Bob's Business

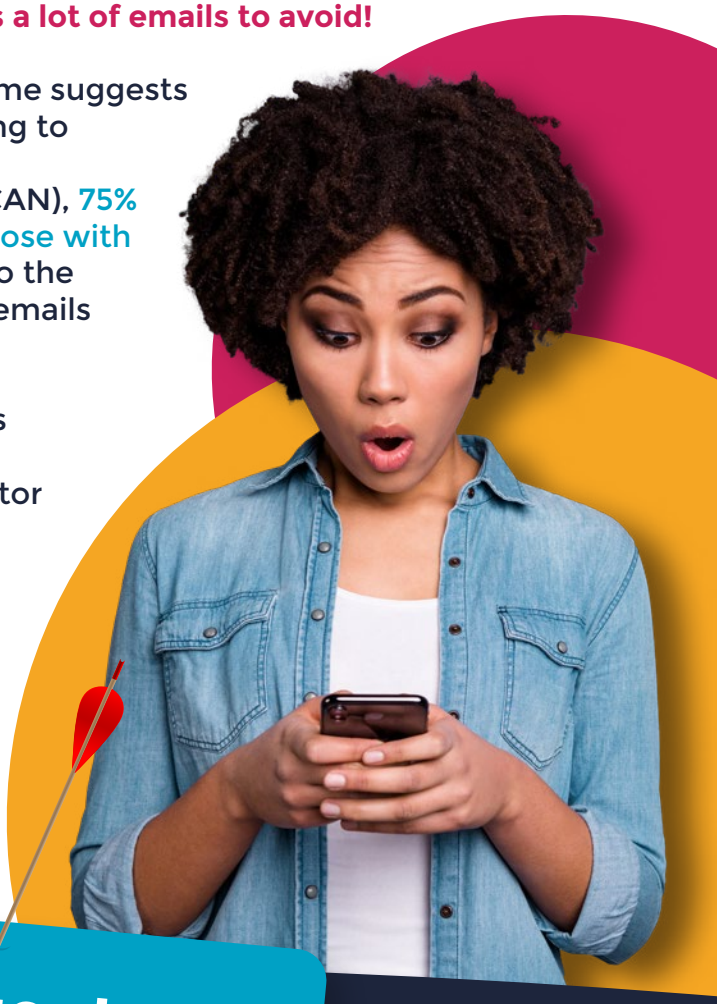
EVERYTHING YOU NEED TO KNOW ABOUT PHISHING

Have you ever received an email that didn't feel right? Like a receipt for an online order you didn't place, or a poorly worded email saying you've got money back from an annual tax return?

Don't be fooled though; these are phishing emails, and they are a genuine concern, particularly for those unaware of the threats they pose.

In a recent report, it was found that phishing and pretexting (a form of social engineering) represent 98% of cyber incidents and 93% of breaches, with organisations nearly three times more likely to be breached by social attacks than via technical vulnerabilities.

Recent reports have found that an astonishing 3.4 billion phishing emails are sent daily. Now that's a lot of emails to avoid!



Spam filters are designed to do what their name suggests and block spam messages. However, according to research from Plymouth's Centre for Security, Communications and Network Research (CSCAN), 75% of phishing emails without links and 64% of those with links made their way past spam filters and into the target inboxes. Even worse, only 6% of those emails were marked as malicious by email clients.

With 2023 now upon us, 39% of UK businesses who identified cyber attacks in 2022 named phishing attempts as their most common vector - A massive rise from 72% in 2017 to 83% to date.

But what is phishing, what types of phishing attempts are there, what should you do if you click a phishing email, and why should you be phishing your team? Join us as we share everything you need to know - and share access to one of our incredible phishing training courses.

Contents

What is phishing?

Phishing is the act of sending emails pretending to be from reputable companies to coax individuals into giving out sensitive information, such as passwords and bank details.

It's a criminal practice that dates back to 1996, stemming from hackers who broke into America On-Line (AOL) accounts by scamming passwords from unsuspecting users.

Phishing attacks have come a long way since they first arrived in inboxes in the late 90s. Today, they utilise proven psychological principles and bold imitations to convince you to give away your private details.

Indeed, phishing attacks have spread beyond even email, with forms of phishing targeting text messages, phone calls and more. This brings us to...

What are the types of phishing attacks?

Spear phishing

This type of attack involves sending a targeted email or electronic communication scam to an individual or organisation. Through social engineering techniques, a cybercriminal will gather data about an individual or organisation to craft detailed, realistic fake emails that deceive you into inputting your credentials.

