A spot of phishing...

It's been reported that 28%* of the population were hybrid workers at the end of 2024.

There are so many benefits that working from home offers for both employees and companies: more flexible hours, increased productivity, and just a better work-life balance – especially being able to sit in the sun in the garden at lunchtime! However, in looking at all these benefits, it's also important to understand what potential cyber security issues may arise from working from home.

Also, as a business, we have taken important steps to improve the education of our colleagues regarding phishing and how it affects everyone both at home and in the office.

So... What is phishing?

'Phishing' is when criminals use fake emails, phone calls, texts or websites to trick their victims. Most phishing scams will attempt to trick their victims into thinking they are a legitimate company or website with underhand tactics. Usually, these fake messages will try to make you click a link, visit a website or provide personal information. Opening these links may give your computer a virus or allow the criminal to access your private information.

Phishing can come in many forms, whether they're emails pretending to be from companies that you're a customer of, spoof SMS messages pretending to be your bank, or even false communications from your workplace. With the rise of AI, these types of attacks are becoming more sophisticated than ever, and it's getting harder to discern what's real and what's not.

We want to outline some methods that criminals use in phishing emails, as well as equip you with the knowledge of what to do if a work communication that you've received just doesn't feel right.

3.4 billion phishing emails are sent a day in 2025**

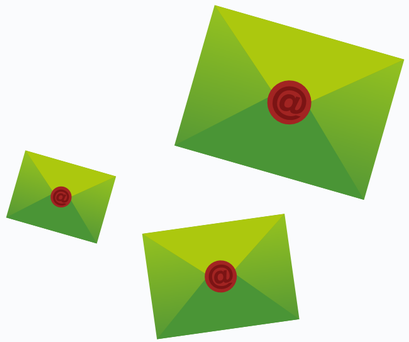
Remote workers are **3 times** as likely to engage in a phishing email***

Understanding your inbox

Your inbox is the main channel that scammers will use to try and trick you into their scam. Below, we've listed some of the common phishing emails that criminals might utilise:

Spam emails

The most common (and annoying) type of unsolicited email that people receive. They are sent to large mailing lists and typically do not have anything to do with the recipient. They might be trying to sell you something or tell you that you've won a prize for example. While advertisement spam mail can seem harmless, any email from an unknown sender that asks you to click a link go to a website may be attempting to steal your personal data. It is always best to mark these kinds of emails as spam and then delete them.



Deceptive emails

These phishing emails have a much smaller mailing list, with the criminal pretending to be someone who is familiar to the recipient in some way, whether that be a company they are subscribed to, their bank or their place of work. A deceptive email might pretend to be from your internet provider informing you about a price increase. They might even use your location to pretend to be from a local council. As these emails are more targeted to a smaller group of people, they have a higher success rate for the criminal than spam phishing.

Spear Phishing emails

These are the most targeted types of phishing emails, and therefore the hardest to spot. They are specifically crafted for a handful of people or sometimes tailored for the individual to try and appear legitimate. Criminals may use things like your social media accounts to craft their attacks further, using names of people you know. Spear phishing emails might pretend to be your manager at work asking for your bank account details for payroll. When criminals target more senior members of a company or those who have IT access, this kind of spear phishing is called 'whaling'.

Here's some useful points to look out for

If a suspicious-looking email has more than one of these red flags, it's probably a phishing email.

Date and time – Was the email sent at a strange time of day, outside of usual working hours? If you weren't expecting the email, think twice before clicking any links.

Sender name and email address – Do you recognise the email handle? Look carefully at the domain name, and make sure it matches the usual sender exactly. Be careful on letter and number substitutions, like 0's for O's, or l's for I's.

Captivating subject line – Does the subject line entice you to read further? If the subject of the email features words like NOW or HACKED, it might be trying to get you to read though the email further and a demand action.

Spelling and grammar – Are there strange wording choices, misspelled words or poor grammar in the email?

