BOXPHISH

Identifying & Protecting your Organisation from Phishing Attacks

What is a phishing attack?

Phishing attacks are constantly on the rise. They have rapidly become the most popular type of cyber-attack, with over **3.4 billion** phishing emails sent out every single day worldwide.

A phishing attack – most commonly delivered via email – is a type of social engineering attack. The attack occurs when the cybercriminal sends a fraudulent message designed to trick the receiver into revealing sensitive information about themselves, or click on a malicious link.

This can be done in several ways, with phishing emails now so sophisticated, that they're often hard to differentiate from the real thing.

Common phishing attacks you might encounter

Although phishing emails can be delivered in countless different ways, they are almost always trying to get you to reveal one of two things: your password or your bank details.

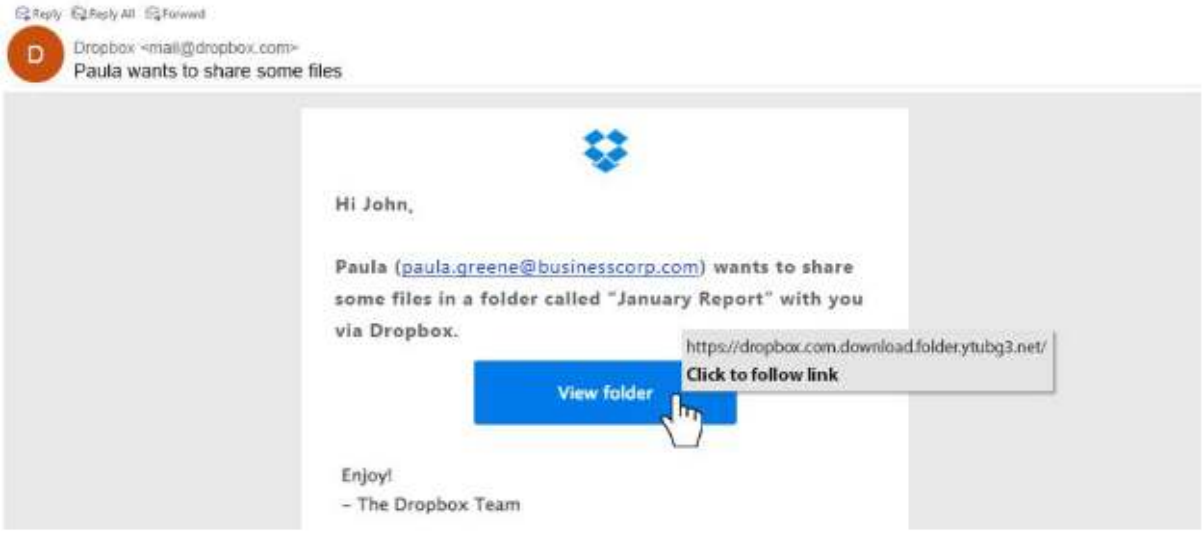
Cyber criminals will attempt to contact you from an account or company you are familiar with, playing on an already established trusting relationship. It's important to remember that a phishing attack can come from **any** source, and there are no names or organisations which can't be spoofed.

The most common email topics include:

- Bank details expired, please confirm card number
- Password needs resetting, please enter details
- Suspicious login on your account, please confirm password
- We've had to reschedule your appointment, please click this link...

Examples

Let's take a look at some popular phishing attacks and highlight the areas you should be looking out for:

