Presentation by:

ARTHUR MOSES OPIO - DICTS

12 MAY, 2026

MAKERERE UNIVERSITY

Email Fraud

Topic:

Email Fraud, Impersonation and Digital Safety WEBINAR | A Mak Community Conversation

Table of Contents:

Introduction

MAKERERE UNIVERSITY

Email Fraud/ Impersonation

The act of using one's name, identity, persona or brand without the consent of the victim. It is usually carried out to give out information that the owner would not avail by will. ***Some of the reasons why cybercriminals do this are to defraud, intimidate, harass, embarrass or threaten a concerned individual.*** Recently people use other people's identities to misinform the public in the interest of their gain.

Is Online Impersonation a crime?

Impersonation by itself is a crime and the legal consequences go beyond when it is accompanied by certain other acts such as committing criminal acts or a civil wrong.

Twitter says "***Twitter accounts that pose as another person, brand, or organization in a confusing or deceptive manner may be permanently suspended under Twitter's impersonation policy.***"

It is has become a very common act in recent days. ***Criminals have faked Police social media accounts to pass on wrong information to the public, Ministries, Social media influencers, politicians, banks and individuals of high social profile have had their accounts impersonated for several reasons.*** It's common to see companies/orgganizations disclaiming social media posts made by impersonators.

3.4 bn spam emails sent everyday

According to AAG, "Around 3.4 billion spam emails are sent every day" and this shows us that email remains the number one attack vector.

In 2022 alone, over 48% of emails sent were spam.

An email address is a unique identifier and hackers know that information through and email carries authenticity and credibility.

What's the punishment for Impersonation in Uganda?

The Uganda Computer Misuse Act 2011 Section 2 defines Electronic Fraud as ***"Deception, deliberately performed with the intention of securing an unfair or unlawful gain where part of a communication is sent through a computer network or any other communication and another part through the action of the victim of the offence or the action is performed through a computer network or both."***

Electronic Fraud criminals are punishable by a hefty fine, ban on using Internet-capable devices or even prison. The act defines the punishment in section 2) (19) (1) which says,

"***A person who carries out electronic fraud commits an offence and is liable on conviction to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both."***

2. How to identify fraudulent and impersonation emails

MAKERERE UNIVERSITY

"A single breach can undo years of brand building." ~ Geraldine Mugumya (NITA-U)

93.5% surge 474 ↑ 245

The Uganda Police Force Annual Crime Report 2024 shows reported cybercrime cases increased from 245 in 2023 to 474 in 2024, representing a 93.5% surge. Financial losses exceeded Shs72bn, with only a small fraction recovered.

MAKERERE UNIVERSITY

SPOT THE DIFFERENCE

CYBER SECURITY STARTS WITH YOU

1
rnicrosoft.com

2
microsoft.com

We are better off safe than sorry!

