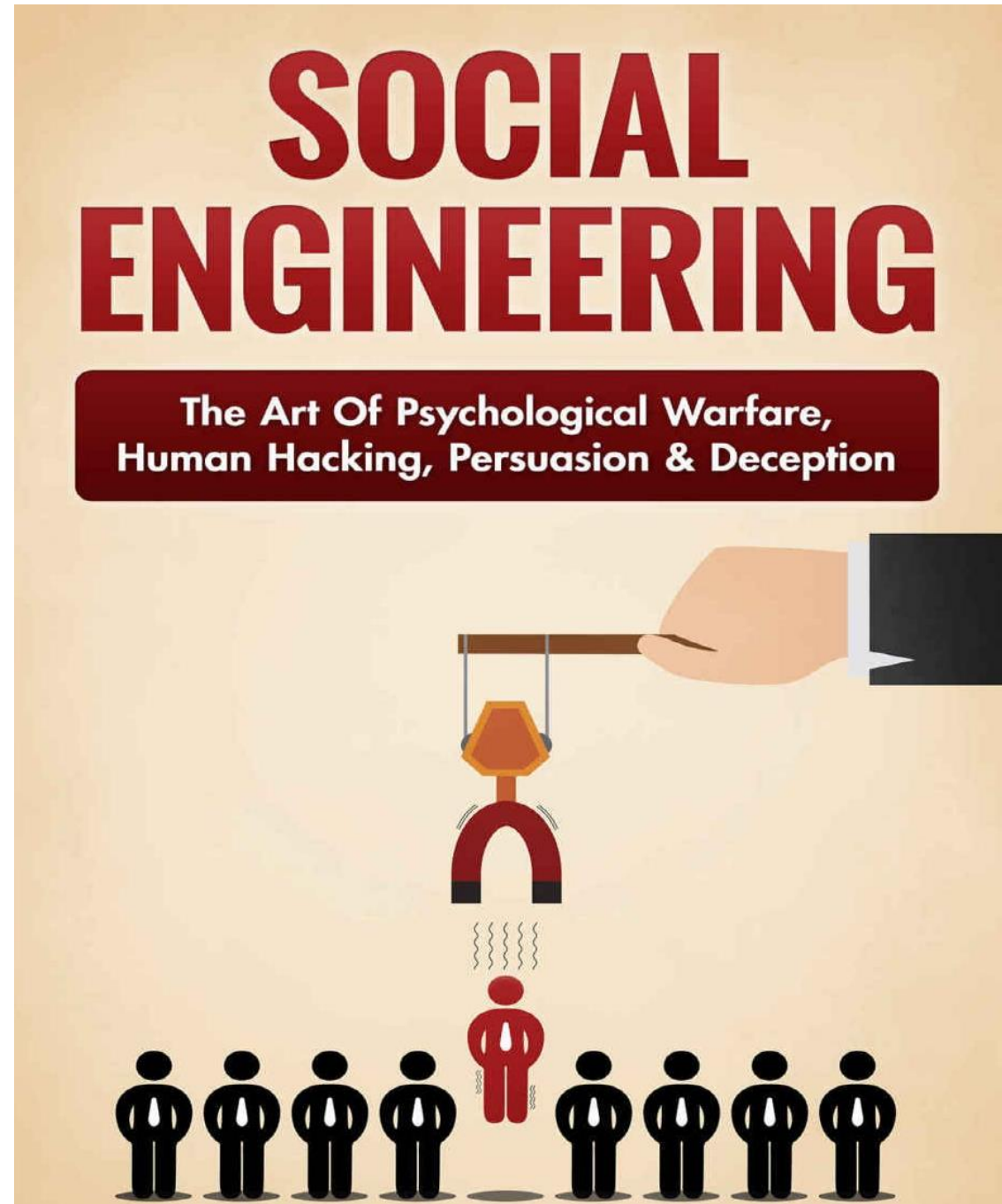




Dr. Marri Channa Reddy
Human Resource Development
Institute of Telangana

Social Engineering Attacks & Prevention

By
Ayub Shaik
Cybersecurity Strategist





Education

Bachelor of Technology in ECE, MBA.