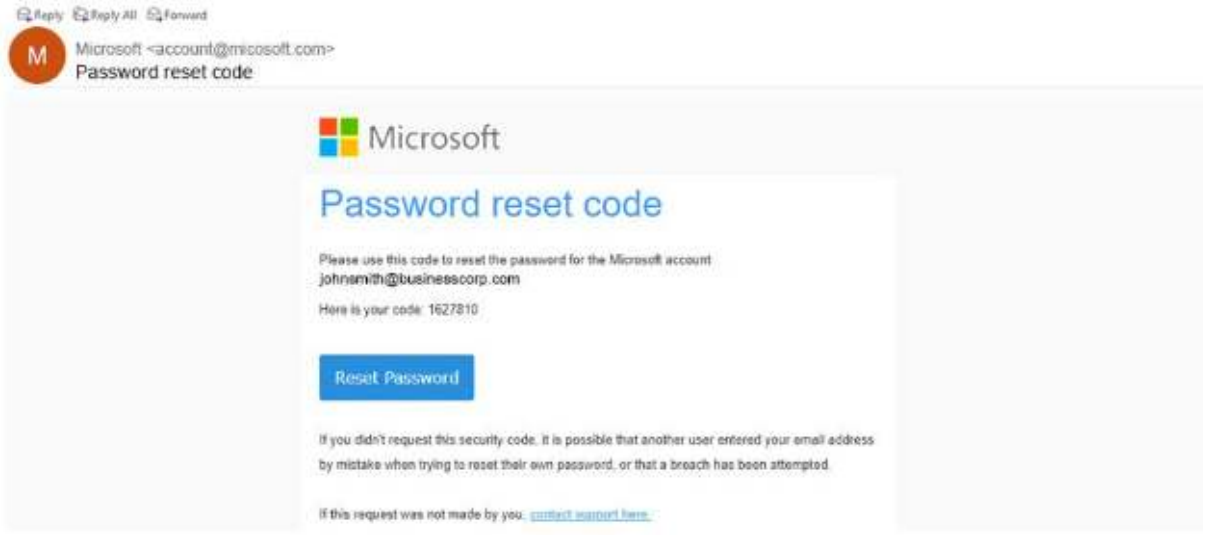


At first glance, this Dropbox email looks like it could be legitimate. The email addresses shown are both valid and there aren't any spelling mistakes in the content. However, whenever you see a link included in an email, you should always act with caution.

In this case, **hovering over the link** reveals that the actual URL is hosted on ytubg3.net, NOT on Dropbox and therefore identifies this as a phishing attack.

You should always hover over a link to check it is legitimate before clicking on it – if you're unable to do this on your mobile device or tablet, either wait until you can use a desktop to review the link, or if you don't have access to a desktop device, copy the link and paste it into an incognito browser window to ensure not of your details are captured.

If you're unable to do either of these options, then act with caution and ignore the email. Reach out to the supposed sender on a separate chain or through a new medium to try and verify if the email is a phishing attack or not.



One of the more tried and tested methods used in phishing emails is through a misspelling or spoofed site name or email address. In this case, the body of the email itself all looks legitimate, with no spelling mistakes or obvious errors – however if you look closely at the sender's email address, you'll spot a **missing r in the spelling of Microsoft**, meaning this is not a legitimate email.

In cases like this, never click on the link and immediately report and delete the email. You should then access the account in question independently, and ideally from a different device. This can help you to verify if the account is compromised and allow you to change your passwords if necessary, or to provide further peace of mind.

This email is very difficult to identify as phishing or not. The email address is valid for the company and there aren't any spelling mistakes or links in the content.

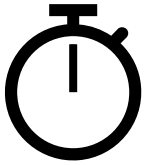
The tell-tale sign that this is a phishing email is in the language used. There are **several instances of urgent language** through the phrases 'right now', 'overdue' and 'fast response'. These prompts coupled with the **request for a large sum of money** flag this email as suspicious and lead us to identify it as a phishing email.

You should always act with caution when you see urgent language in an email, as it can be used very effectively as a scaremongering tactic – aimed at getting recipients to act impulsively without thinking.

You also need to consider who the request is coming from and whether it's part of the correct procedure to make a request for a large sum of money over email.

In cases like this, you should report the email to your IT department and then delete it from your server.

Always remember:



Take your time – no matter who the email appears to be from or what it is about, take the time to read it properly before acting

Check it twice – verify the validity on another device/browser, through a separate app or by browsing in incognito

Seek advice – if the email has come from someone you work with, ask them about it directly for confirmation

Just say no – if in any doubt whatsoever, report the email to your IT department and delete it from your inbox

The Increasing Threat

96% of phishing attacks are delivered via email, the other 4% are carried out via malicious websites (3%) and mobile phones (1%)

1/99 analysis of over 55 million emails has found that 1 in every 99 emails is a phishing attack

30% of phishing emails are opened, a figure that is up 7% from 2020 – showing how relevant the attack method remains

1.3m new phishing websites are created every month – even though they only account for 3% of total phishing attacks

71% of targeting attacks involve the use of spear phishing – where a particular individual or organisation is targeted

