How to Spot Phishing Emails

Phishing attacks continue to play a dominant role in the digital threat landscape – as the most common attack vector for cyber criminals. Despite major advancements in security technologies in recent years, phishing attacks continue to increase in number and impact.

Security has always been a major concern for all companies, but there’s a misconception that threats only come from the outside. Reports show that employees are one of the biggest security threats, due to their risky habits and poor security knowledge, which is why it’s so important to train your team to spot and avoid suspicious communications, such as phishing emails.

Let's look at some of the common features of phishing to help you spot the malicious content and protect yourself:

**Phishing Emails May Appear to Be From a Company You Know**

Many phishing emails will be structured to look like they are from commonly known sites or sources, such as your bank or companies like Netflix. They will use the company’s logo and try to pass it off as a message from a reputable source. It is always important to check the sender details, to ensure that the email address that the mail came from is as expected.

**Phishing Emails Often Ask You to Confirm Personal Information**

As phishing attacks become more sophisticated, the quality of the attacks have improved to the point where it’s very difficult to tell it apart from an authentic mail. The most difficult mails to spot are ones which are a near identical clone of a mail you typically receive, such as an email from your bank, government agencies, or subscription providers. These are most easily replicated, because there are so many mails coming out from these organisations, so it’s very easy for cyber criminals to build templates that look the exact same. One thing to consider, is that these organisations would rarely, if ever, ask you do provide bank details or personal details directly through email. If you are ever asked to provide personal or confidential details through an email, you should assume it’s suspicious and inspect it further. Do not reply or click any links, instead contact the company directly using publicly accessible details (not the details provided in the mail) and confirm if the communication is authentic.

**Suspicious Attachments**

In the age of cloud-hosted file management solutions, it’s not as common for people to share documents as attachments anymore. So, if you receive an email with an attachment from a company or individual that you do not recognize, it should be an immediate red light. Attachments from cyber criminals can contain malicious content, which installs a virus or malware on your device or network. In most cases, a virus will sit on your network for months before any action is taken by the criminals. They will sit in your files, gather data and once they have enough, they will execute an attack.

**Emails Demanding Immediate Action or Response**

Most phishing emails are designed to make the recipient panic, by including an urgent request. For example, many phishing mails may contain a message that threatens to cancel your Netflix subscription or electricity, because your credit card details have expired and you have not paid this month’s bill. These mails will claim the only way to resolve the issue is by immediately providing your bank details using the link provided. If you receive a mail like this, it is essential that you take your time to review the mail and assess if the ask is reasonable. If you’re unsure, you should contact the company who sent the email to confirm if it is authentic.

**Inconsistencies / Unfamiliar Elements**

If you are emailing the same people regularly, you should be pretty familiar with their tone of voice in an email, what language they use, what greeting they open an email with etc. Be aware of any deviate from what you are familiar with, as this may be a phishing email. For example, if you email someone who always opens with ‘Hi’ or ‘Morning’, but they suddenly send an email over starting with ‘Dear X’, you should assume it is a suspicious mail and inspect it further before responding or selecting anything in the message. Also look out for language used throughout the mail and the sign off, to see if there are any differences from the messages you typically receive.

**What To Do If You Spot a Phishing Email?**

The same advice applies for all suspicious looking emails – stop and think, before clicking or responding to anything. Phishing attacks are getting more sophisticated, but there are a lot of things that individuals can do to avoid being attacked and compromising your data. The most important thing you can do is be cautious when you’re communicating through email and if you have any concerns over communications, flag it with your IT department or provider.

At Nostra, it is our job to help people and organisations to feel safe and protect their businesses from any cyber criminals looking to take advantage of your vulnerabilities. If you are interested in discussing how Nostra can help safeguard your organisation from even the most sophisticated threats, please contact our expert team at <https://nostra.ie/contact/>