SOCIAL ENGINEERING
WHAT YOU NEED TO KNOW.

Presented by
Haguma Jimmy
Cyber Crime Officer

Agenda

#1: Introduction

#2: Social Engineering techniques

#3: SE threat and attacks_UG cyber space

#4: Government Legal & Regulatory Environment

#5: SE best practices

#6: Way forward

Click Safe

#1: Introduction

INTRODUCTION

- It encompasses a **broad spectrum of malicious** activity.
- The old fashioned technical way of breaking into the computer systems by brute forcing the user logins or ports have now been replaced by sophisticated methods that not only are easier, but yield better and faster results based on human psychology.

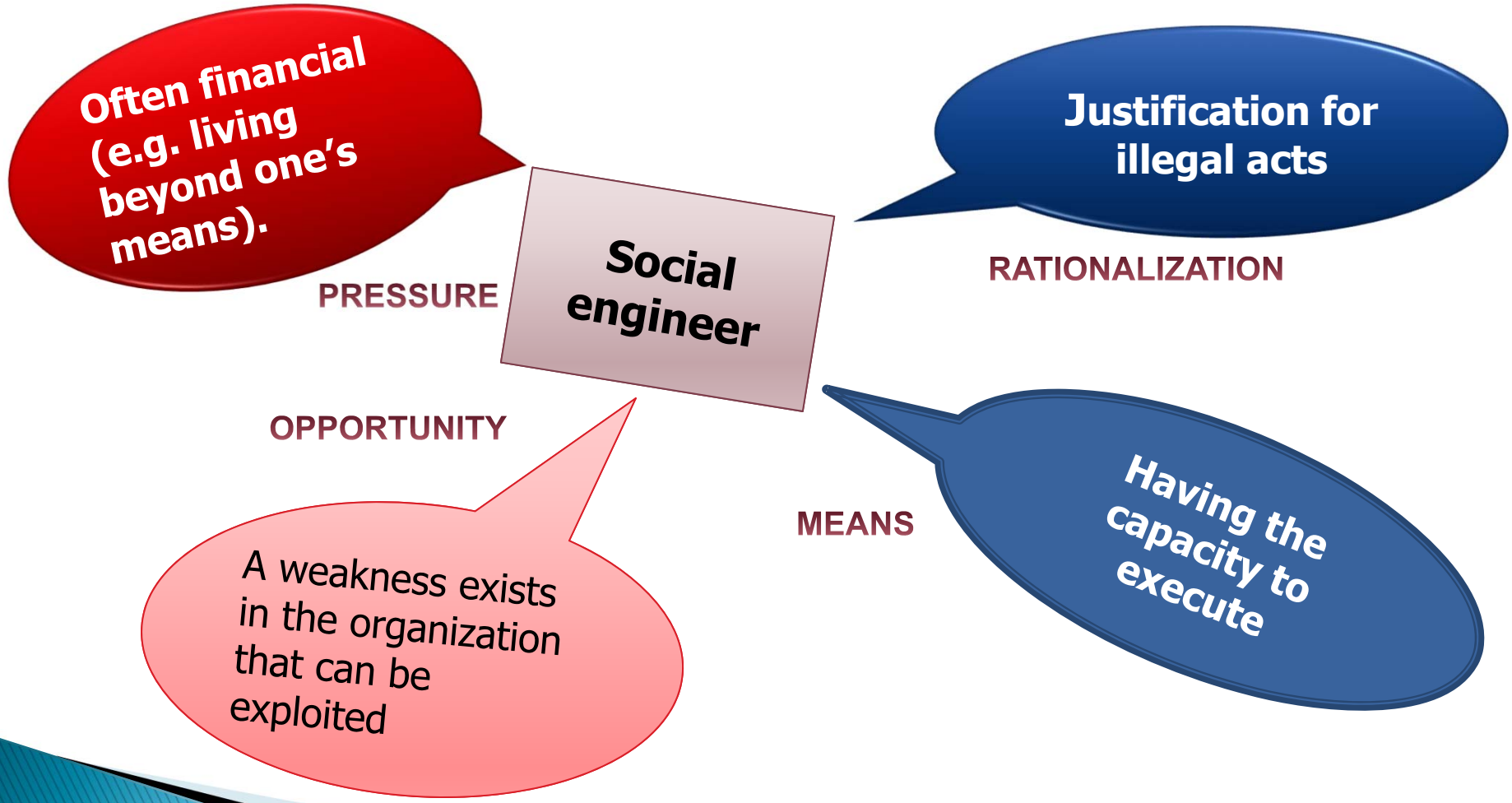
- These attacks can help the attacker get access to any system irrespective of the platform, software or hardware involved.