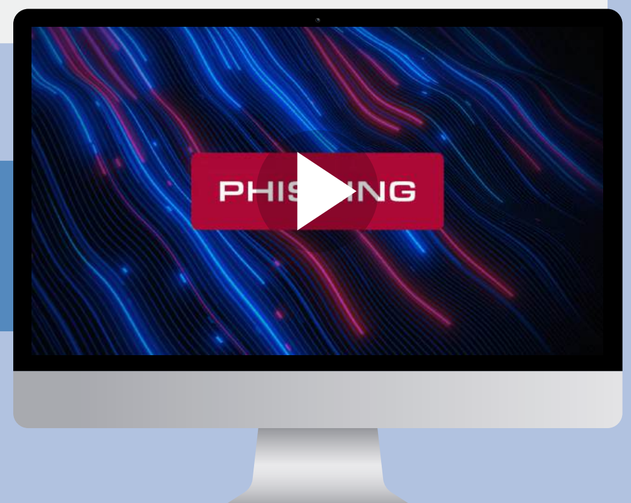
Demanding action – Does the email tell you that you need to do something quickly, or use threatening language? Phishing emails will insist that you download a file, click a link or provide information immediately in order to scam you.

Links and attachments – Is there an incorrect link when you hover the cursor over it, or an unexpected attachment in the email? These links could take you to phishing websites, and the suspicious attachment might download malware onto your device.

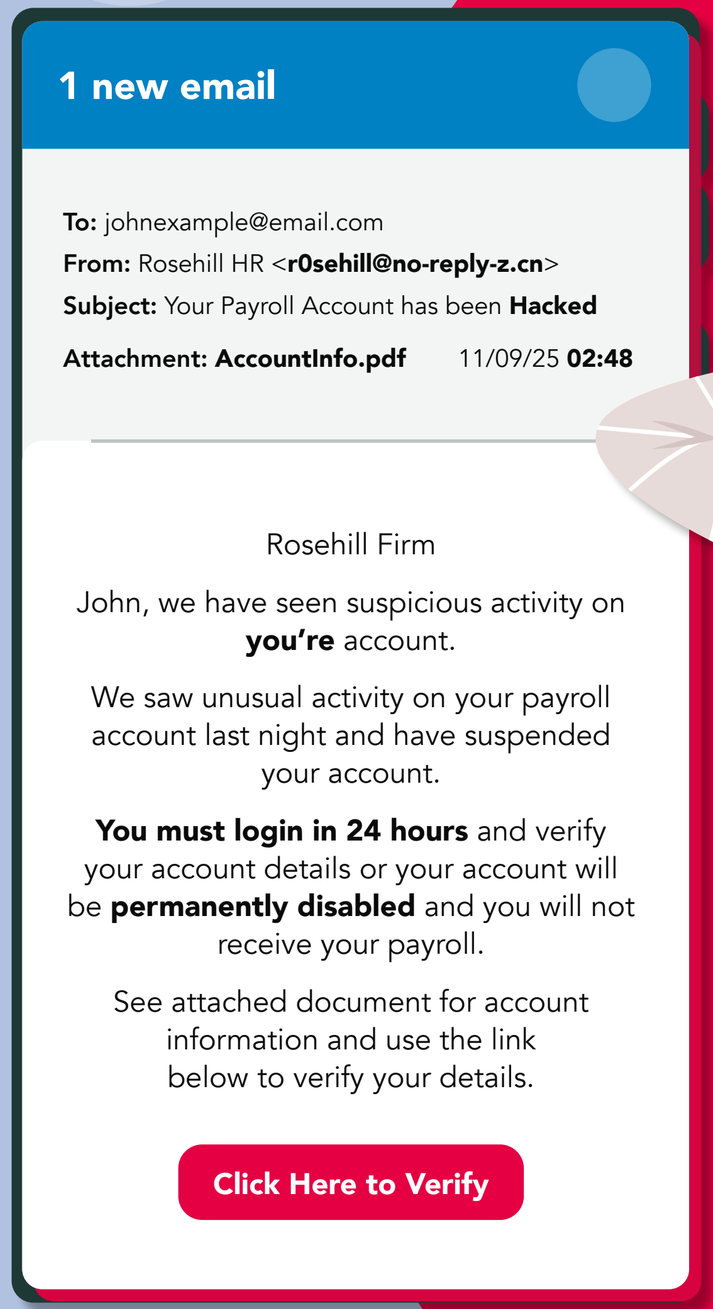
Too good to be true – Does what they're offering sound too good to be true? Unfortunately, it's unlikely someone will truly be selling expensive items for very low costs, or that you really are entitled to a large sum of money for no apparent reason. If it's too good to be true, it probably isn't true.