Experience

20 Years of IT Critical Infrastructure, Cyber Defense, Digital Transformation

Certification

ISO27001

ISO 22301 LI

CoBIT5

TOGAF 9

Prince2

CBCI (BCM)

MCITP

CCNA

Oracle Big Data

Oracle Virtualization

Oracle DB12

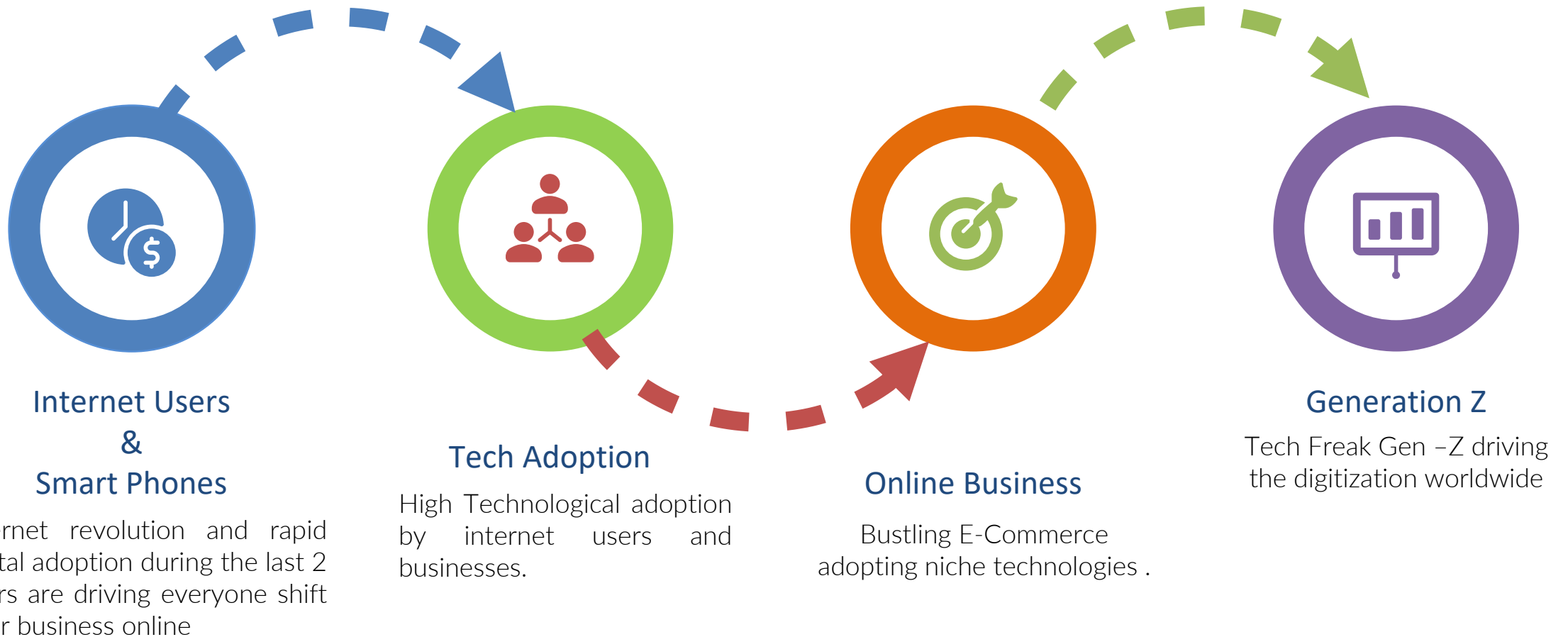
Oracle GTM

Expertise

Cybersecurity, Governance & management

Digitalization Factors

The implications of COVID-19 have accelerated digital adoption. The increasing use of technology to work, play, and stay connected have shaped new digital habits.



