RENU

Introduction to **Cybersecurity**

21st May, 2025

Samuel Wekobosya

swekobosya@renu.ac.ug

Knowledge | Community | Solutions

Cybersecurity

Outline

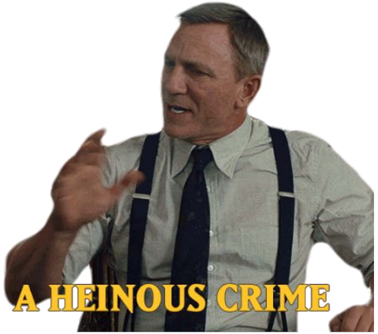
- Cyber Crimes
- Cybersecurity Principles
- Vulnerabilities
- Staying safe

Cyber Crime

Cyber crimes are, as the name implies, crimes committed using computers, phones or the internet.

Some types of cyber crime include:

- Illegal interception of data.
- System interferences.
- Copyrights infringements
- Sale of illegal items



Security is a process, not a product.

Bruce Schneier

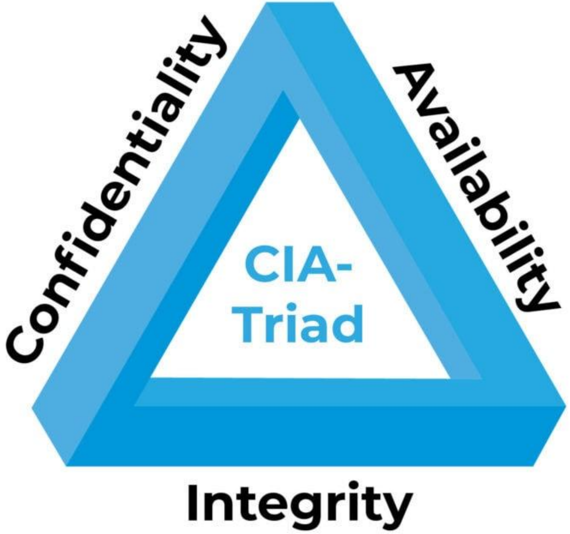
Cyber Security

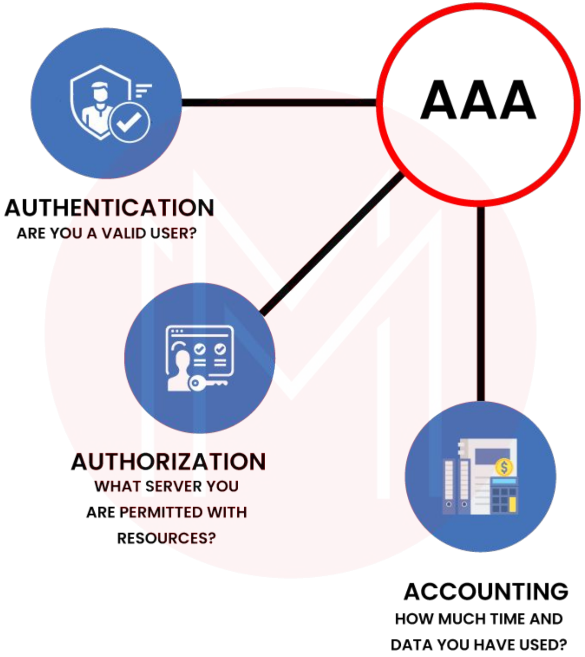
- Cyber security refers to technologies, processes and practices involved in protecting individuals and organisations from cyber crime.

- It is designed to protect integrity of networks, computers, programs and data from attack, damage or unauthorised access.

Cyber Security Principles

There are six key principles in cyber security





Cybersecurity Principles

Confidentiality

A set of rules that limit access or place restrictions on certain type of information

Availability

The guarantee of reliable access to the information by authorized people

Integrity

Assurance that the information is trustworthy and accurate

Cybersecurity Principles

Authorisation

Process of determining what an authenticated user is allowed to do.

Authentication

Process of verifying the identity of a user, system or device before access to resources

Accountability

Process of recording and tracking user activities on a system

Cyber Threat

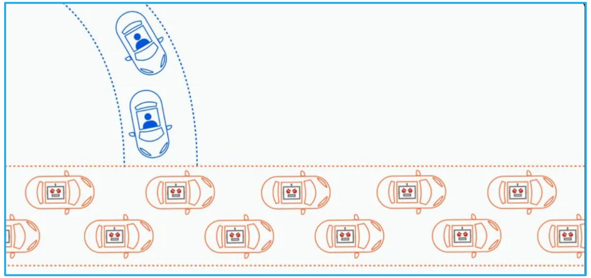
- A cyber threat is any malicious act that attempts to gain access to a computer network without authorisation or permission from the owners.

