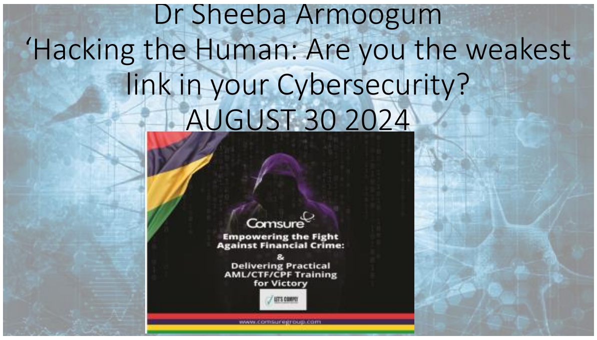


Dr Sheeba Armoogum
‘Hacking the Human: Are you the weakest link in your Cybersecurity?
AUGUST 30 2024

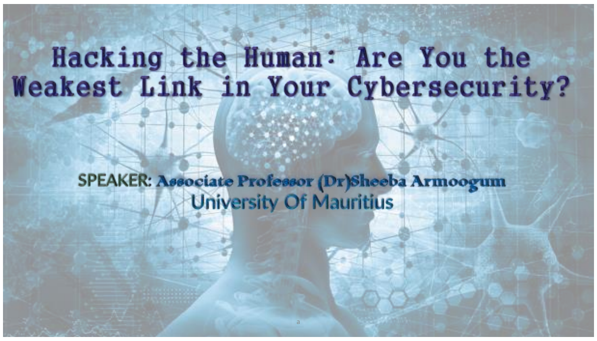
Comsure

Empowering the Fight Against Financial Crime:
&
Delivering Practical AML/CTF/CPF Training for Victory

LET'S COMPLY

www.comsuregroup.com

1



Hacking the Human: Are You the Weakest Link in Your Cybersecurity?

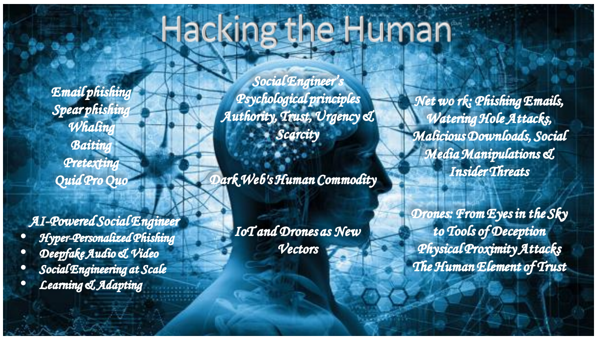
SPEAKER: Associate Professor (Dr)Sheeba Armoogum
University Of Mauritius

2

Who Am I

- ***Associate Professor*** *@ the University of Mauritius*
- ***PhD*** *in Cybersecurity*
- *More than18 years of experience in teaching and research at the university*
- ***Founder*** *of the CyberSecurity & Forensics Research Group (CSFRG) and* ***Head***
- *PhD Supervisor in Cybersecurity & Cyberpsychology and International PhD Examiner*
- ***International Patent Holder*** *in the field of Cybersecurity*
- *Global Women Inventors & Innovators Network (****GlobalWIIN****) Special Recognition Award 2023 and other international awards.*
- *Executive Board Member for the region of Mauritius & African Countries | International Cyber Security & Investigation Committee*
- *Chairperson (Interim) |Southern African Federation of Engineering Organization (SAFEO) Industry Committee on ICT*
- *Research Areas: Cybersecurity, Quantum Cybersecurity, Cyber Forensics / Digital Forensic Investigation*

3



Hacking the Human

Email phishing
Spear phishing
Whaling
Baiting
Pretexting
Quid Pro Quo

Social Engineer's
Psychological principles
Authority, Trust, Urgency &
Scarcity

Net wo rk: Phishing Emails, Watering Hole Attacks, Malicious Downloads, Social Media Manipulations & Insider Threats