SOCIAL ENGINEERING (SE) DEFINED

- Social Engineering is a non-technical kind of intrusion relying heavily on human interaction which often involves tricking other people into breaking normal security procedures the attacker uses social skills and human interaction to obtain information about an organization or their computer systems

- The art of manipulating people into performing actions or divulging confidential information

CRITICAL INGREDIENTS



#2: Social Engineering techniques

The Social Engineering Life Cycle

Developing a relationship with the target who is usually an employee or someone working in the business

Social engineer manipulates the trust that he has gained in the previous phase so as to extract as much confidential information as possible

Foot printing → Establishing Trust → Psycholological Manipulation → Exit

Technique of accumulating information regarding the target(s) and the surrounding environment. E.g. list of names and emails

Terminate link once mission is achieved

SOCIAL ENGINEERING TECHNIQUES

SHOULDER SURFING

DUMPSTER DIVING

SOCIAL ENGINEERING TECHNIQUES

ROLE PLAYING

TROJAN HORSE

PHISHING

SURFYING ONLINE CONTENT

SOCIAL ENGINEERING TECHNIQUES

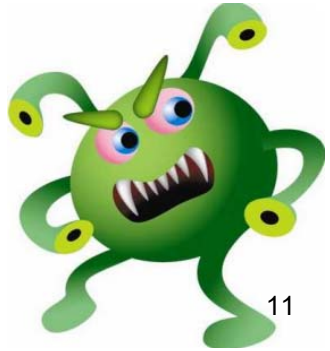
- **Shoulder Surfing** is a security attack where in, the attacker uses observation all techniques, such as looking over someone's shoulder, to get information while they are performing some action

- **Dumpster diving** _attacker can use retrieved infromation from dumped items like company phone books, system manuals, organizational charts, company policy manuals, calendars of meetings, printouts of sensitive data or login names and passwords, printouts of source code, disks and tapes, company letterhead and memo forms.

SOCIAL ENGINEERING TECHNIQUES

- **Role playing** involves persuading or gathering information through the use of an online chat session, emails ,phone or any other method that your company uses to interact online with the public pretending to be a helpdesk, employee, technician.

- **Trojan horse** involves tricking the victims to download a malicious file to the system which on execution creates a backdoor in the machine that can be used by the attacker any time in the future



SOCIAL ENGINEERING TECHNIQUES

- **Phishing** creating and using web sites and emails designed to look like those of well known legitimate businesses, financial institutions and government agencies to *deceive* Internet users into disclosing their personal information and falsely claiming to be an established legitimate enterprise in an attempt to scam the user

NOTE

- **Vishing** involves making phone calls

SOCIAL ENGINEERING TECHNIQUES

- Surfing Organization Websites & Online forums _ This is related to google hacking techniques.
- Huge amount of information regarding the organization structure, email ids, phone numbers are available openly on the company website and other forums. This information can be used by the attacker to refine his approach and create a plan on whom to target

#3: SE Threats & Attacks _Ugandan cyber space

SE threats and attacks

- Internet frauds – identity thefts, password harvesting, foot-printing, social engineering.
- Financial frauds – Salami techniques (Banks), Payment cards frauds, eTax payment frauds, insurance schemes

SE threats and attacks

- Telecom frauds – mobile money, SIM card swapping, unsolicited SMS or voice calls, VIOP interceptions
- Utility frauds – water, electricity bill payments
- Domain Hosting frauds – website cloning and hacking i.e. *pharming*
- **Ransomware**