Global Cybercrime Damage Costs:

- **\$6 Trillion USD a Year.** *
- **\$500 Billion a Month.**
- **\$115.4 Billion a Week.**
- **\$16.4 Billion a Day.**
- **\$684.9 Million an Hour.**
- **\$11.4 Million a Minute.**
- **\$190,000 a Second.**



ALL FIGURES ARE
PREDICTED BY 2021

* SOURCE: CYBERSECURITY VENTURES



**CYBERSECURITY
VENTURES**




Social Engineering

The hacking of humans

Using knowledge of human behavior to elicit a defined response.

Types of Cyber Attack

1 Malware
●●●



TREND

2 Web based attacks
●●●



TREND

3 Web application attacks
●●●



TREND

4 Phishing
●●●




TREND

5 Spam
●●



TREND

6 Denial of service
●●●●




TREND

7 Ransomware
●●●



TREND

8 Botnets
●



TREND

9 Insider threat
●●●●●●●



TREND

10 Physical manipulation damage / theft / loss
●●



TREND

11 Data breaches
●●●



TREND

12 Identity theft
●●●●



TREND

13 Information leakage
●●●●●



TREND

14 Exploit kits
●●●●



TREND

15 Cyber espionage
●●●●●



TREND

KILL CHAIN

- Reconnaissance
- Weaponisation
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions on Objectives