Whaling

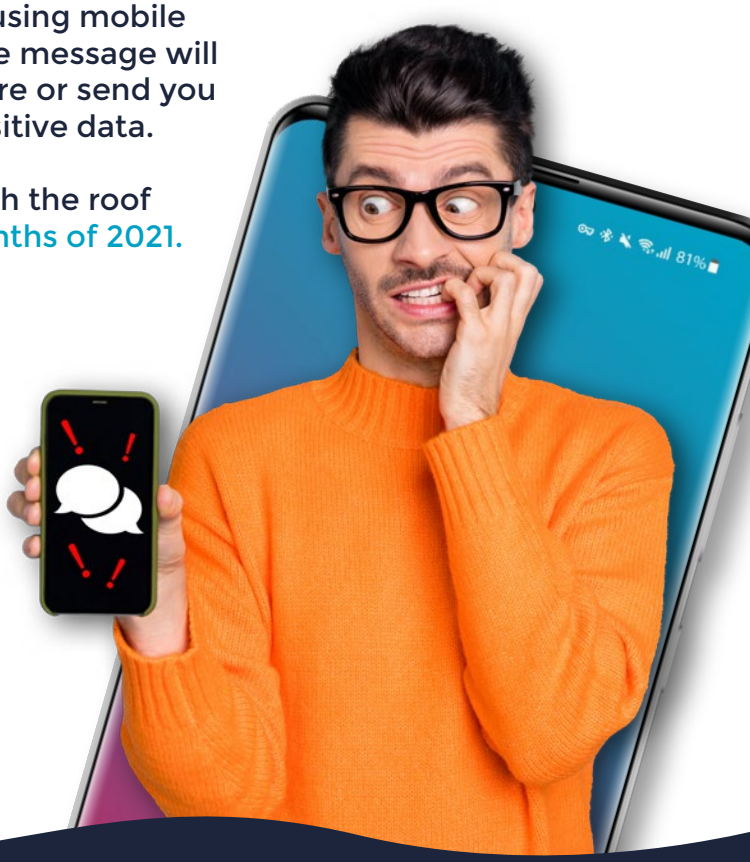
Whaling refers to a phishing attack aimed at senior executives or an email masquerading as an executive to steal sensitive data or prompt the transfer of money.

Only recently, the toy company Mattel lost over $3 million due to a whaling attack where a finance executive transferred money, believing the request had come from the company's new CEO.

Smishing

Smishing refers to SMS phishing, an attack using mobile text messaging to extract sensitive data. The message will include a link to download malicious software or send you to a fake website that will capture your sensitive data.

Cases of smishing attacks have gone through the roof recently, rising over 700% in the first six months of 2021.



Vishing

A vishing attack is one that uses phone calls or leaving voicemails to trick the recipient into sharing sensitive information. The caller will usually pretend to be a person of authority, such as calling from a bank or an IT support team, and will ask a series of questions that give access to your accounts. Look out for calls that encourage you to answer questions without consideration.