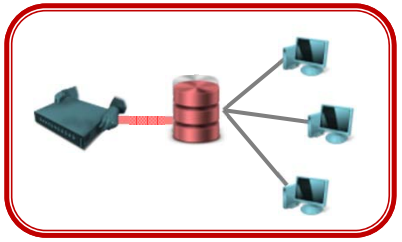
THREAT ACTORS

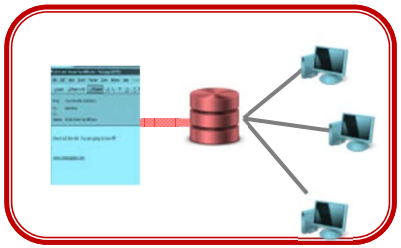
HACKTIVISTS

CRIMINAL ELEMENTS

THREAT VECTORS

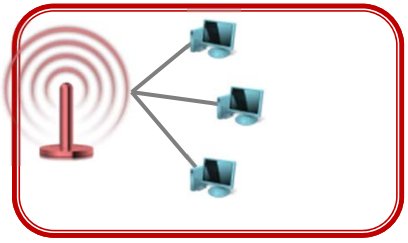
SUPPLY CHAIN VULNERABILITY

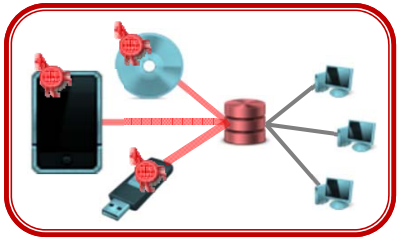




INSIDER THREAT

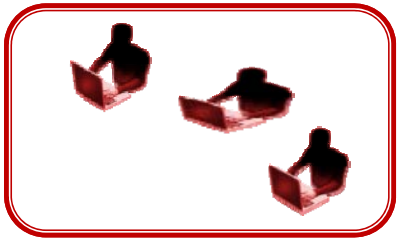
SECURITY MISCONFIGURATION





REMOVABLE MEDIA

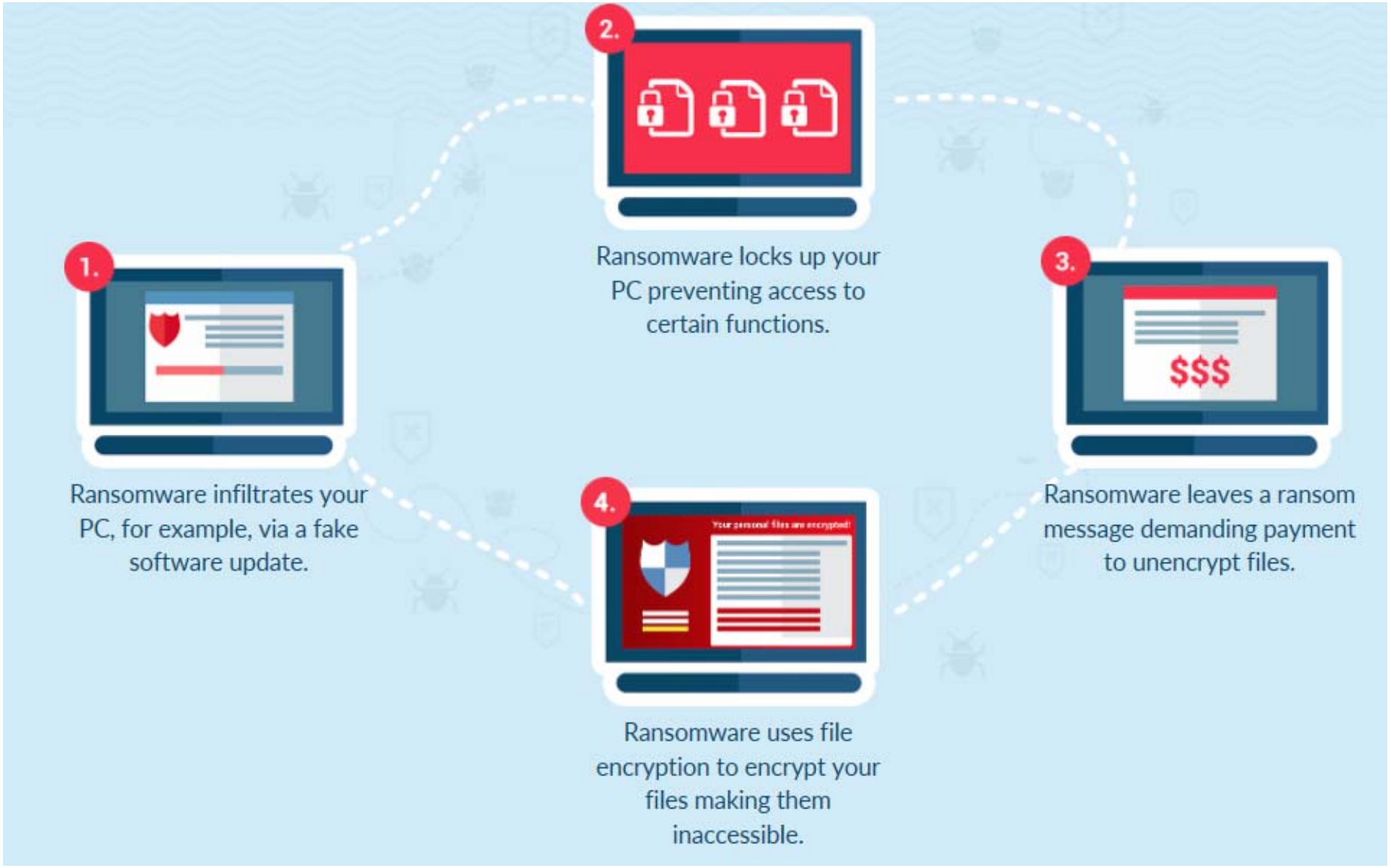
GOVERNANCE



Ransomware escalation process

- Infiltrates PC via vulnerabilities either spam mail, unpatched software, etc.
- Locks PC preventing access to certain functions literally session hijacking or DoS attacks
- It leaves a message demanding payment to un encrypt files

RANSOMWARE LIFE CYCLE



Sample case highlights

- On 13th November 2019, Steve applied for *online job scams* following advert on social media from 'Java House'. He was to earn "$425 per month plus other allowances including travel, overtime, medical and house. A few days later, another email came telling him he had to attend a hotel workers' training and was required to send $55 (Shs 198,000) to a provided bank account, a mobile money number or through Western Union

Sample case highlights cont'd

- Another rather disheartening yet very true main stream social media crime is one that was tagged as *Raped on Facebook*. On April 11, 2013 at about 3:00pm, in the underground parking yard of Oasis Mall, Turigye allegedly raped a girl who he had seen for the first time. Turigye hacked into another girl's Facebook account and "stole" it.

Sample case highlights

- On November 8, 2017, Police and Ugandan Communications Commission arrested five imposters who were posing as agents of Kampala Serena hotel. These fraudsters *hacked into their victims' Facebook accounts* and sent messages to friends and relatives asking for money
- People have fallen for dubious online investment clubs on the promise of daily profits ranging between 7 -10 percent of the money deposited. Pyramid and Ponzi schemes

Sample case highlights

- Telex Free
- Inonfunds.com
- EasyCoin
- Global Finance

- Over shs7 billion injected
- Clients lost Shs 300 million
- 20 people lost Shs 250 million
- Conned people of Shs worth 800 million

#4: Government Legal & Regulatory Environment

Enabling Legal & Regulatory Environment

ICT Legal and Regulatory Framework

- The Electronic Transactions Act, 2011,
- The Electronic Signatures Act, 2011
- The Computer Misuse Act, 2011