- It refers to the wide range of malicious activities that can damage or disrupt a computer system, a network or the information it contain.

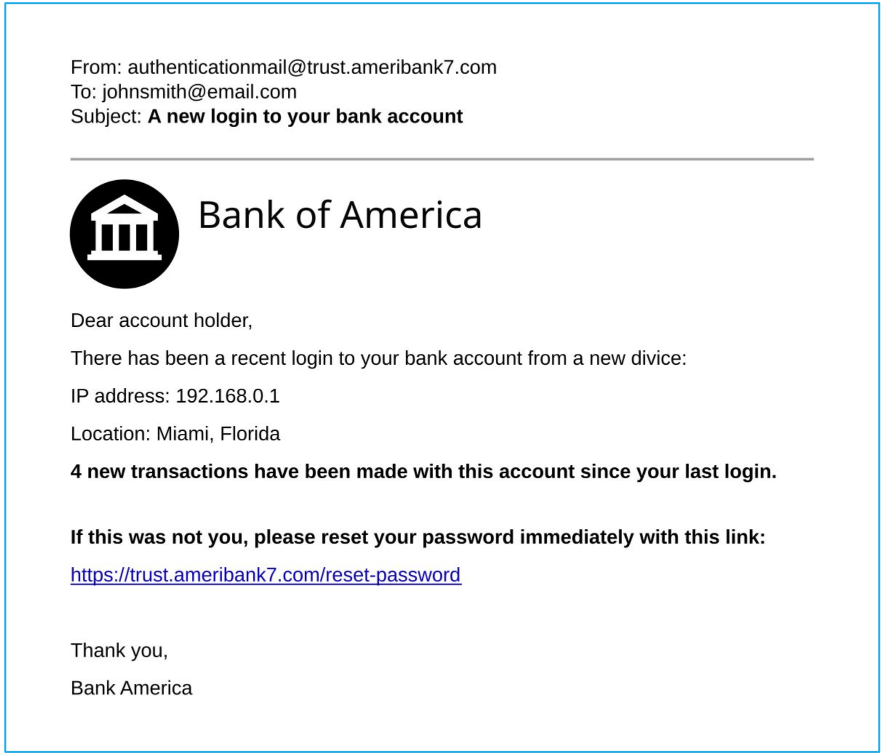
- Most common cyber threats: social engineered trojans, unpatched software, phishing, network worms etc.

Cyber Threats

Malware



Denial of Service



From: authenticationmail@trust.ameribank7.com
To: johnsmith@email.com
Subject: **A new login to your bank account**

Bank of America

Dear account holder,

There has been a recent login to your bank account from a new divice:

IP address: 192.168.0.1

Location: Miami, Florida

4 new transactions have been made with this account since your last login.

If this was not you, please reset your password immediately with this link:

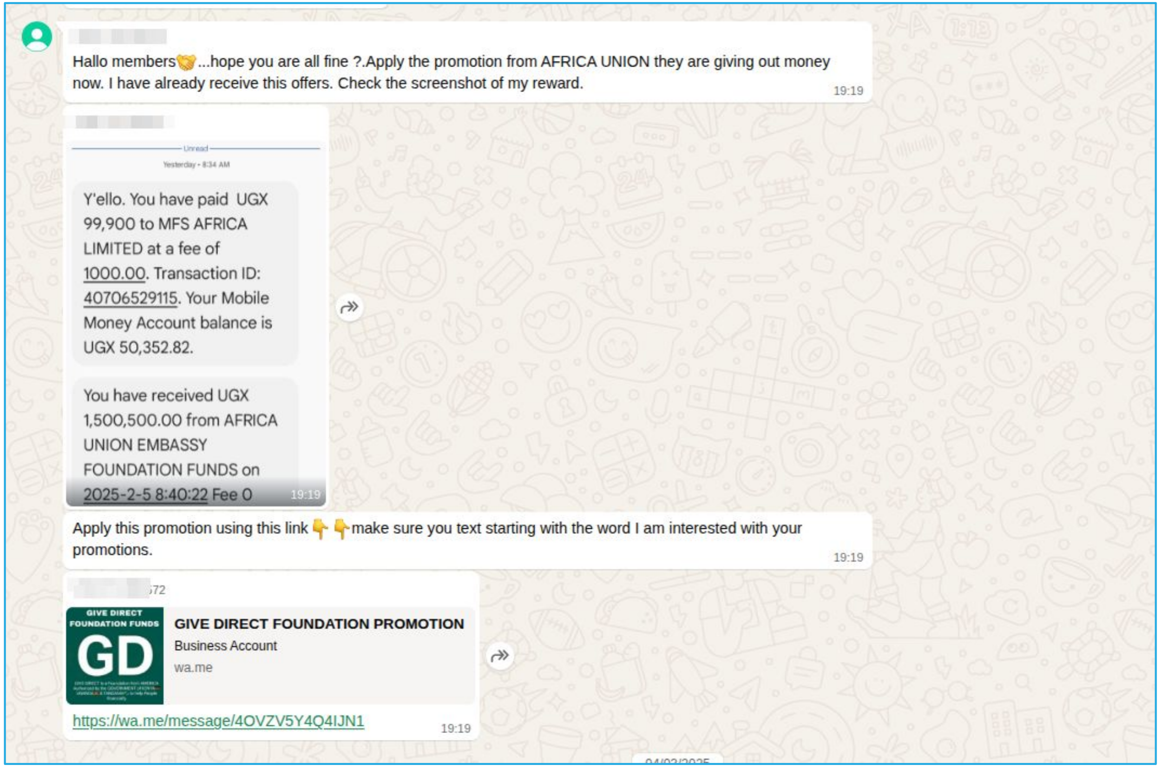
https://trust.ameribank7.com/reset-password