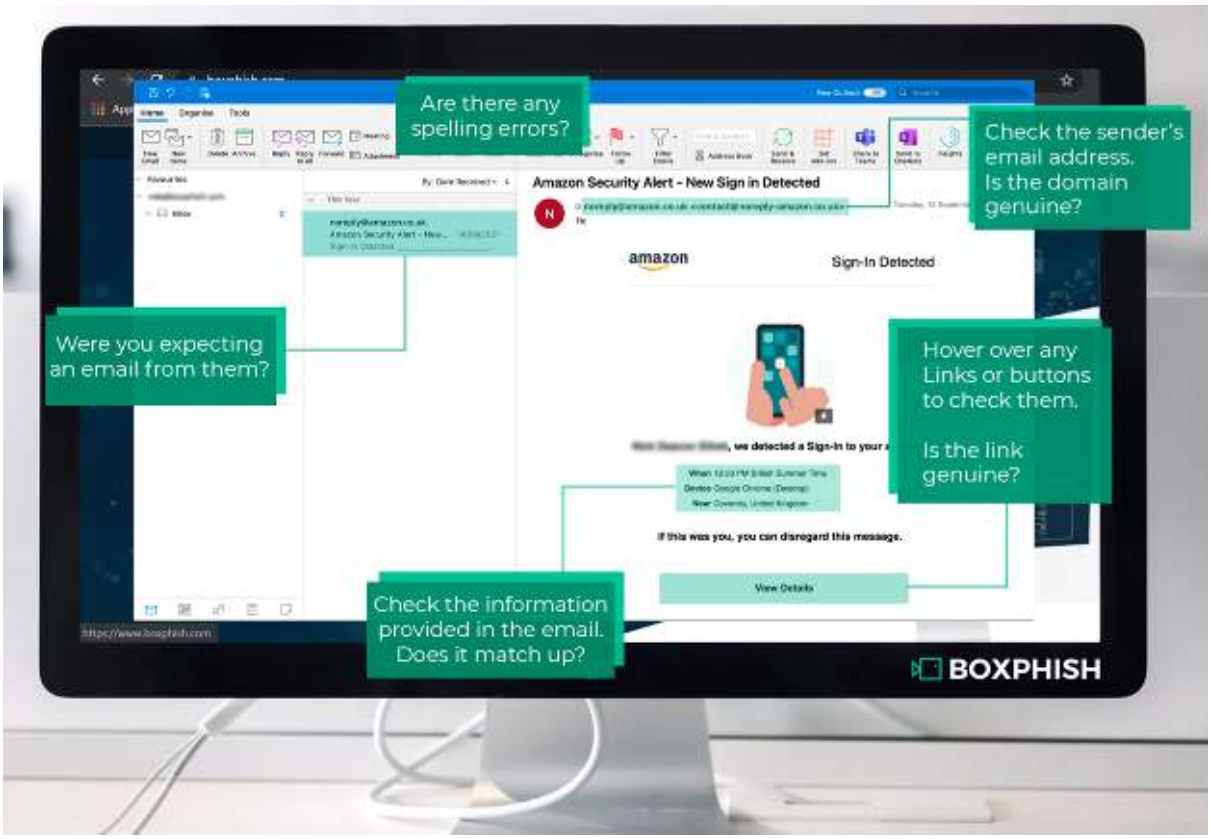
$15m is lost by companies worldwide as a result of phishing attacks every year – more than triple what it was just five years ago

Key Identifiers

As you'll have seen in the examples above, phishing emails often only have very minor errors in them, designed to be missed unless properly inspected. A few key things to look out for are:

- Urgent language
- Time sensitive requests
- Spelling mistakes
- Spoof website domains
- Unfamiliar email addresses
- Requests for large sums of money
- Suspicious links or click buttons
- Attachments

It's likely that you won't encounter all these identifiers in one single email, so you need to be constantly aware of them and constantly checking for them. Unfortunately, cybercriminals are now very advanced, so phishing emails tend to only include one very tiny error – remember though that if you are ever in doubt, be cautious and avoid interacting with the email.



How to protect your organisation

As phishing attacks and the cybercriminals behind them continue to evolve, we need to be as prepared as possible to deal with them. There are key things you should implement in your workplace to mitigate the risk of phishing attacks:

1. Secure email gateways

A secure email gateway allows you to monitor your employee's inbound and outbound emails, giving you the ability to scan them for malicious content and potential phishing attacks. If a potential threat is detected, the software will quarantine or block the email, stopping it from reaching the desired recipient.

However, while SEGs have been very effective in the past, they sometimes struggle to identify the more sophisticated phishing attacks, meaning many can slip the net.

2. Cloud email security

Cloud email security systems are embedded directly into your email network, monitoring all communications for malicious content. Cloud solutions use AI to identify potential cyber-attacks, which means they are more likely to capture the more sophisticated attacks – however they are still not regarded as 100% effective.

3. Cyber security training

Without question, the best way to defend your organisation against phishing attacks and other cyber security threats, is to invest in a reliable security awareness training platform. This limits the reliance on automated programmes and AI, putting the responsibility in the hands of your staff and training them to be the first line of defence.

At Boxphish, we offer cyber security awareness training alongside phishing simulations, providing our users with the tools needed to identify and avoid cyber-attacks before they take place.

Our phishing simulations impersonate real-world attacks, including everything from Microsoft and Google logins, to Netflix account verification, DPD deliveries, social media account verifications and even simulations that can be tailored specifically to your organisation.

The emails are delivered via our platform directly to the recipients' inbox, just as a real phishing attack would be and our reporting platform then allows you to identify where the biggest threat to your organisation is – right down from department to individual email addresses.

Alongside this we also offer wider cyber security awareness training, providing interactive content and bite-sized quizzes across a range of relevant topics. Our learning journeys are specific to each organisations' needs, covering topics including phishing, malicious software, physical and mobile device safety, GDPR, CEO fraud and many more.

To find out more about how cyber security training might be right for your organisation, visit www.boxphish.com and enquire about booking a free awareness training demo.