Cyber Laws effective 15th April 2011

- **UN Convention (Budapest Convention)**
- NITA-U Act, 2009
- E-Transactions Regulations,2013
- E-Signatures Regulations, 2013
- E-Government Regulations, 2015
- National IT Policy Framework 2003
- National IT Standards
- MDA IT related Standards

#5: Click clever practices

Click clever practices

- **Do not open any emails from untrusted sources.** Be sure to contact a friend or family member in person or via phone if you ever receive an email message that seems unlike them in any way.
- **Do not give offers from strangers the benefit of the doubt.** If they seem too good to be true, they probably are.
- **Lock your laptop/Phone** whenever you are away or not seemingly busy with it.

Click clever practices

- **Purchase anti-virus software.** No AV solution can defend against every threat that seeks to jeopardize users' information, but they can help protect against some.
- **Read your company's privacy policy** to understand under what circumstances you can or should let a stranger into the building.

Click clever practices

Click Safe

- Set **strong passwords**, and don't share them with anyone.
- Keep **your computer updated** with the latest anti-virus and anti-spy ware software, and use a good firewall.
- **Never send your online account details** through an email and think carefully before you give away any personal or financial information.
- **Check the privacy settings** and think about who you really want to have access to your personal information.

Click clever practices

Click Safe

- **Limit the amount of personal information** you post online, and use privacy settings to avoid sharing information widely.
- **Never enter your personal information** on a website if you are not certain it is genuine.
- **Don’t click on the link provided in an email** or **call the phone number provided**; instead, find the business's contact details through a general internet search.

#6: Way forward

WAY FORWARD

- Security Awareness Trainings
- Background Verification as a core recruitment strategy
- Physical security both IDS and IPS (Detection and prevention)
- Limited data leakage through continuous monitoring
- Routine Mock Social Engineering drills
- Data Classification policy. For example shredding of documents, non disclosure levels and privileges.

THANK YOU

Q & A


Cyber Security
is our shared
responsibility...
Always Stop,
Think before you
Connect.