Thank you,

Bank America

Phishing

Cyber Threats



[redacted]

Hallo members🤝...hope you are all fine ?.Apply the promotion from AFRICA UNION they are giving out money now. I have already receive this offers. Check the screenshot of my reward. 19:19

[redacted]

Unread

Yesterday • 8:34 AM

Y'ello. You have paid UGX 99,900 to MFS AFRICA LIMITED at a fee of 1000.00. Transaction ID: 40706529115. Your Mobile Money Account balance is UGX 50,352.82.

You have received UGX 1,500,500.00 from AFRICA UNION EMBASSY FOUNDATION FUNDS on 2025-2-5 8:40:22 Fee 0

19:19

Apply this promotion using this link 👇 👇make sure you text starting with the word I am interested with your promotions. 19:19

[redacted]

GIVE DIRECT FOUNDATION PROMOTION

Business Account

wa.me

https://wa.me/message/4OVZV5Y4Q4IJN1 19:19

What threat is this?

Sources of Cyber Threats

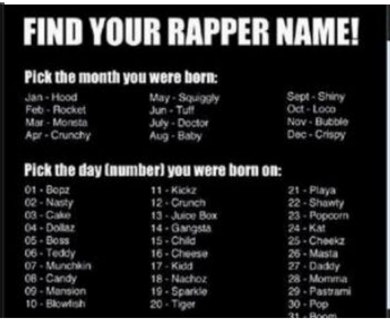
Cyber threats can come from a wide variety of sources, some notable examples include:

- National governments
- Terrorists
- Industrial secret agents
- Rogue employees
- Hackers
- Business competitors
- Organization insiders

Cyber Threat Classifications

How people think they get hacked:

What really happens!!



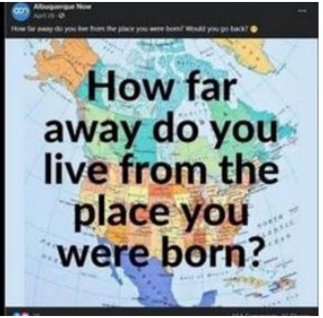
FIND YOUR RAPPER NAME!

Pick the month you were born:

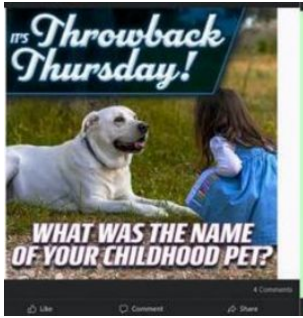
Jan - Hood
Feb - Rocket
Mar - Monsta
Apr - Crunchy
May - Squiggly
Jun - Tuff
July - Doctor
Aug - Baby
Sept - Shiny
Oct - Loco
Nov - Bubble
Dec - Crispy

Pick the day (number) you were born on:

01 - Bopz
02 - Nasty
03 - Cake
04 - Dollaz
05 - Boss
06 - Teddy
07 - Munchkin
08 - Candy
09 - Mansion
10 - Blowfish
11 - Kickz
12 - Crunch
13 - Juice Box
14 - Gangsta
15 - Child
16 - Cheese
17 - Kidd
18 - Nachoz
19 - Sparkle
20 - Tiger
21 - Playa
22 - Shawty
23 - Popcorn
24 - Kat
25 - Cheekz
26 - Masta
27 - Daddy
28 - Momma
29 - Pastrami
30 - Pop
31 - Boom

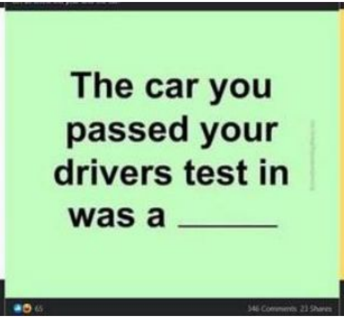


How far away do you live from the place you were born?

