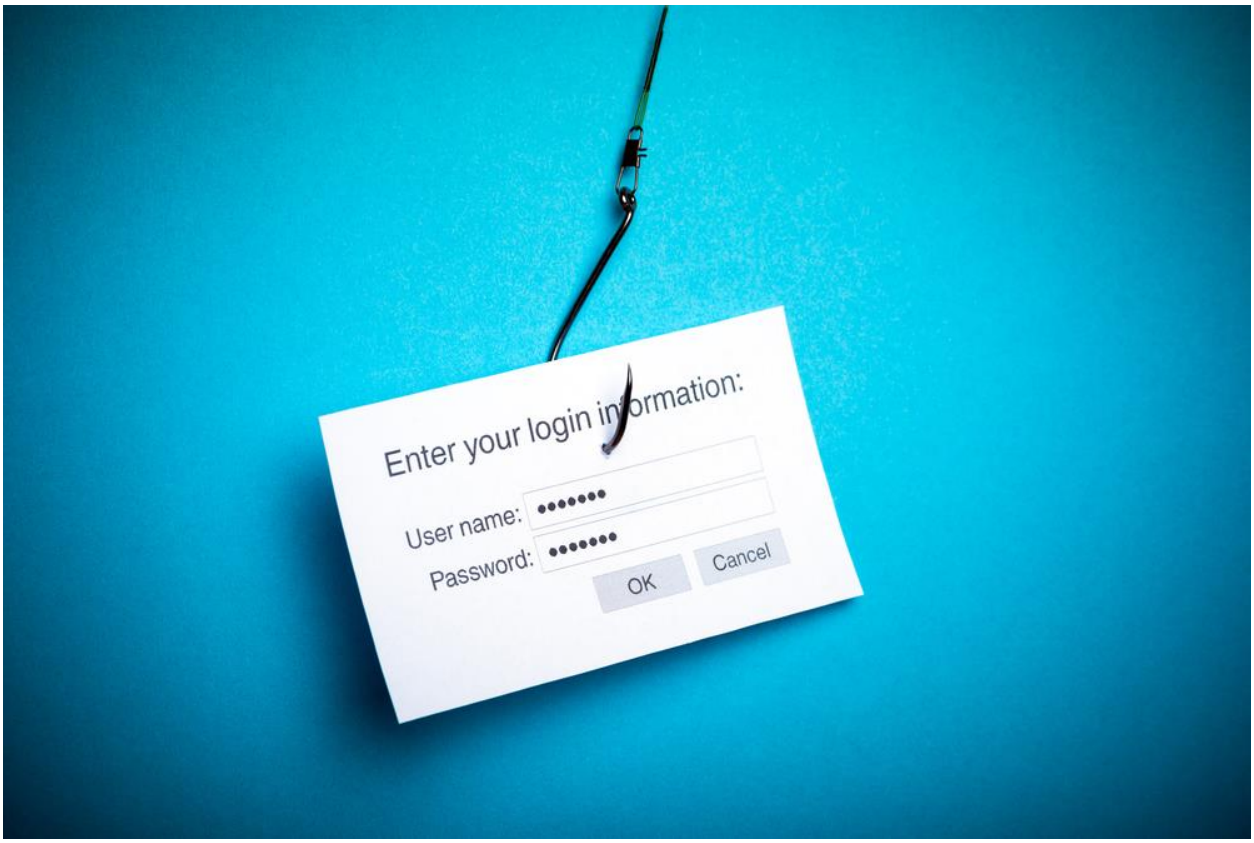
5 Ways to Spot a Phishing Email



A phishing attack is a form of social engineering by which cyber criminals attempt to trick individuals by creating and sending fake emails that appear to be from an authentic source, such as a business or colleague. The email might ask you to confirm personal account information such as a password or prompt you to open a malicious attachment that infects your computer with a virus or malware.

Phishing emails are one of the most common online threats, so it is important to be aware of the tell-tale signs and know what to do when you encounter them. Here are five ways to spot phishing attacks.

1. **The email asks you to confirm personal information**

Often an email will arrive in your inbox that looks very authentic. Whether this email matches the style used by your company or that of an external business such as a bank, hackers can go to painstaking lengths to ensure that it imitates the real thing. However, when this authentic-looking email makes requests that you wouldn't normally expect, it's often a strong giveaway that it's not from a trusted source after all.

Keep an eye out for emails requesting you to confirm personal information that you would never usually provide, such as banking details or login credentials. Do not reply or click any links and if you think there's a possibility that the email is genuine, you should search online and contact the organization directly – do not use any communication method provided in the email.

2. **The web and email addresses do not look genuine**

It is often the case that a phishing email will come from an address that appears to be genuine. Criminals aim to trick recipients by including the name of a legitimate company within the structure of email and web addresses. If you only glance at these details they can look very real but if you take a moment to actually examine the email address you may find that it's a bogus variation intended to appear authentic – for example: @mail.airbnb.work as opposed to @Airbnb.com

Malicious links can also be concealed with the body of email text, often alongside genuine ones. Before clicking on links, hover over and inspect each one first.

3. **It's poorly written**

It is amazing how often you can spot a phishing email simply by the poor language used in the body of the message. Read the email and check for spelling and grammatical mistakes, as well as strange turns of phrase. Emails from legitimate companies will have been constructed by professional writers and exhaustively checked for spelling, grammar and legality errors. If you have received an unexpected email from a company, and it is riddled with mistakes, this can be a strong indicator it is actually a phish.

Interestingly, there is even the suggestion that scam emails are deliberately poorly written to ensure that they only trick the most gullible targets.

4. **There's a suspicious attachment**

Alarm bells should be ringing if you receive an email from a company out of the blue that contains an attachment, especially if it relates to something unexpected. The attachment could contain a malicious URL or trojan, leading to the installation of a virus or malware on your PC or network. Even if you think an attachment is genuine, it's good practice to always scan it first using antivirus software.

5. **The message is designed to make you panic**

It is common for phishing emails to instill panic in the recipient. The email may claim that your account may have been compromised and the only way to verify it is to enter your login details. Alternatively, the email might state that your account will be closed if you do not act immediately. Ensure that you take the time to really think about whether an email is asking something reasonable of you. If you're unsure, contact the company through other methods.

Ultimately, being cautious with emails can't hurt. Always member this top STOP. THINK. CONNECT.™ tip:

When in doubt, throw it out: Links in emails, social media posts and online advertising are often how cybercriminals try to steal your personal information. Even if you know the source, if something looks suspicious, delete it.

Author Bio

Mike James is a Brighton based writer and cybersecurity professional who specializes in penetration testing, ethical hacking and other cybersecurity issues facing businesses of all sizes.

https://staysafeonline.org/blog/5-ways-spot-phishing-emails/