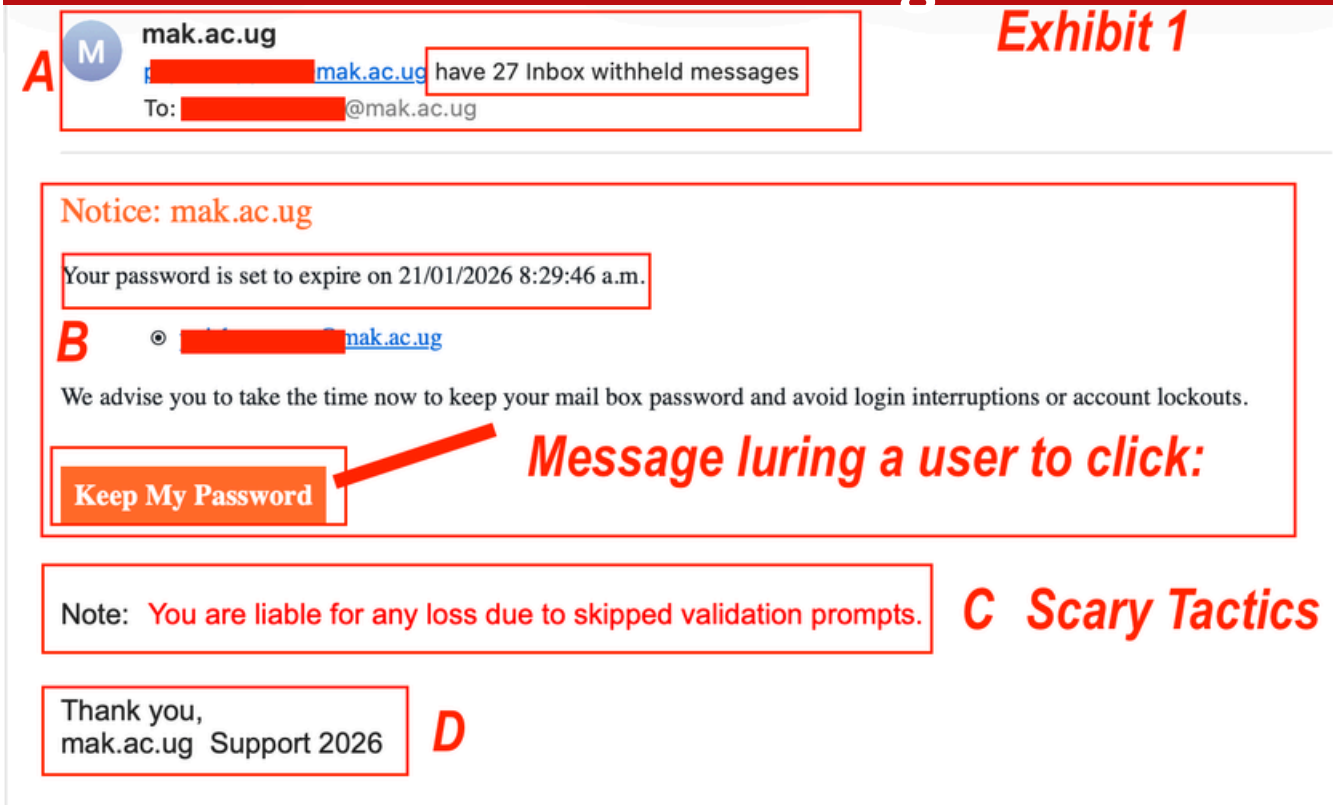
𝕏@DICTSMakerere

2. How to identify fraudulent and impersonation emails

MAKERERE UNIVERSITY

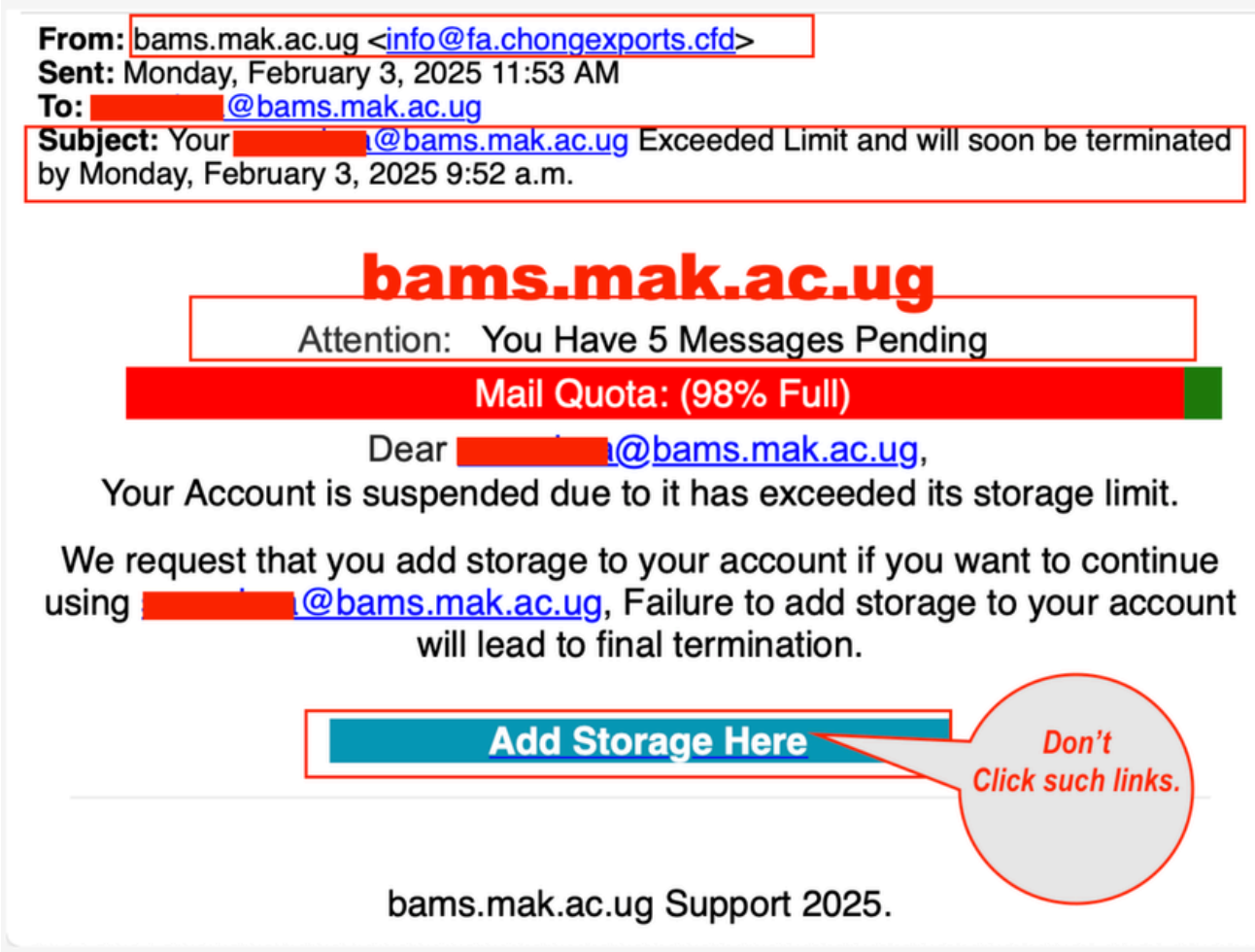
27 Withheld Messages

1



Mail Quota (98% Full)

2



3. How to verify sender identities before acting on any request

MAKERERE UNIVERSITY

Makerere University defines the policies that govern the use of the University's ICT resources. Mentioned among the Unacceptable use of ICT resources is Online Impersonation.

The policy says, "Sending electronic mail that purports to come from an individual other than the person actually sending the message using, for example, a forged address" is Unacceptable.