Dark Web's Human Commodity

AI-Powered Social Engineer
- Hyper-Personalized Phishing
- Deepfake Audio & Video
- Social Engineering at Scale
- Learning & Adapting

IoT and Drones as New Vectors

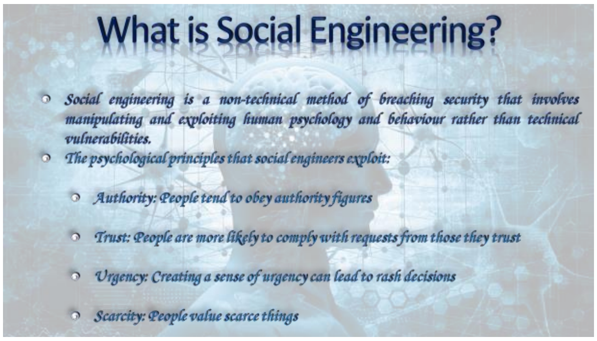
Drones: From Eyes in the Sky to Tools of Deception
Physical Proximity Attacks
The Human Element of Trust

4

Outline

- *Social Engineering*
- *Common Social Engineering Tactics*
- *The AI-Powered Social Engineer - A New Era of Deception?*
- *Your Network - A Playground for Human Hackers*
- *The Dark Web's Human Commodity: Your Information*
- *Human Hacking Takes Flight: IoT and Drones as New Vectors*
- *Why Social Engineering is So Effective*
- *Protecting Yourself and Your Organization*
- *What to Do If You've Been Targeted*
- *Call to Action*

5



What is Social Engineering?

- *Social engineering is a non-technical method of breaching security that involves manipulating and exploiting human psychology and behaviour rather than technical vulnerabilities.*
- *The psychological principles that social engineers exploit:*
  - *Authority: People tend to obey authority figures*
  - *Trust: People are more likely to comply with requests from those they trust*
  - *Urgency: Creating a sense of urgency can lead to rash decisions*
  - *Scarcity: People value scarce things*

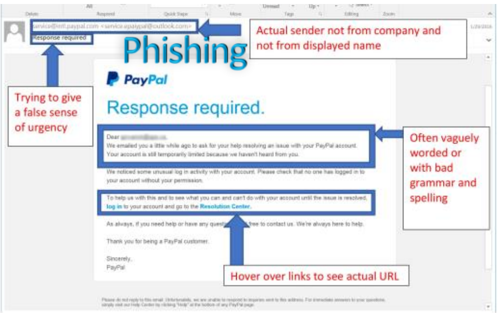
6

Common Social Engineering Tactics

- *Phishing: Types of phishing (email phishing, spear phishing, whaling)*
- *Baiting: Uses the promise of something desirable to lure victims*
- *Pretexting: Attackers create a false sense of identity or a fabricated scenario*
- *Quid Pro Quo: Offering something in exchange for information or access*

7

Phishing



service@intl.paypal.com <service.epaiypal@outlook.com>

Response required

Actual sender not from company and not from displayed name

Trying to give a false sense of urgency

PayPal

Response required.

Dear [redacted]

We emailed you a little while ago to ask for your help resolving an issue with your PayPal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

As always, if you need help or have any questi[...] free to contact us. We're always here to help.

Thank you for being a PayPal customer.

Sincerely,
PayPal

Often vaguely worded or with bad grammar and spelling

Hover over links to see actual URL

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

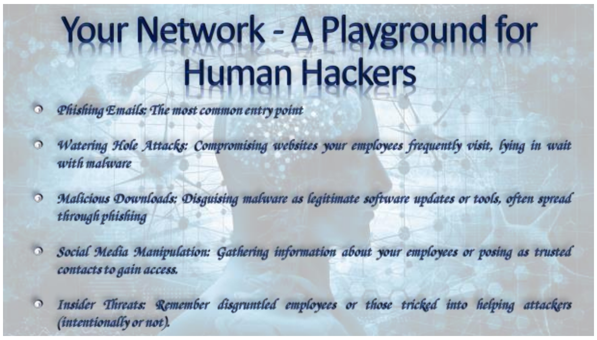
Even if you think the email is legitimate, if it is not something you are expecting it is a good idea to contact the

8

The AI-Powered Social Engineer - A New Era of Deception?