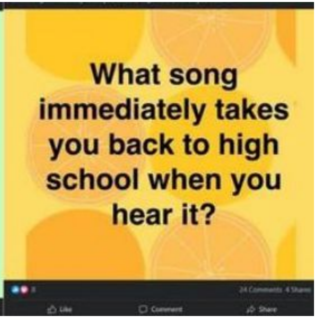


It's Throwback Thursday!

WHAT WAS THE NAME OF YOUR CHILDHOOD PET?



The car you passed your drivers test in was a ______



What song immediately takes you back to high school when you hear it?

Cyber Threats Classifications

Unstructured

Resources: Individual or small group

Organization: Little to no

Funding: Negligible

Attack: Easy to detect and make use of freely available cyber attack tool.

Exploitation based on documented vulnerabilities.

Structured

Resources: Well trained individual or group

Organization: Well planned

Funding: Available

Attack: Against particular individual or organisation

Exploitation based on information gathering.

Highly structured

Resources: Extensive resources

Organization: Extensive

Funding: Negligible

Attack: Long term attack on a particular machine

Exploitation with multiple methods: technical, social and insider help

Motives, Goals and Objectives of Cyber Attacks

- Disrupt business continuity
- Perform information theft
- Manipulating data
- Create fear and chaos by disrupting critical infrastructures.
- Bring financial loss to the target
- Propage religious or political beliefs.
- Achieve a state's military objectives
- Demand Ransom

Attacks = Motive (Goal)+Method+Vulnerability

Types of Cyber Attacks

Advanced Persistent Threat (APT):
A network attack in which an unauthorised person gains access to network and stays there undetected for a long period of time.

Backdoor:
Method of bypassing normal authentication and gaining access in OS or application.

Types of Cyber Attacks

Buffer Overflow:

An exploit that takes advantage of the program that is waiting for a user's input.

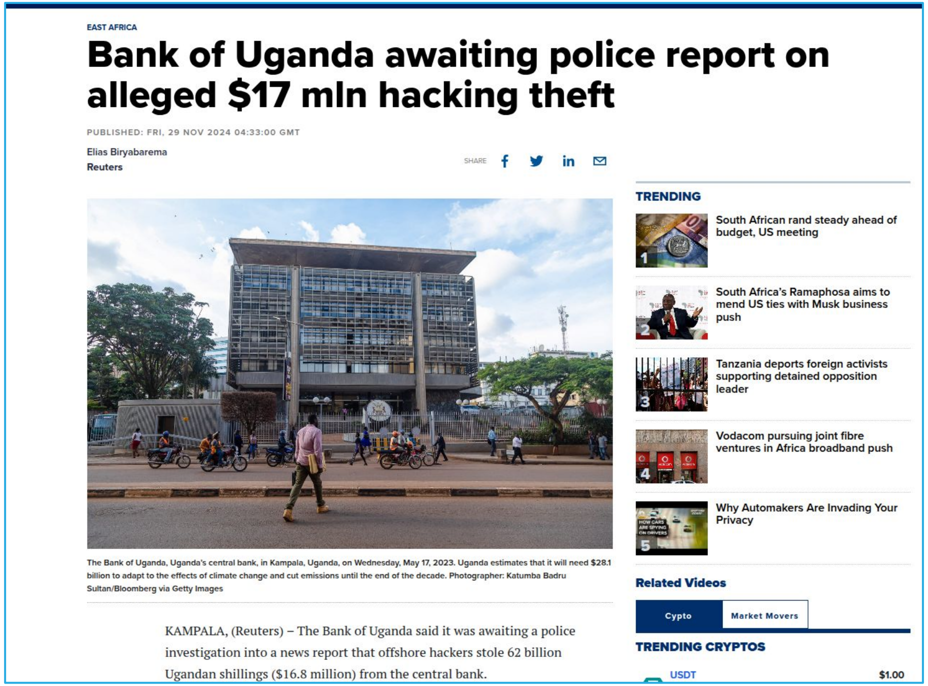
Man-in-the-middle Attack:

This attack intercepts and relays messages between two parties who are communication directly with each other.