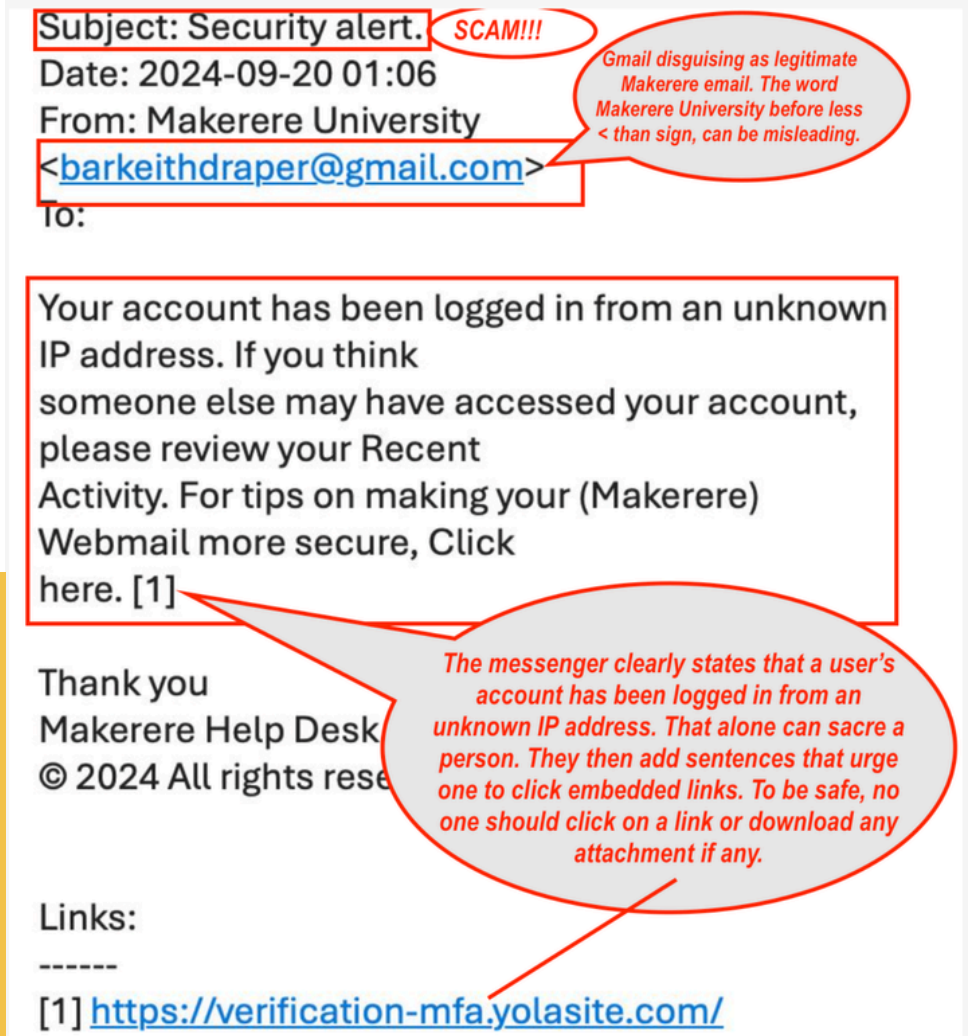
1 Wrong Email Header

Always look at the **<From>** Section:

In this case, the email seems to say, it is from **bams.mak.ac.ug** which is a makerere domain but the **angle brackets <>** show a different email **info@fa.chongexports.cfd** which is being disguised or covered up with the mak domain. This can apply to any other email. So it's important to verify.

2

This is another example: The From part shows: **Makerere University** but the angle brackets <> shows **barkeithdraper@gmail.com**



Always pay attention as well to the body message and signature part. There is a lot of urgency, scary messages embedded with links to click.