- *Hyper-Personalized Phishing*
- *Deepfake Audio & Video*
- *Social Engineering at Scale*
- *Learning & Adapting*

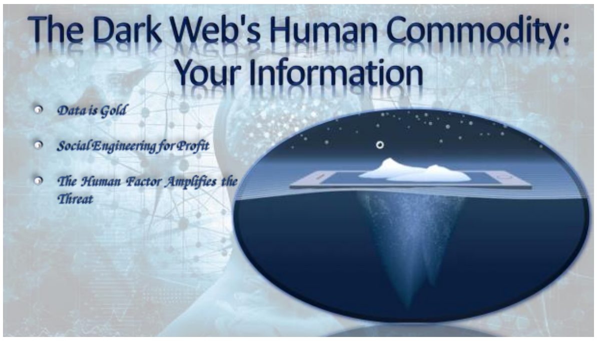
9



Your Network - A Playground for Human Hackers

- *Phishing Emails: The most common entry point*
- *Watering Hole Attacks: Compromising websites your employees frequently visit, lying in wait with malware*
- *Malicious Downloads: Disguising malware as legitimate software updates or tools, often spread through phishing*
- *Social Media Manipulation: Gathering information about your employees or posing as trusted contacts to gain access.*
- *Insider Threats: Remember disgruntled employees or those tricked into helping attackers (intentionally or not).*

10



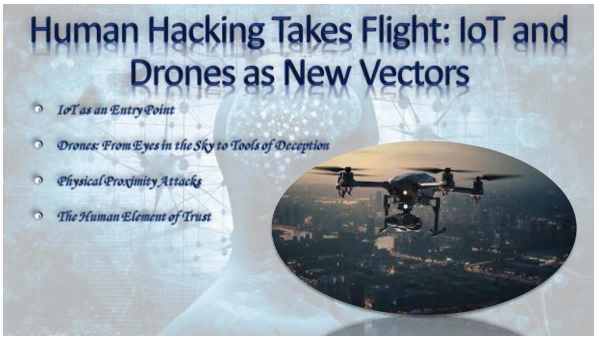
The Dark Web's Human Commodity: Your Information

- *Data is Gold*
- *Social Engineering for Profit*
- *The Human Factor Amplifies the Threat*

11

Dark Web

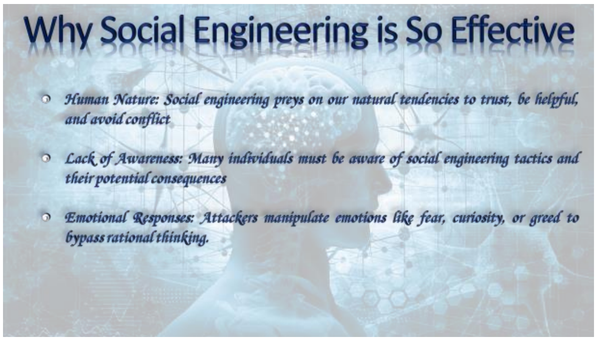
12



Human Hacking Takes Flight: IoT and Drones as New Vectors

- *IoT as an Entry Point*
- *Drones: From Eyes in the Sky to Tools of Deception*
- *Physical Proximity Attacks*
- *The Human Element of Trust*