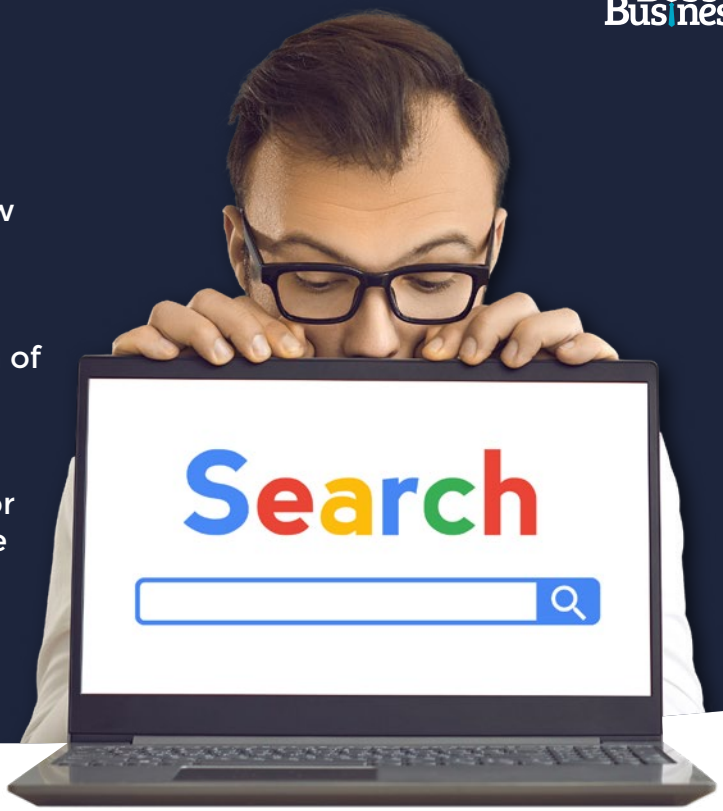
Email phishing

This is the type of phishing that most people are familiar with. This is a phishing scam that is sent by email to entice recipients to reveal sensitive data, either by directly responding to the email with information or by clicking a link that collects data. These general phishing emails are non-targeted and are instead cast as wide as possible. After all, it only takes one person in your organisation to fall victim to compromise your internal security.

Search engine phishing

Search engine phishing is a relatively new phishing technique that involves the fraudster creating a legitimate-looking website that features in search engine rankings - often in the 'shopping' section of a search query.

The website will typically offer amazing deals, but when the website user pays for their order the products never arrive. The payment details might also be used for further fraudulent purposes, such as making big purchases.



How to spot a phishing email

We're all humans, and, as such, we're not always the best when it comes to judging risk. Some of us receive hundreds of emails a week, with many perfectly legitimate, which can lull us into a false sense of security, assuming that every email we receive is to be trusted.

Making small changes to your habits, so that you treat every incoming email with suspicion, can make a significant difference when it comes to preventing a potential breach

7 Signs to look out for when spotting a phishing email

1 The sender's address doesn't seem right

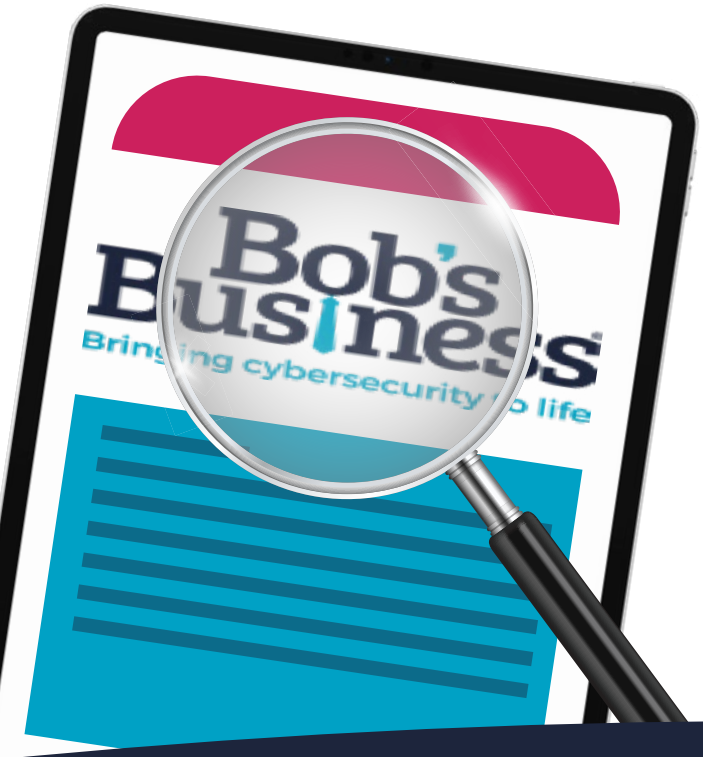
When you open an email, always check the sender's email address first. If an email claims to be from a company you know, but the sender's email address doesn't match up, then that's a sign something isn't right.

Emails from addresses such as '1253628uwhdnwd@hotmail.co.uk' or 'info@amazen.co.uk' are early telltale signs that the email is not to be trusted.

2 The email has poor spelling and grammar

When you're reading an email, look out for any spelling or grammar errors, and also consider how well-written the email is. Official emails will usually contain no spelling or grammatical errors, typically because professionals wrote them. Criminals, however, tend to cut corners.

Then you need to start asking questions!



3 The email has an odd use of imagery

Some phishing emails will often use attractive imagery and graphics, such as photographs or company logos, to make them look more like emails you'd get from a marketing team.

Remember to bear in mind that just because the email contains nice pictures and looks like it's laid out professionally doesn't mean it might not be a phishing email.

Check the logos and images, if they're blurry, of poor quality or look stretched out, that's a dead giveaway that somebody has taken it from a quick Google search.