4. How to report suspicious communication through the right channels

MAKERERE UNIVERSITY

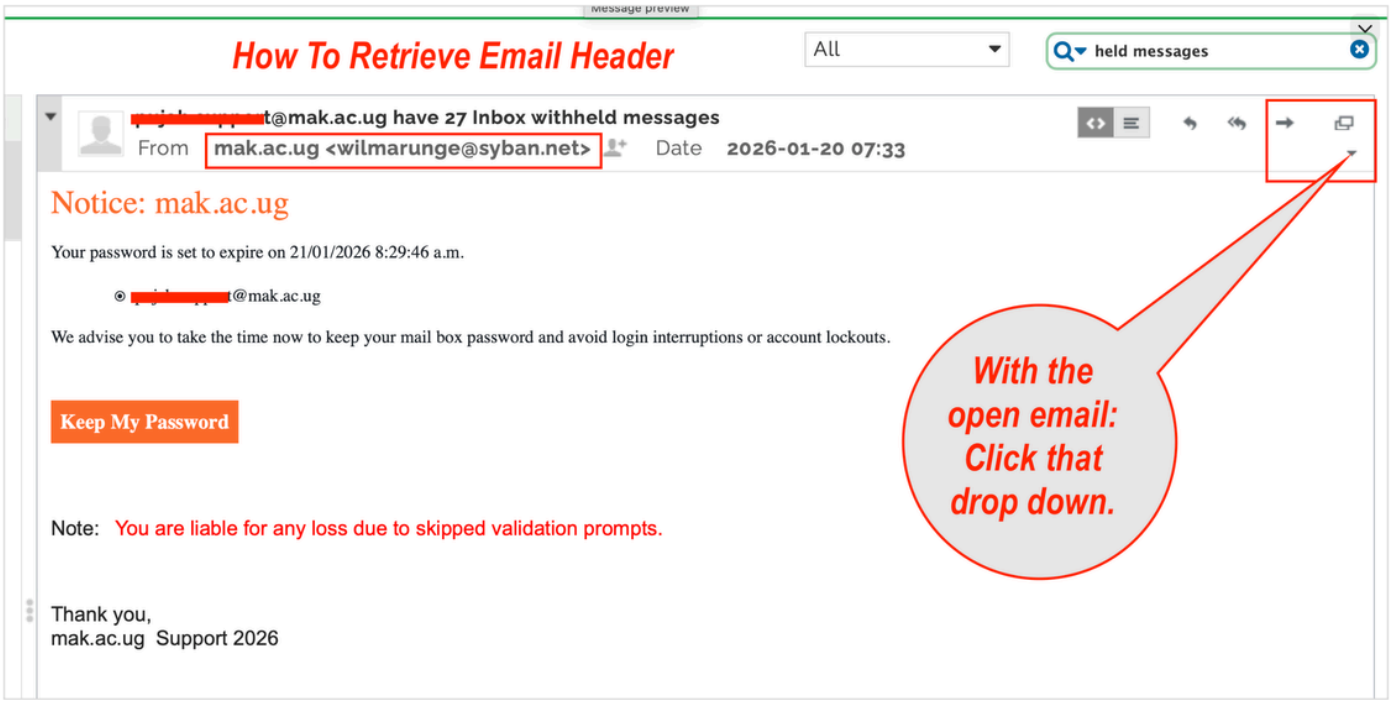
To report any incident:

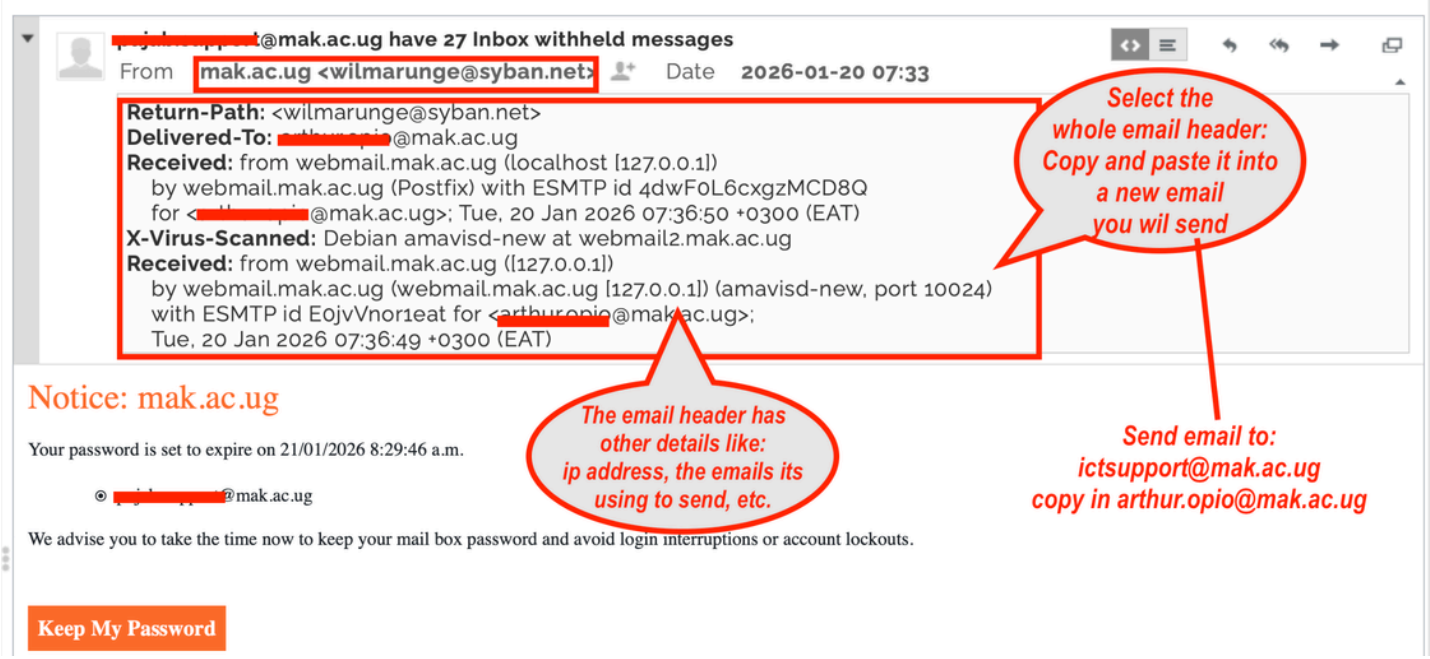
- Always log a ticket via **https://support.mak.ac.ug** or
- Send an email to **ictsupport@mak.ac.ug** and cc: **arthur.opio@mak.ac.ug, stephen.mpirirwe@mak.ac.ug**