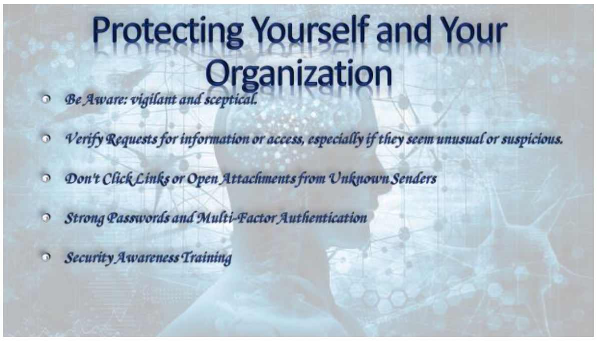
13



Why Social Engineering is So Effective

- *Human Nature: Social engineering preys on our natural tendencies to trust, be helpful, and avoid conflict*
- *Lack of Awareness: Many individuals must be aware of social engineering tactics and their potential consequences*
- *Emotional Responses: Attackers manipulate emotions like fear, curiosity, or greed to bypass rational thinking.*

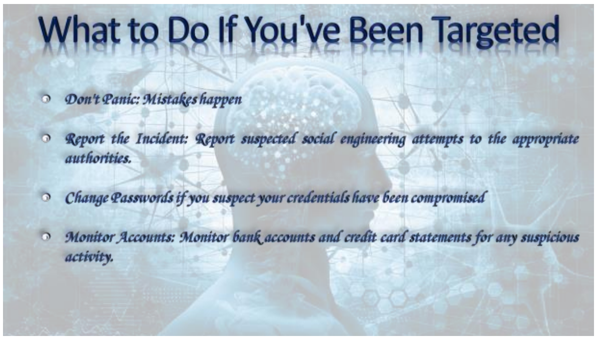
14



Protecting Yourself and Your Organization

- *Be Aware: vigilant and sceptical.*
- *Verify Requests for information or access, especially if they seem unusual or suspicious.*
- *Don't Click Links or Open Attachments from Unknown Senders*
- *Strong Passwords and Multi-Factor Authentication*
- *Security Awareness Training*

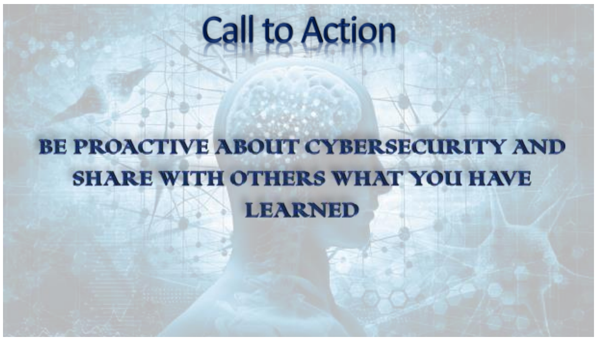
15



What to Do If You've Been Targeted

- *Don't Panic: Mistakes happen*
- *Report the Incident: Report suspected social engineering attempts to the appropriate authorities.*
- *Change Passwords if you suspect your credentials have been compromised*
- *Monitor Accounts: Monitor bank accounts and credit card statements for any suspicious activity.*

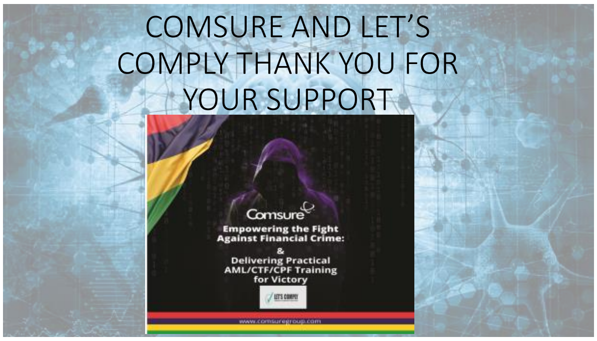
16



Call to Action

BE PROACTIVE ABOUT CYBERSECURITY AND SHARE WITH OTHERS WHAT YOU HAVE LEARNED

17



COMSURE AND LET'S COMPLY THANK YOU FOR YOUR SUPPORT

Comsure
Empowering the Fight Against Financial Crime:
&
Delivering Practical AML/CTF/CPF Training for Victory
LET'S COMPLY
www.comsuregroup.com

18