

# Social Media: Threats, risks

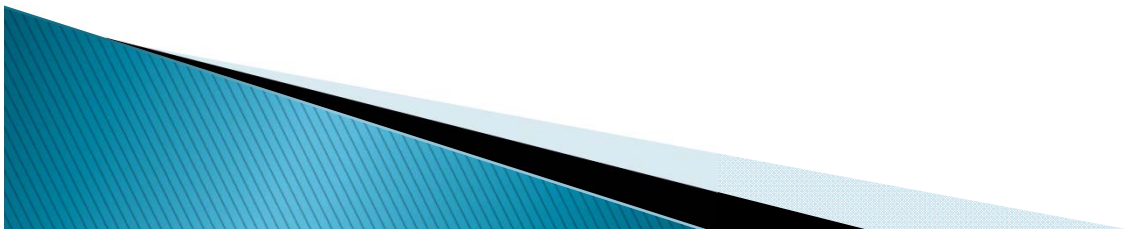


A presentation by  
Haguma Jimmy – Cyber Crime Officer

# Focus Areas



- ▶ Social media as an enabler of cybercrime– The threats and risks (Cyber bullying, cyber staking, social engineering, phishing)
- ▶ Cyber crime incidents in Ugandan cyber space
- ▶ Best practices for mitigating cyber enabled crime.
- ▶ What should social media users know and do?



# Agenda



**#1: Social media defined**

**#2: SM digital security terms**

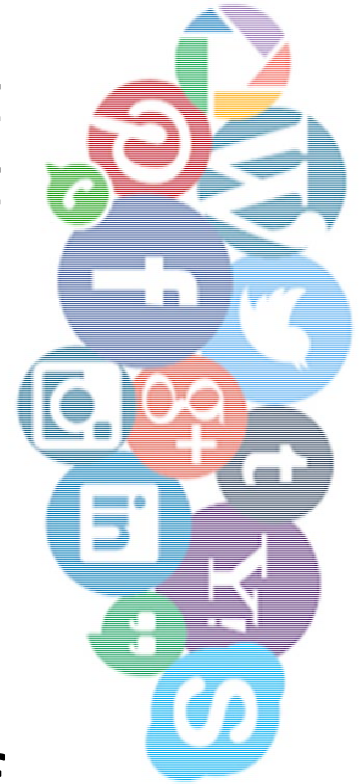




# #1: Social media defined

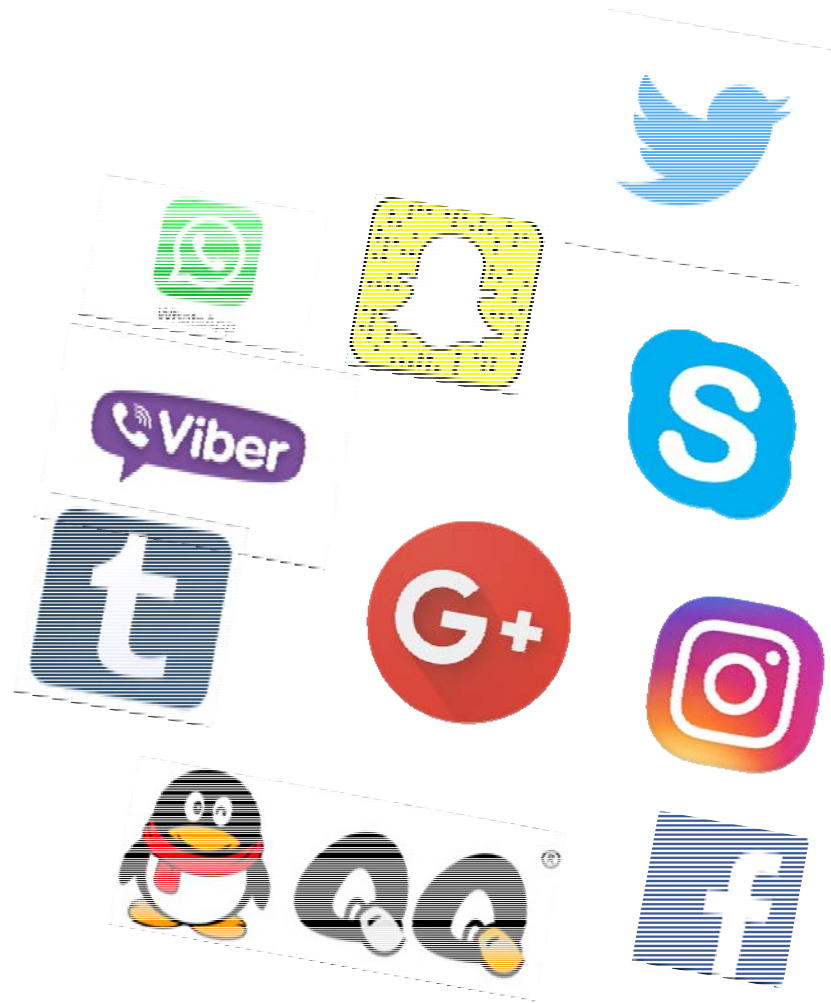
# Social Media (SM) defined

- ▶ It refers to websites and applications that enable users to create and share content or to participate in social networking online Communities.
- ▶ Social media is a set of online technologies, sites and practices which are used to share opinions, experiences and perspectives
- ▶ Social media isn't simply a collection of platforms driven by data. It's a global community powered by people