Details to send with the report:

Step 1: Log into **https://webmail.mak.ac.ug**

Step 2: Retrieve the email header





5. How to protect your personal and institutional information online

MAKERERE UNIVERSITY

1. **Be Wary of Impersonation Scams:** *Always scrutinize URLs, email addresses, and social media handles before engaging. If in doubt, directly contact the institution via their official website or office contact numbers. In our case, for support challenges support.mak.ac.ug or ictsupport@mak.ac.ug*

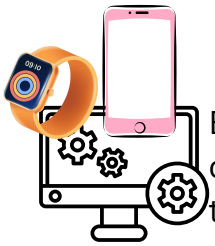
2. **Stay Alert for Phishing Attacks:** *Never click on a link in an email or message that seems suspicious. Instead, go directly to the website by typing its URL into your browser. If the email is asking for personal information or payment, verify the source first.*

3. **Strong Passwords = Strong Protection:** *Use a combination of letters, numbers, and special characters in your passwords. Always enable 2FA wherever possible for added protection.*

4. **Monitor Your Financial Transactions:** *Set a routine to review your bank statements, or activate alerts for every transaction. If you spot anything unfamiliar, contact your bank immediately.*

5. ***Beware of Fake Apps*** *Only download apps from official app stores like Google Play or the Apple App Store. Always check the reviews and ratings before installing any app.*

6. ***Trust Your Gut: Recognize Email Scams*** *Never open attachments or click on links from unknown senders. Always verify the email's authenticity by contacting the sender directly if you're unsure.*



7. ***Keep Your Devices Up to Date*** Enable automatic updates for your operating system, apps, and browsers to ensure you're always using the latest, most secure versions.

At Makerere University, we are committed to creating a secure digital environment for both staff and students. However, the first line of defense starts with you. By staying informed and implementing these cybersecurity practices, you can significantly reduce the risk of falling victim to online fraud. Remember, online safety is a shared responsibility, and your vigilance can help protect not only yourself but the entire university community.

Stay Safe, Stay Secure!

Cyber SecurityToolkit V1

MAKERERE UNIVERSITY

MAKERERE UNIVERSITY

Acquaint yourself with Cyber knowledge on your finger tips:

CYBER SECURITY TOOLKIT V1

Scan QR Code or visit link

http://bit.ly/3Kl1O6L

@DICTSMakerere

https://support.mak.ac.ug
https://answers.mak.ac.ug
https://dicts.mak.ac.ug