldn't forget to spell check his 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, he 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 his email address.

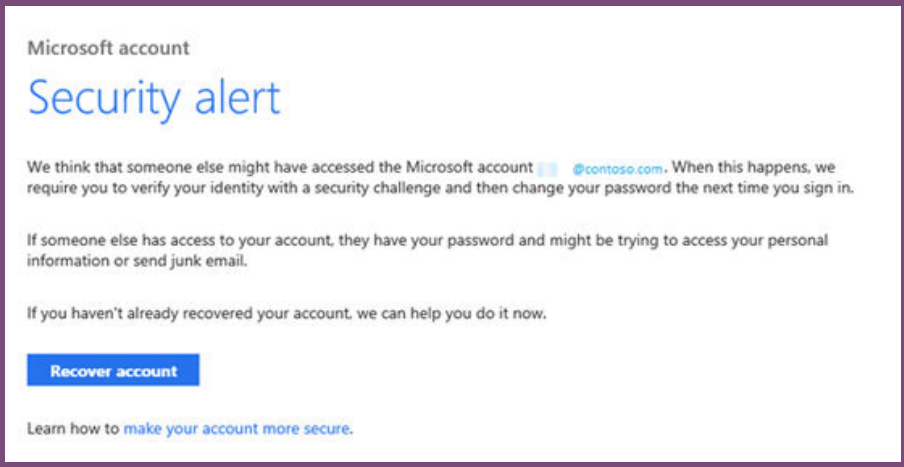
Time to walk across the office and ask him if he really sent this email!

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.


Microsoft account

Security alert

We think that someone else might have accessed the Microsoft account @contoso.com. When this happens, we require you to verify your identity with a security challenge and then change your password the next time you sign in.

If someone else has access to your account, they have your password and might be trying to access your personal information or send junk email.

If you haven't already recovered your account, we can help you do it now.

Recover account

Learn how to make your account more secure.

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, and be left thinking perhaps it was a bug your login didn't work the first time.

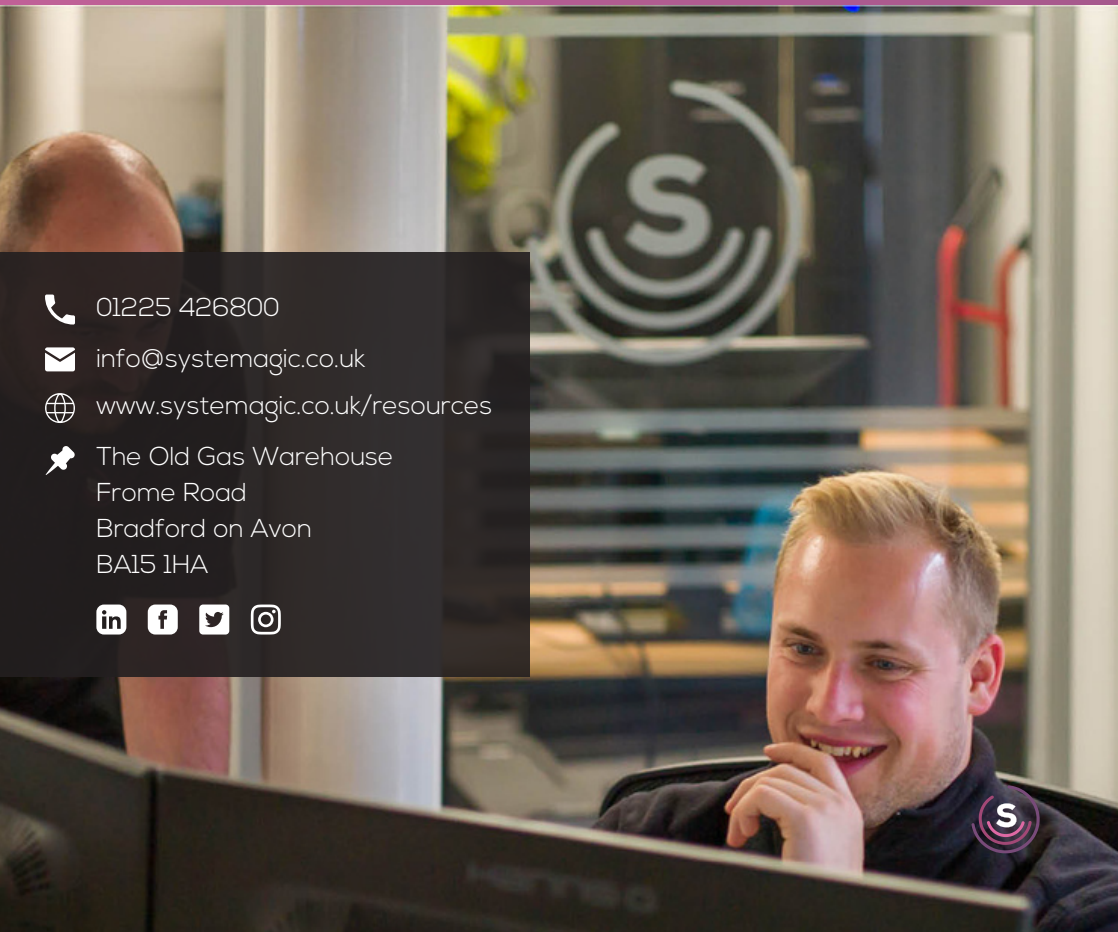
In Doubt? Give Us a Shout!

If you're one of our lovely clients and 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.



01225 426800

info@systemagic.co.uk

www.systemagic.co.uk/resources

The Old Gas Warehouse
Frome Road
Bradford on Avon
BA15 1HA