4 The email is designed to make you panic or make a hasty decision

Many phishing emails are designed to create a sense of urgency or make you panic, such as time-sensitive offers and situations that prompt you to act immediately and make impulsive decisions without thinking.

You might receive an email claiming to be from one of the systems that you use telling you that your account will be deleted if you don't confirm your email address within an hour. This is a tactic designed to make you panic and throw caution to the wind.

Our research has found that combining a sense of danger with the appearance of an internal email can result in 94% of recipients clicking through, highlighting just how potent these psychological principles can be.

5 The email sounds too good to be true

> Good news. Having looked at your tax payments for 2022, you overpaid by £157. Click here to start processing your claim.

At a glance, you'd probably think it was a nice quick win for your bank account.

Unfortunately, phishing emails usually offer attractive incentives like this so that you rush into getting your hands on it without a second thought. Whenever there's an incentive in an email, always think twice. Remember, if it reads too good to be true, it probably is!

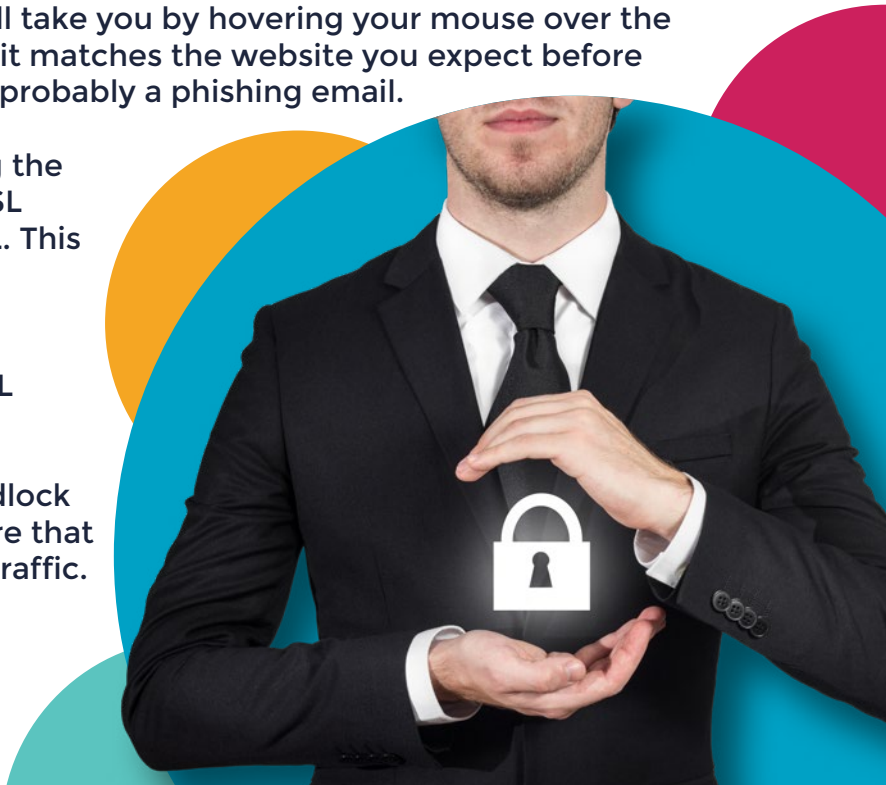
6 The URL you're being linked to isn't legit

Hiding a link in an email is easy. Some phishing emails will place links on bits of text or buttons so it doesn't have to reveal a URL.

But you can check out where a link will take you by hovering your mouse over the text. Take note of the URL and ensure it matches the website you expect before clicking! If the URL doesn't match, it's probably a phishing email.

Another good practice when checking the validity of a link is to look out for an SSL certificate at the beginning of the URL. This will show as HTTPS as opposed to just HTTP.

When installed on a web server, an SSL (Secure Sockets Layer) allows secure connections from a web server to a browser. This will appear as a little padlock at the far left of the URL bar and ensure that no cybercriminals can snoop on your traffic. Note, however, this doesn't ensure a website is legitimate in the first place.



7 Check the company branding in the email

Phishing emails will try to mimic well-known brands to gain your trust and get you to let your guard down, whether you use those services or not.

If you receive an email from a company that you haven't subscribed to, that's probably because it's a phishing email trying to impersonate that company.

You can easily catch these emails out by comparing them to ones you've received before from the company, do the logos match up? Are there glaring differences between the two?

What to do if you click a phishing link?

With phishing emails making up 1% of emails sent, an astonishing 3.4 billion hit our inboxes daily. Naturally, it's only a matter of time before somebody in your team accidentally clicks a link.