Denial of Service Attack:

An attack where the attackers attempt to prevent the authorised users from accessing the service.

What happened at the Bank of Uganda



EAST AFRICA

Bank of Uganda awaiting police report on alleged $17 mln hacking theft

PUBLISHED: FRI, 29 NOV 2024 04:33:00 GMT

Elias Biryabarema
Reuters

SHARE

The Bank of Uganda, Uganda's central bank, in Kampala, Uganda, on Wednesday, May 17, 2023. Uganda estimates that it will need $28.1 billion to adapt to the effects of climate change and cut emissions until the end of the decade. Photographer: Katumba Badru Sultan/Bloomberg via Getty Images

KAMPALA, (Reuters) – The Bank of Uganda said it was awaiting a police investigation into a news report that offshore hackers stole 62 billion Ugandan shillings ($16.8 million) from the central bank.

TRENDING

1 South African rand steady ahead of budget, US meeting

2 South Africa's Ramaphosa aims to mend US ties with Musk business push

3 Tanzania deports foreign activists supporting detained opposition leader

4 Vodacom pursuing joint fibre ventures in Africa broadband push

5 Why Automakers Are Invading Your Privacy

Related Videos

Cypto | Market Movers

TRENDING CRYPTOS

USDT	$1.00

Knowledge | Community | Solutions

Impacts of Cyber Attacks

A successful cyber attack can cause major damage to organisations or systems, as well as to business reputation and consumer trust.

Some potential results include:

- Financial loss.
- Reputational damage.
- Legal consequences.

Common Types of Malicious Code

Virus:
Malicious software program, when it is executed, it replicates itself by modifying other computer programs and inserting its own code.

Network worm:
Standalone malware which replicates itself in order to spread to other computers.

Trojan Horse:
A program that claims to free your computer from viruses but instead introduces viruses onto your system.

Vulnerability

A cyber security term that refers to a flaw in a system that can leave it open to attack.

Vulnerability is the composition of three elements:

- A flaw in system
- Access of attacker to that flaw.
- Capability of attacker to exploit the flaw

Classification of Vulnerabilities

Vulnerabilities are classified according to the asset:

- Hardware.
- Software.
- Network.
- Personal.
- Physical site.
- Organizational.

Vulnerabilities Continued

Some of the vulnerability in the system occur due to:

- Missing patches.
- Cleartext credentials.
- Using unencrypted channels.
- RF Emanation.

Simple Steps to Stay Secure

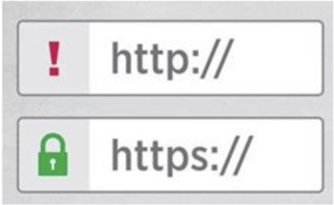
- Creating strong passwords
- Using multi-factor authentication (MFA)
- Software updates & patch management
- Recognizing phishing attempts
- Safe browsing habits:visit secure sites,avoid clicking suspicious ads or pop-ups.

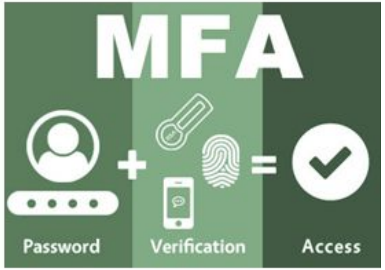
Simple Steps to Stay Secure

LastPass•••|

bitwarden

KeePassXC



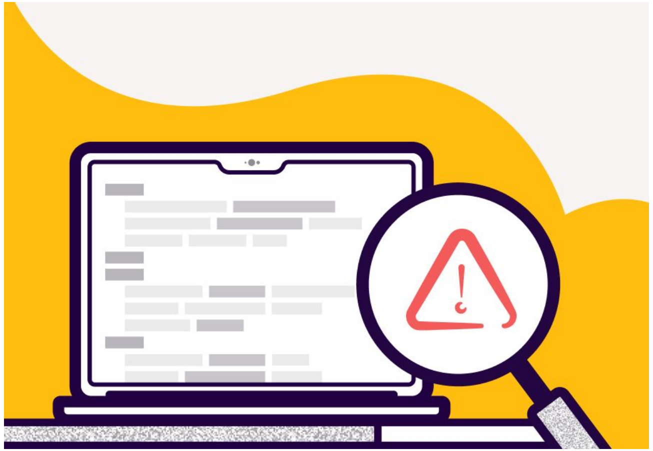


Cybersecurity at RENU

Pentesting

eduVPN

Vulnerability Scans



THE END

Discussion