# Common SM apps

- ▶ Facebook.
- ▶ WhatsApp
- ▶ Tencent QQ
- ▶ WeChat
- ▶ QZone
- ▶ Tumblr
- ▶ Instagram
- ▶ Twitter
- ▶ Google+
- ▶ Skype
- ▶ Snapchat



# Social Media latest trends



- ▶ According to the Digital 2020 reports published in partnership with Hootsuite, social media have become an indispensable part of everyday life for people all over the world.
- ▶ More than 4.5 billion people now use the internet, while social media users have passed the 3.8 billion mark.
- ▶ Nearly 60 percent of the world's population is already online, and the latest trends suggest that more than half of the world's total population will use social media by the middle of this year.



# Digital report Jan 2020

**JAN  
2020**

## **DIGITAL AROUND THE WORLD IN 2020**

THE ESSENTIAL HEADLINE DATA YOU NEED TO UNDERSTAND MOBILE, INTERNET, AND SOCIAL MEDIA USE

TOTAL  
POPULATION



**7.75  
BILLION**

URBANISATION:

**55%**

UNIQUE MOBILE  
PHONE USERS



**5.19  
BILLION**

PENETRATION:

**67%**

INTERNET  
USERS



**4.54  
BILLION**

PENETRATION:

**59%**

ACTIVE SOCIAL  
MEDIA USERS



**3.80  
BILLION**

PENETRATION:

**49%**



we  
are  
social



KEPIOS

# Digital report Jan 2020

**JAN  
2020**

## **SOCIAL MEDIA USE AROUND THE WORLD**

BASED ON THE NUMBER OF MONTHLY ACTIVE USERS OF TOP SOCIAL MEDIA PLATFORMS IN EACH COUNTRY OR TERRITORY

TOTAL NUMBER OF  
ACTIVE SOCIAL  
MEDIA USERS



we  
are  
social

**3.80  
BILLION**

SOCIAL MEDIA  
PENETRATION (USERS  
vs. TOTAL POPULATION \*)



we  
are  
social

**49%**

ANNUAL GROWTH IN  
THE TOTAL NUMBER OF  
SOCIAL MEDIA USERS



KEPIOS

**+9.2%**

TOTAL NUMBER OF SOCIAL  
MEDIA USERS ACCESSING  
VIA MOBILE PHONES



global  
web  
index

**3.75  
BILLION**

PERCENTAGE OF TOTAL  
SOCIAL MEDIA USERS  
ACCESSING VIA MOBILE



**99%**

# Digital report Jan 2020

**JAN  
2020**

## FACEBOOK ACCESS BY DEVICE

THE DEVICES THAT FACEBOOK USERS USE TO ACCESS THE PLATFORM

PERCENTAGE OF FACEBOOK  
USERS ACCESSING VIA ANY  
KIND OF MOBILE PHONE



**98%**



PERCENTAGE OF FACEBOOK  
USERS WHO ONLY ACCESS VIA A  
LAPTOP OR DESKTOP COMPUTER



**1.9%**



PERCENTAGE OF FACEBOOK  
USERS WHO ACCESS VIA BOTH  
PHONES AND COMPUTERS



**19%**

we  
are  
social

PERCENTAGE OF FACEBOOK  
USERS WHO ONLY ACCESS  
VIA A MOBILE PHONE



**79%**

# **#2: SM digital security terms**



# SM digital security terms

- ▶ Encryption
- ▶ Authentication
- ▶ Virus/Worms
- ▶ Back doors
- ▶ Honey pot
- ▶ *Phishing/Vishing*
- ▶ Eavesdropping
- ▶ *Pharming*
- ▶ *Ransomware*



# Key terms of digital security

- ▶ Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft.
- ▶ Pharming is a cyber attack intended to redirect a website's traffic to another, fake site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software.



# Key terms of digital security

- ▶ Ransomware, also known as scareware, is malicious software that restricts access to an infected computer while displaying a notification making demands for the computer user to pay a fee to restore access to the infected system.
- ▶ The extortion price varies, ranging from USD\$20 to more than USD\$600, but may be much higher.



# THANK YOU

## Q & A

