

Go phish!

The top ten types of phishing scams

Learn the tricks to spot
and prevent them





Spot the phish

Many of us receive hundreds of emails a day, making staying on top of things and working through them all quite the hassle. But as if that wasn't enough, we don't just receive business-related emails. Many spam emails sneak themselves into your inbox, pretending to be a 'normal' email – maybe an urgent password request from your business partner or CEO.

You're already stressed and distracted. Then you open the email to send them your details before realising that you were tricked. Tricked into revealing sensitive and business threatening data.

With the shift to hybrid working, our inboxes have been taken over by phishing emails waiting to blast businesses' databases. To help you better protect yourself and safeguard your data, we've listed the top 10 phishing scams, how you can spot them, and how you can prevent them in the future.





#1 Email phishing

Email Phishing is the most common type of phishing attack. Cybercriminals will send these kinds of emails to any email addresses they have, impersonating a certain brand, informing you that your account has been compromised and claiming that immediate action needs to be taken. They'll include a malicious link, prompting you to click on it or download an asset. You'll then be either redirected to a website that steals your credentials or infects your device with malware, or you'll automatically download malware onto your computer.

How to spot email phishing:

- **Spelling mistakes:** this type of email usually includes language or grammar mistakes and are easier to spot than other scams.
- **Shortened links:** shortened links are used to trick Secure Email Gateways.
- **Information & fake branding:** try to find legitimate information about the brand and compare it to the sending domain to see if you can identify any misspellings or a wrong domain.
- **Logos & images:** look for logos or images that could include malicious links.



#2 Spear phishing

A spear is used to catch a specific phish, hence the name Spear Phishing. This type of attack follows a more targeted approach to a specific person or group of people within an organisation. Hackers go and find publicly available data of an employee, for example, on your business' website or social media. They use this information to impersonate a fellow colleague or familiar person to make it look like an internal request, tricking individuals into sharing sensitive information such as passwords.

How to spot spear phishing:

- **Unusual behaviour:** unusual requests coming from a person with a specific job function can indicate a scam. Would this person ask you for this?
- **Password-protection:** if you're asked to provide a login and password to open documents, this could be a tactic to trick you into sharing your credentials.



#3 Whaling or CEO fraud

Whaling emails or so-called CEO fraud emails will impersonate the 'whale', the big fish of a company. Cybercriminals will find personal information about the CEO, managing director, or another leading person of an organisation and use their details to trick their staff into revealing sensitive data such as tax IDs or bank account numbers. Scams involving tax returns are very popular as they can reap highly valuable data.

How to spot whaling or CEO fraud:

- **Unusual behaviour:** it might be odd for a senior member to get in touch with you to request money personally.
- **Mismatching email address:** double-check if the email address really matches the sender's details.





#4 Smishing & vishing

Smishing is an attack that happens over text messages, whereas vishing happens via phone calls. Cybercriminals will send text messages or call individuals and ask them to take action against their best interests. Smishing messages will usually include a link or return phone number and ask you to verify your bank details, while on vishing calls, you'll be asked to reveal personal information directly.

How to spot smishing & vishing:

- **Salutation:** smishing usually uses very formal ways of addressing people with 'Sir' or 'Madam'.
- **Phone number:** vishing callers usually use a blocked phone number. For smishing messages, you should always compare the sender's message with the brand or organisation's details they're impersonating.
- **Unusual behaviour:** the request might be unusual for this type of brand or organisation.



#5 HTTPS phishing

HTTPS (hypertext transfer protocol secure) is considered a secure version of HTTP and conveys the legitimacy of an organisation. However, many phishing websites are served on HTTPS now and send links including HTTPS to trick people into clicking on a legitimate-looking link.

How to spot HTTPS phishing:

- **Shortened links:** shortened links are usually malicious links.
- **Hypertext:** hypertext within the email that is used to hide the actual URL could indicate HTTPS phishing.

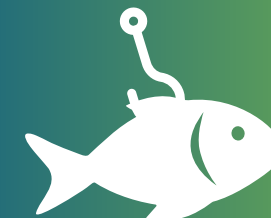


#6 Watering hole phishing

With this type of phishing, cybercriminals will monitor which websites your employees tend to visit often. They will then infect these IP addresses with malicious links or downloads. Anytime your employees visit that website, they will download the malicious code, meaning malware is installed on your systems. Hackers will then be able to steal your data and the malware will start spreading to other systems.