Clicking on a link in a phishing email can leave a business vulnerable to data loss. It is crucial that you and everyone in your organisation understand the right steps to take in the event of accidentally responding to a phishing email.

Phishing emails can be sent to anyone at an organisation, even people like fraud managers or IT security employees can fall victim to a cyberattack. Companies should have a cybersecurity policy and training awareness program in place that will help employees take the correct actions.

These are the steps that need to be taken after clicking a phishing link:

1 Report the incident

Your first step should always be to report the incident to your relevant internal team.

By immediately reporting the incident to the relevant team, such as the IT security incident team or service desk, action can be taken to prevent other people in the organisation from doing the same thing.

It is important to note, however, employees might be embarrassed that they have been tricked by a scam and become hesitant about reporting the incident. This is why it's so important that your organisation provides training and awareness that encourages employees to report security incidents without fear that they will be in trouble.

2 Change login passwords

One of the ways that data is compromised through phishing attacks is by tricking people into providing their login credentials, so it is vital that your passwords are changed as soon as possible after a phishing attack.

In many cases, a victim will use the same password for numerous accounts; this can cause a chain reaction of breaches across their accounts. As such, you will need to update all of your passwords as soon as possible.

Passwords should be difficult to guess, training should be provided to ensure that employees know how to set difficult passwords.

Looking for a proven method for secure passwords? Pick three random words and combine them with numbers for an easy-to-remember, impossible-to-guess password! Something like Track4Super9Warthog& fits the bill perfectly.

3 Investigation of the attack

Once a phishing attack has been reported, the relevant team should conduct a thorough investigation into the circumstances. Endpoint analysis will help to identify if any malicious software has been introduced onto the PC or network.

The investigation should help to decide whether there is a specific security process or system weakness that requires strengthening.

4 Inform the regulators and legal authorities

Organisations must comply with the rules of their regulatory authorities, such as reporting a phishing incident within a specific amount of time. It may also be necessary to inform the police so that criminal investigations can be completed.

How can you stop phishing attacks in your organisation?

The bad news, when it comes to stopping phishing attacks from arising, you're out of luck. In fact, studies have found that 75% of phishing emails without links and 64% of those with links made their way past spam filters from the most popular email providers.

The good news? Your team can be trained to spot and report them before they click and expose your business.

The answer is simulated phishing training. At its heart, it's the practice of deploying carefully designed fake phishing emails to your team, then directing those that click to specialised training that shows them how they can spot and stop attacks in the future.

Analysis of our simulated phishing campaigns found that just 1 year of campaigns reduced the likelihood of an employee opening a phishing email by 29%.

Bob's Business makes deploying simulated phishing campaigns simple, affordable and achievable for organisations of any size.

Fully managed and designed in conjunction with behavioural scientists, Bob's Phishing is your award-winning ticket to a more secure and knowledgeable team.

Ready to get started? Click here to book a meeting with one of our cybersecurity experts, or get a taste of one of our phishing training courses with the innovative Hook, Line and Sinker by clicking the logo below.

HOOK, LINE AND SINKER

Phishing Simulation Game

Click here to access your free training course

Why choose Bob's Business?

At Bob's Business, we make reducing your risk easy, measurable and engaging.

Working closely with your key stakeholders, we create a bespoke package tailored to your business needs, eliminating the necessity and high costs of employing extra staff to deliver effective training solutions.

Changing behaviour and creating a positive security culture takes time and consistency, which is why we stay with you from start to finish, providing regular metrics, support and reinforcement materials to ensure that lessons learned are not lost.

We believe in quality over quantity, and with engagement rates of over 90%, you can be sure your staff are getting a premium solution that relies on science and psychology to implement measurable and long-lasting behavioural change.

Trusted by:

HOTEL Chocolat. · Charlotte Tilbury · HELLY HANSEN · mfg motor fuel group · East of England COOP

About Bob's Business

Founded in 2007 by Melanie Oldham OBE, Bob's Business was created to mitigate the risk which makes all organisations susceptible to cybersecurity breaches - their workforce.

Today, Bob's Business is a leading provider of scientifically-informed cybersecurity awareness training and phishing simulation, working with organisations across the private and public sector to educate staff, transform cultures and deliver meaningful change.

Get in Touch

Visit us online:
www.bobsbusiness.co.uk

Call us:
01226 337335

Email us:
info@bobsbusiness.co.uk

Book a Demo