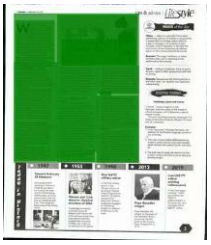
Media Title : New Sarawak Tribune
Headline : How to tell if an email is a scam?
Date : 28 February 2023
Section : News
Page : 3



How to tell if an email is a scam?

WE'VE all received strange and suspicious emails in our inbox. But while some are easy to identify as spam, others are less obvious. Maybe it's an email from Netflix, PayPal, or another account you use, claiming your password's been compromised. Or an old friend is suddenly reaching out to ask for financial help. These emails look and seem legitimate. But are they?

Here are some examples to demonstrate the common signs that someone is trying to scam you.

1. The email comes from a generic domain (Gmail, Yahoo, etc.)

Generic email domains such as @gmail.com, @yahoo.com, @hotmail.com, and @outlook.com are cybercriminals' favourites for sending scam emails. No legitimate organisation will send emails from an address that ends '@gmail.com'. Not even Google.

Except for some small operations, most companies will have their own email domain and email accounts. For example, genuine emails from Google will read '@google.com'. If the domain name (the bit after the @ symbol) matches the apparent sender of the email, the message is probably legitimate. By contrast, if the email comes from an address that isn't affiliated with the apparent sender, it's almost certainly a scam.

2. Urgent or threatening tone

Hackers want you to act quickly without realizing it's a scam. And the easiest way to do that is to prey on your emotions. The "scare" tactic is standard in phishing scams. By creating a sense of urgency or fear, they'll trick you into clicking on a link or downloading a suspicious attachment.

One of the most common phishing messages is claiming that your legitimate accounts have already been hacked. In this scam, they create emails that look like they're coming from an account you trust and use phrasing such as, "Unauthorised login attempt on your account," or "We've detected some unusual activity." These scam emails can be hard to identify, especially if they reference accounts you actually use. Before you click on a link, check the "From" email address. Is it from the actual company? If not, it's a scam.

3. A 'too good to be true' promise

Scare tactics aren't the only way that scammers prey on your emotions. If you receive an email claiming that you qualify for a reward or prize from a contest in which you didn't participate, it's likely a scam. For example, let's say you're living in Malaysia and you receive an email saying you won a US$50,000 prize from a competition in the US — but you've never been to the US (or entered the contest). Even if they use your full name or a common username, there's a pretty low chance that it's a lucky mistake. Instead, scammers are most likely trying to get you to enter your financial information or download malware on your devices.

4. Suspicious or unexpected links in the body of the email

The goal of most fake emails is for you to click on a link and go to a website that's designed to steal your sensitive information. Always double-check email links before clicking on them. You can do this by hovering your cursor over the linked text to see where it takes you. If the link is suspicious or doesn't match up with what you expect (based on the text or sender's name), be very cautious.

5. The domain name is misspelt

There's another clue hidden in domain names that provides a strong indication of phishing scams, known as typosquatting Also known as URL hijacking, typosquatting is when someone — maybe a cybercriminal, hacker, or perhaps just someone hoping to advertise a product or service — registers a domain name that is an intentionally misspelled version of other popular websites.

A famous example is the site Goggle.com, an address you might accidentally type when you want to perform a Google search. Originally, this site attempted to install a fake security programme on your computer, one filled with malware. If you type Goggle.com today, you'll end up at a site that immediately asks visitors for their age and gender for what it claims is a presidential election survey.