COMMON ATTACK TECHNIQUES

PHISHING
ATTACKS



SPEAR
PHISHING



PRETEXTING



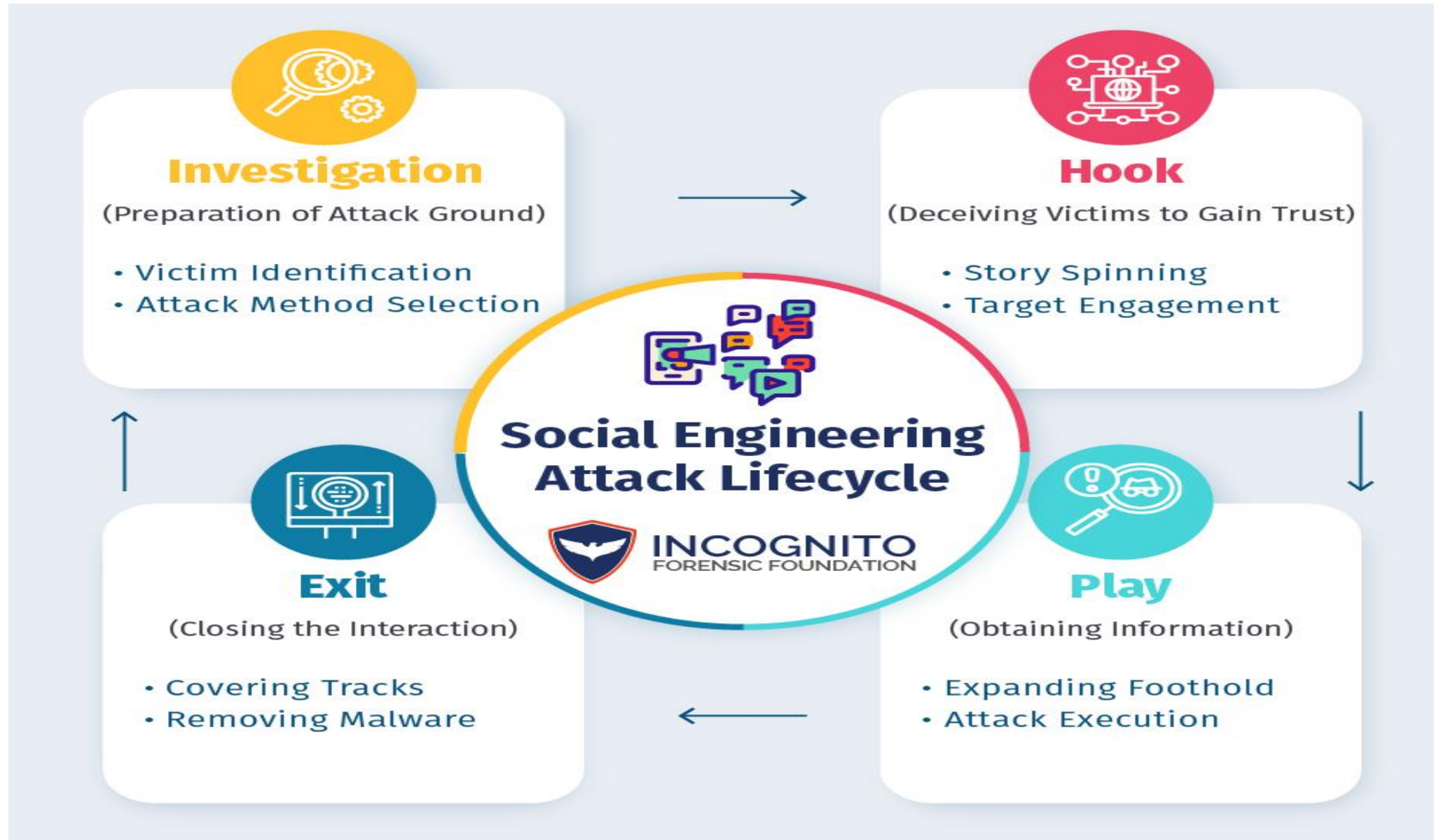
PSYCHOLOGICAL
MANIPULATION



TRUST
FACTOR



Attack Methodology



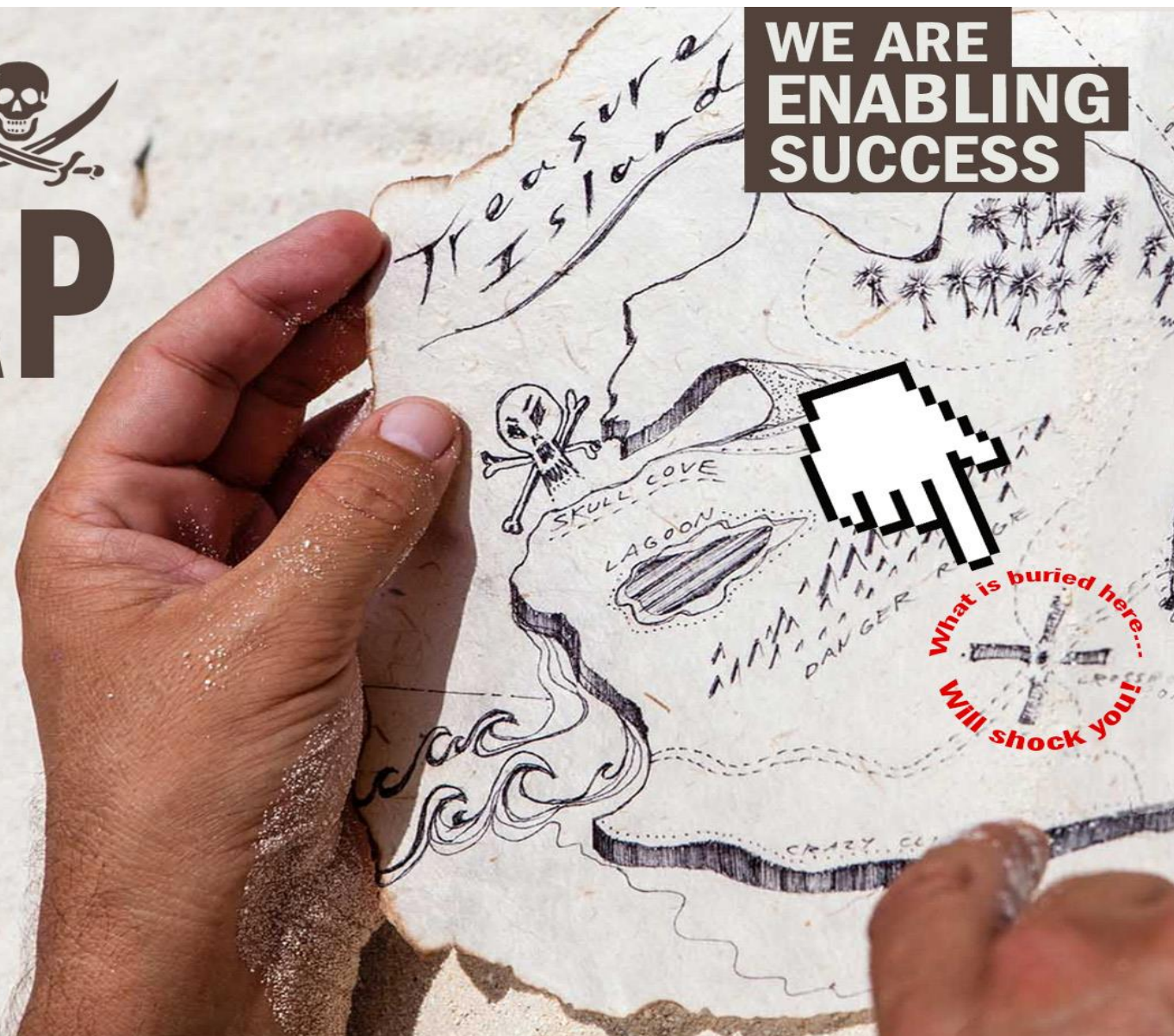
Honeytraps

DO not FALL for the HONEYTRAP

Beware of clickbait (sensationalized links); the Web is swimming in sites waiting to hijack computing devices and/or loot personal data.

THINK BEFORE YOU CLICK. Never give away your password, reveal personal information, or install unsolicited software.

**WE ARE
ENABLING
SUCCESS**



Generative AI Tools for Cyber Crime



DeepFakes

- Deepfake is a type of artificial intelligence used to create convincing images, audio and video hoaxes.
- Spread misinformation and inspire misunderstanding, fear or mislead.
- Create false narratives of people or group
- Create revenge porn to impact their integrity.
- Generate a specific public image for the subject (and sometimes make a one of themselves that contrasts and depends on the subject's falsified public image)
- Censure or mock the subject for deception
- Societal unrest



