One of the most popular ways for cybercriminals to steal personal information is by using email phishing scams. Cybercriminals often use this method of attack to trick employees from large organisations into clicking onto malicious links so they can gain access to corporate networks that contain valuable data. Here are 10 tips on how to avoid becoming an email phishing victim.

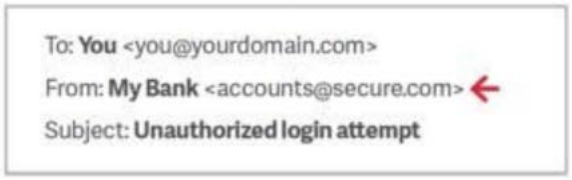
Phishing emails often masquerade as correspondence from a legitimate and trusted organisation, luring victims to click on links that will make them download malicious content or trick them into inputting sensitive information onto a fake website.

Recently, the Australian Communications and Media Authority (ACMA) warned Netflix users about a fake email that contained links to a phishing site that looks almost identical to the real Netflix page.

Security vendor Proofpoint has 10 tips on how to avoid falling for phishing scams:

#1 Don't Trust The Display Name

A favourite phishing tactic among cybercriminals is to spoof the display name of an email. Here's how it works: If a fraudster wanted to impersonate the hypothetical brand "My Bank", the email may look something like:



Since My Bank doesn't own the domain "secure.com", email authentication defences will not block this email on My Bank's behalf.

Once delivered, the email appears legitimate because most user inboxes and mobile phones will only present the display name. Always check the email address in the header from — if looks suspicious, flag the email. It's important to note that email addresses can be faked so it's not a fool-proof indicator.

#2 Look But Don't Click

Cybercriminals love to embed malicious links in legitimate-sounding copy. Hover your mouse over any links you find embedded in the body of your email. If the link address looks weird, don't click on it. If you have any reservations about the link, send the email directly to your security team.

#3 Check for spelling mistakes

Brands are pretty serious about email. Legitimate messages usually do not have major spelling mistakes or poor grammar. Read your emails carefully and report anything that seems suspicious.

#4 Analyse The Salutation

Is the email addressed to a vague 'Valued Customer?' If so, watch out—legitimate businesses will often use a personal salutation with your first and last name.

#5 Don't Give Up Personal Or Company Confidential Information

Most companies will never ask for personal credentials via email — especially banks. Likewise most companies will have policies in place preventing external communications of business IP. Stop yourself before revealing any confidential information over email.

#6 Beware Of Urgent Or Threatening Language In The Subject Line

Invoking a sense of urgency or fear is a common phishing tactic. Beware of subject lines that claim your "account has been suspended" or ask you to action an "urgent payment request."

#7 Review The Signature

Lack of details about the signer or how you can contact a company strongly suggests a phish. Legitimate businesses always provide contact details. Check for them.

#8 Don't Click On Attachments

Including malicious attachments that contain viruses and malware is a common phishing tactic. Malware can damage files on your computer, steal your passwords or spy on you without your knowledge. Don't open any email attachments you weren't expecting.

#9 Don't Trust The Header From Email Address

Fraudsters not only spoof brands in the display name, but also spoof brands in the header from email address, including the domain name. Keep in mind that just because the sender's email address looks legitimate (e.g sendername@yourcompany.com), it may not be. A familiar name in your inbox isn't always who you think it is.

#10 Don't Believe Everything You See

Phishers are extremely good at what they do. Many malicious emails include convincing brand logos, language, and a seemingly valid email address. Be sceptical when it comes to your email messages — if it looks even remotely suspicious, do not open it.

REMEMBER:

If you are unsure of any emails that you receive or any attachments that you get, contact the helpdesk on the details below and or forward the email as an attachment to the helpdesk.

t 02 8267 4404 **e** helpdesk@nswact.uca.org.au