How to spot watering hole phishing:

- **Browser alerts:** these state that the website might have malicious codes.
- **Firewall protection:** through firewall monitoring, you can prevent traffic coming from an infected website.





#7 Clone phishing

Clone Phishing is a scam where cybercriminals replicate a legitimate message that the victim might have received at some point. The links or attachments in the email will be swapped with a malicious link or malicious attachments and sent from a seemingly legitimate address.

How to spot clone phishing:

- **URL mismatch:** mismatching links and the displaced URL can indicate clone phishing. Compare the link and the displaced URL by hovering over the link.
- **Sender mismatch:** double-check if the sender is off somehow and if it matches the sender's details.



#8 Social media phishing

With social media phishing, hackers will use social media channels like Facebook or Instagram to get your data or trick you into clicking on malicious links. By creating fake accounts and impersonating a brand or someone the targeted person might know, they'll try to fool the victim.

How to spot social media phishing:

- **Suspicious link:** if you have received a message asking to open a link, ensure that this is a legitimate contact.
- **Too good to be true:** if you're offered a deal that sounds too good to be true, then it's probably fake.



#9 Evil twin

Evil twin is a type of phishing scam where a cybercriminal will create a fake Wi-Fi hotspot that looks like a real one. If a user enters the hotspot, hackers can eavesdrop on their network and steal credentials, passwords, or other sensitive information transferred through the connection.

How to spot evil twin:

- **Unsecure warning:** don't use a hotspot if your device tells you that this might be an unsecured network.
- **Login details:** it's unusual that a hotspot which doesn't usually require a login suddenly asks for one.





#10 Pharming

Pharming is a more technical approach and harder to detect. Hackers won't target their victims directly, but they target DNS servers (Domain Name System). DNS converts natural language into IP addresses to locate and direct visitors to devices. Through pharming, hackers will target DNS servers and redirect visitors to malicious websites that look very real. In this way, cybercriminals can steal the website visitor's data.

How to spot pharming:

- **Unsecure website:** websites with HTTP are usually not secure. HTTPS are secure websites.
- **Fake websites:** unusual fonts, language errors, or mismatching colours are usually a sign for fake websites.

Red flags that can indicate phishing scams



Poor grammar or spelling mistakes



Messages that convey a sense of urgency



Unusual greeting or salutation



Inconsistent or mismatching email addresses, domains, or links



Too good to be true offers



Suspicious downloads or attachments



Messages asking for personal information



How to protect your business from phishing attacks

Implementing the right solutions and tools can help you mitigate risks and protect your business from falling victim to a phishing scam.

Create a password policy

Remembering several complex passwords is almost impossible. That's why many employees use very simple passwords across many accounts leaving you vulnerable to phishing scams. Enforce a password policy with specific rules on password length, complexity, etc., and use a password manager where your staff can store their passwords.

Deploy multi-factor authentication

Cybercriminals are usually on the hunt for credentials and passwords. However, aside from creating complex passwords, implementing multi-factor authentication for your accounts will make it harder for them to get into your accounts and systems.

Keep your systems up to date

Running regular updates and keeping your software up to date is crucial when it comes to data protection. If you don't install regular updates, this might create security gaps and vulnerabilities in your systems. Update, update, update!

Train your employees

The best and most important thing you can do to protect your business and your data from phishing scams is to train your staff on how to spot them. With a comprehensive cybersecurity awareness training, they will learn everything about phishing attacks and how to spot and prevent them. Your employees are the strongest layer of protection.

Install security software

Robust security software is your first layer of protection against phishing scams. Software like anti-virus, anti-malware, firewalls, and spam filters can protect your systems from malicious links and attachments. Deploying web filters that prevent your staff from going onto malicious websites adds protection too.




Back up your data

Make sure to back up your data regularly in case you fall victim to a phishing scam. This is important to avoid damaging downtime or business failure in the event of a disaster. A comprehensive business continuity plan can help you keep your business operations running.



With the rise of phishing scams and the increased threat to your business, it's crucial to think about your next steps for your cybersecurity strategy. Whether you need to train your employees, set up comprehensive security software, or are looking to get cyber essentials certified, Ratcliff IT will help you get the protection you need.

With Ratcliff IT your IT is in safe hands.

 020 3551 6262
 hello@ratcliff.it
 www.ratcliff.it