Phishing Attack



Attacker

Attacker sends an email to the victim

1



Victim

2

Victim clicks on the email and goes to the phishing website

10101011010101
10010101001010
11010101010101
101010101010

Attacker collects victim's credentials

3



Phishing Website

4

Attacker uses victim's credentials to access a website



Legitimate Website

Business Email Compromise



Phishing
Emails



Steal email
credentials



Search for financial
transactions



Disable
MFA



Compromise
account



Configure inbox
rule



Delete key
messages



Enable forwarding to
external address



Impersonate
communications

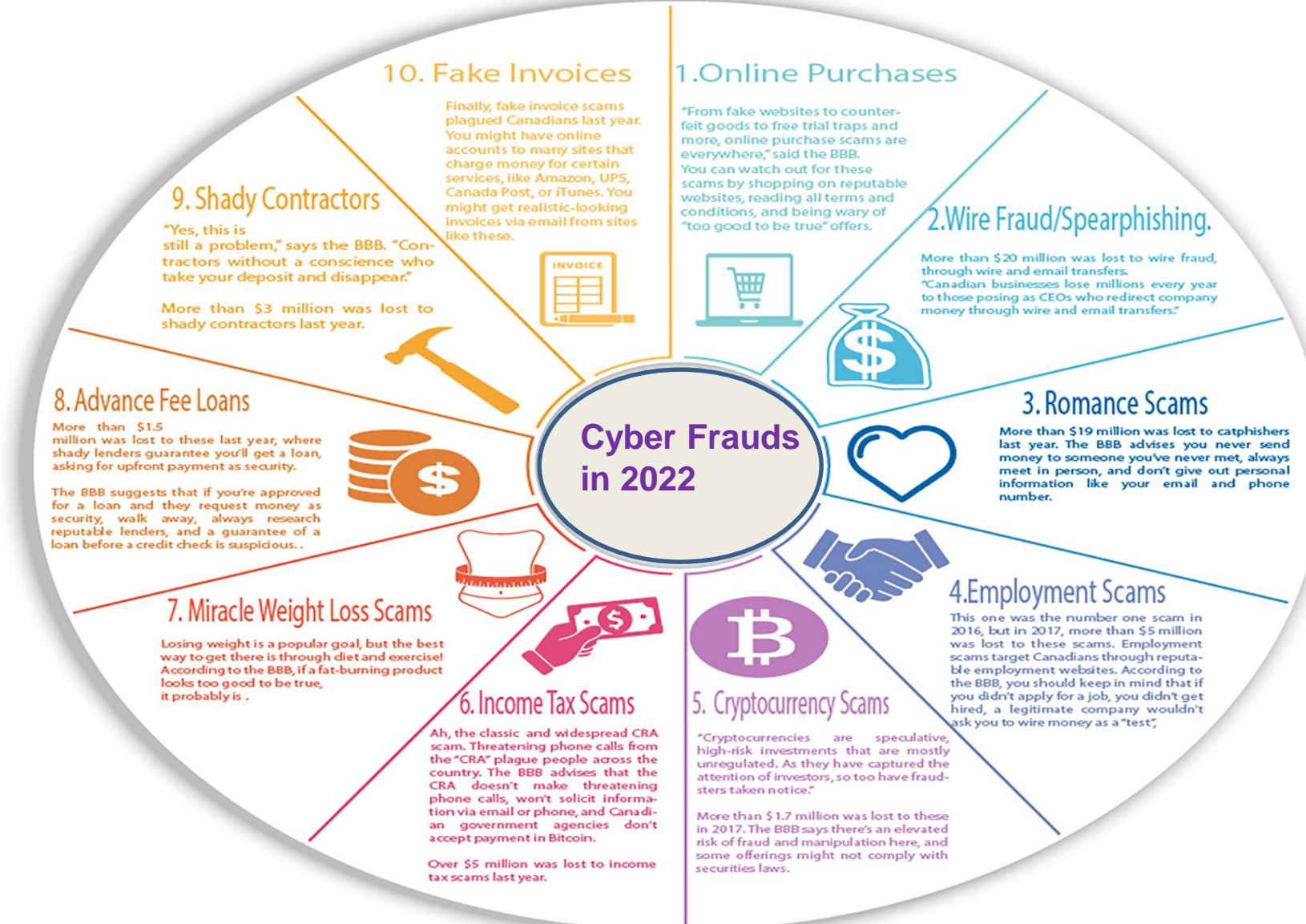


Request
payments



Redirect to fraudulent
accounts

Social Engineering Attacks



HOW TO PREVENT SOCIAL ENGINEERING ATTACKS

EDUCATION



MULTI FACTOR
AUTHENTICATION




PENETRATION
TESTING




UPDATING ANTIVIRUS
AND ANTI-MALWARE
SOFTWARE




CYBER SAFETY CHECKLIST



Back up online and offline files regularly and securely



Strengthen your home network




Use strong passwords




Keep your software updated



Manage social media profiles



Check privacy and security settings



Avoid opening and delete suspicious emails or attachments



INTERPOL

BE VIGILANT . BE SKEPTICAL . BE SAFE

15 WAYS

TO PROTECT YOUR BUSINESS FROM CYBERCRIME



SECURITY
ASSESSMENT



SECURITY
AWARENESS



PASSWORDS



DNS
PROTECTION



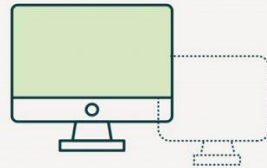
MOBILE DEVICE
SECURITY



ADVANCED ENDPOINT
DETECTION
AND RESPONSE



SIEM/LOG
MANAGEMENT



DARK WEB
RESEARCH



BACKUP



COMPUTER
UPDATES



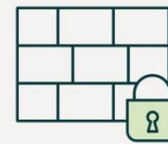
SPAM EMAIL



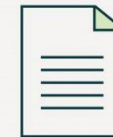
MULTI-FACTOR
AUTHENTICATION



ENCRYPTION



FIREWALL



CYBER
INSURANCE

How to Report Cyber Crime

भारत सरकार
GOVERNMENT OF INDIA

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

www.cybercrime.gov.in

Language 



राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
National Cyber Crime Reporting Portal



Resources Section"