View a helpful video:

SATT Phishing Module
A guide to phishing



Email red flags in action



1 new email

To: johnexample@email.com
From: Rosehill HR <**r0sehill@no-reply-z.cn**>
Subject: Your Payroll Account has been **Hacked**
Attachment: AccountInfo.pdf 11/09/25 **02:48**

Rosehill Firm

John, we have seen suspicious activity on **you're** account.

We saw unusual activity on your payroll account last night and have suspended your account.

You must login in 24 hours and verify your account details or your account will be **permanently disabled** and you will not receive your payroll.

See attached document for account information and use the link below to verify your details.

Click Here to Verify

Phishing websites

Phishing websites are usually what phishing emails will be asking you to visit. These phishing websites 'spoof' legitimate webpages – they pretend to be a website you know and trust to trick you. Even if you are utilising an anti-virus software, these websites can give your devices malware or steal card details or login credentials.
Here's some ways that you can identify fake websites:

Suspicious domain names - In spoofing established websites, criminals will register their websites with names that are similar to well-known websites. These are usually only different by subtle spelling or letter changes. Some websites linked in emails will have nothing to do with the content of the emails. If the domain is different than the usual site, this is a red flag.

Top Level domain - These come at the end of a URL; things like '.com,' '.co.uk' or '.org.uk'. Sometimes, a phishing website will be the same as the real page, with the only different being the top-level domain. Be wary of supposed large websites and companies using the less common top-level domains such as '.biz', '.cn' or '.casa'.

http/https - At the beginning of the URLs of webpages that you are inputting sensitive information like card details or a phone number, the domain should be using 'https'.
If it is only using '**http**,' this is a major red flag.

Website content - Official company websites will have sharp webpages, with tight writing and content. If there are low quality images and spelling mistakes on the website, it might be a scam. Fraud websites don't often have an 'About Us' or 'Contact Us' page, so look out for those as well.

View a helpful video:

SATT Phishing Module
A guide to phishing websites

What should you do if you've been sent a phishing email?

Ignore all attachments and links. Don't open any attachments or links from a source that you don't trust.

Don't reply. Don't reply to scam emails, even just to say 'No,' as then the scammers will know your email is active and will send you more emails.

Double-check before sending any details. If you get an unexpected email from your job, look up their contact information and give them a quick email or call them to check.

Stay protected. Make sure that your anti-virus software is updated on your personal devices, and make sure you understand whatever anti-virus measures are in place on your work devices. Report the email. While not engaging with the email is the correct thing to do, reporting the email is also important in helping the scammer stop.

Reporting Phishing

If you are remote working, report the email to your employers IT services. This is especially important if the email has any sort of detail from your work, as it is more than likely that the criminal will try to target other employees as well. Even if you think you're being paranoid, it's better to be safe than sorry.

Forward any suspicious emails to **report@phishing.gov.uk**. As of June 2025, the National Cyber Security Centre (NCSC) states that there have been 43 million scams reported, which has resulted in 225,000 scams being removed across 405,000 URLs.

Always report suspicious emails and sites. Whilst you might not have fallen for the scam, their next target might not be so lucky. Reporting these phishing scams not only protects you and your employer but might also help someone else too.

If you think you've been a victim of phishing fraud, you should **report it to Action Fraud, the UK's national fraud reporting centre**.

*The Office for National Statistics
** Astra Security: https://www.getastra.com/blog/security-audit/phishing-attack-statistics/
*** EMCRC: https://www.emcrc.co.uk/post/remote-work-navigating-the-benefits-and-pitfalls-of-wfh