



Phishing - Don't be caught by email scams!

In today's interconnected world, email scams pose a significant threat to both individual and university security. UNISA encourages all staff members and students to recognise warning signs and adopt best practices for online safety to effectively protect themselves, and others from these deceptive tactics.



Cybersecurity Awareness Campaign offers the following course designed to equip you with essential knowledge in just a matter of minutes:

- **Phishing** – Six clues that should raise your suspicious (4 min)

This course is tailored to empower you with the ability to **recognise malicious activities** from threat actors.

We strongly encourage you to complete these courses, as they will be instrumental in bolstering our collective cyber security.

How to participate in the training:

- You will have received an e-mail from noreply@terranovosite.com This e-mail is legitimate (and most definitely not a phishing e-mail) and from UNISA.
- Simply click on "Login Now" and participate in these valuable training courses.

Define tomorrow.

UNISA



Since phishing is the most common form of social engineering,

Let's take a closer look at seven areas in an email and their corresponding red flags.

The diagram shows an email interface with several red flags highlighted by callouts:

- FROM:** An email coming from an unknown address. You know the sender (or the organisation), but the email is unexpected or out of character.
- TO:** You were copied on an email and you don't know the other people it was sent to.
- DATE:** You receive an email that you would usually get during normal business hours, but it was sent at 3:00 a.m.
- HYPERLINKS:** There are misspellings in the link. The email contains hyperlinks asking you to take an action. When you hover your cursor over the link, the link address is for a different website.
- SUBJECT:** The subject line of an email is irrelevant or doesn't match the message content. It's an email about something you never requested or a receipt for something you never purchased.
- CONTENT:** The sender is asking you to click on a link or open an attachment. The email is asking you to look at a compromising or embarrassing picture of yourself or someone you know. You have an uncomfortable feeling, or it just seems odd or illogical.
- ATTACHMENTS:** Any attachment you receive that you aren't expecting.

The email content shown in the diagram is:

From: hr@yourorganization.cnet
To: judy@yourorganization.net
Date: Tuesday, December 3:00 AM
Subject: Urgent Notice

Hi Judy,

Now that our new CFO has been selected and starting soon, I'm asking everyone to fill out this quick survey so all the accounting functions can be captured. It should take you only few minutes. Must be completed by the end of the day.

Click here to take the [\[Survey\]](#) or download the attachment.

Thanks in advance for your cooperation!





<https://survey-monkee.com/>

Thanks so much. This really helps me out!

Your CEO

The diagram also shows a PDF attachment icon with a red arrow pointing to it.

NB: Additional Steps to Cyber Safety: Stay Secure, Stay Smart – keep UNISA secure!

			
<p>Use Strong Passwords</p> <p>The longer the password, the more secure it is.</p> <ul style="list-style-type: none"> • At least 16 characters long, • Includes uppercase and lowercase letters, numbers, and random symbols. • Doesn't include personal information, • Doesn't contain consecutive numbers or letters. 	<p>Turn on Multifactor Authentication</p> <p>Set-up MFA on your O365 accounts.</p> <ul style="list-style-type: none"> • Step-by-step on how to setup MFA – SOP Attached. 	<p>Update Your Software</p> <p>Keep your software up to date by enabling automatic updates.</p> <ul style="list-style-type: none"> • Request the ICT for further assistance. • Make sure that the following devices are updated with the latest operating system: Laptops, desktops, mobile phones, tablets, laptops, etc. • Also, update your applications – especially your web browsers – on all your devices too. 	<p>Think Before You Click!</p> <p>Think before you click.</p> <ul style="list-style-type: none"> • According to the Cybersecurity and Infrastructure Security Agency (CISA), "More than 90% of successful cyber-attacks start with a phishing email." • Pay attention to the above "red flags" shared.

Contact ICT-Help for reporting incidents.

<p>Contact details</p>	<p>ICT-Help: 012 429 4125 and student: 0800 00 1870</p> <p>Use the ICT-Self-service (MAXIMO) to submit your request: Welcome to Unisa ICT Service Desk</p> <p>Alternatively: Email: ict-help@unisa.ac.za (Unisa staff) or enquire@unisa.ac.za (Unisa students)</p>
-------------------------------	---