- [REPORT WOMEN/CHILD RELATED CRIME +](#)
- [REPORT OTHER CYBER CRIME](#)
- [TRACK YOUR COMPLAINT](#)
- [CYBER VOLUNTEERS +](#)
- [RESOURCES +](#)
- [CONTACT US](#)
- [HELPLINE](#)



HELPLINE NUMBER
1930

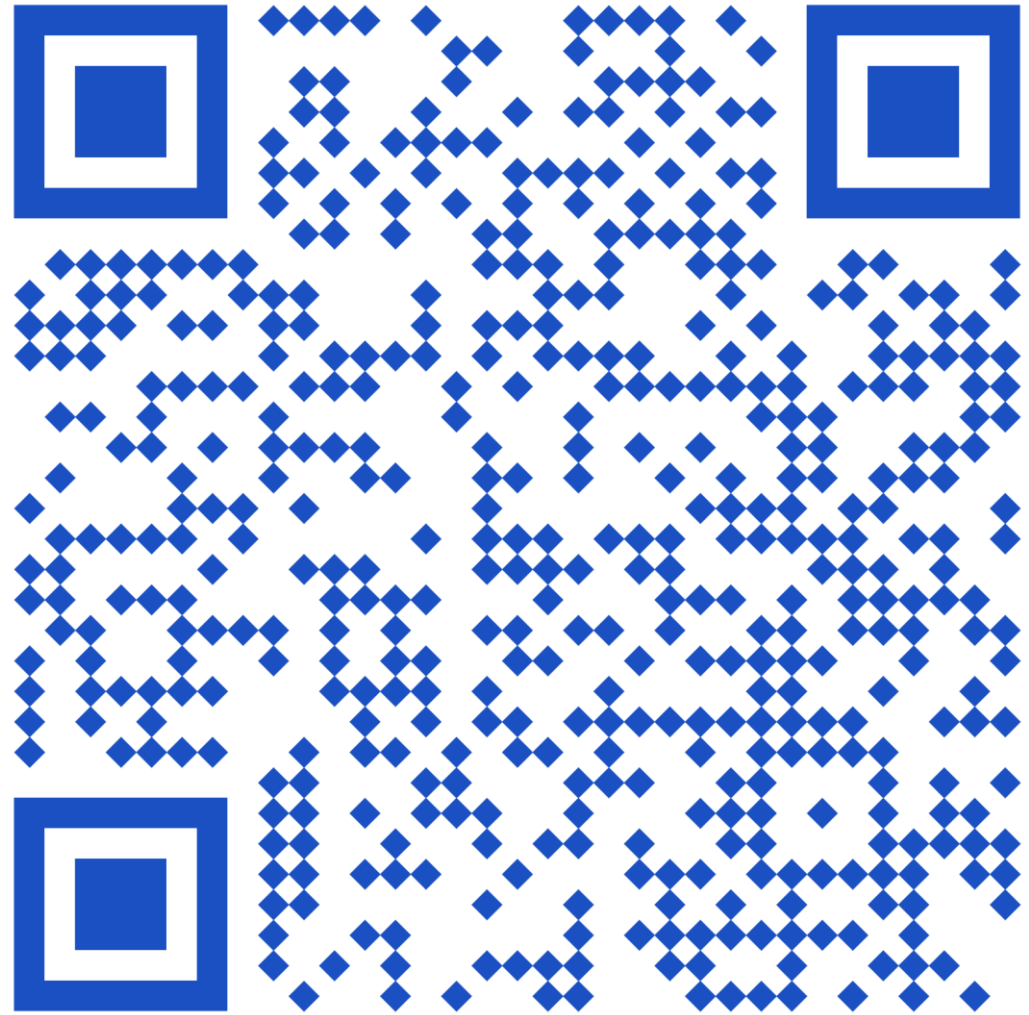


If you are a victim of
Financial Cyber Fraud
Dial Helpline Number 1930



Reach out for Guidance

www.linkedin.com/in/smayub



LET'S DISCUSS



HUNTMETRICS

ayub@huntmetrics.tech

+91 900 040 4422