

# New Technologies Used In Cybercrime



## Challenges with Investigation

**Herbert Gustav Yankson**  
**Chief Supt Of Police**  
**Head , Cybercrime Unit**  
**CID Headquarters. Accra**



# PRESENTAION OUTLINE

**Ghana's Digital Statistics**

**Cybercrime Landscape In Ghana**

**Prevalent Cybercrime Cases**

**The Ghana Cybercrime Statistic**

**The Challenges For Investigations**

**Conclusion**



# GHANA'S LOCATION





# GHANA'S DIGITAL STATS

JAN 2018

## GHANA

A SNAPSHOT OF THE COUNTRY'S KEY DIGITAL STATISTICAL INDICATORS



TOTAL POPULATION



**29.15**  
MILLION

URBANISATION:

**56%**

INTERNET USERS



**10.11**  
MILLION

PENETRATION:

**35%**

ACTIVE SOCIAL MEDIA USERS



**5.60**  
MILLION

PENETRATION:

**19%**

MOBILE SUBSCRIPTIONS

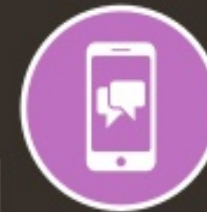


**34.57**  
MILLION

PENETRATION:

**119%**

ACTIVE MOBILE SOCIAL USERS



**4.90**  
MILLION

PENETRATION:

**17%**

92

SOURCES: POPULATION: UNITED NATIONS, U.S. CENSUS BUREAU; INTERNET, INTERNET WORLD STATS, IFLY, EUROSTAT, INTERNETLIVESTATS, CIA WORLD FACTBOOK, MEDIASTHEMIA.ORG, FACEBOOK, GOVERNMENT PORTALS, REGULATORY AUTHORITIES, REPUTABLE MEDIA; SOCIAL MEDIA AND MOBILE SOCIAL MEDIA: FACEBOOK, TWITTER, WHATSAPP, KAKAO TALK, LINE, SKYPE, WECHAT, PINTEREST, INSTAGRAM, POKEMON UNOFFICIAL; MOBILE: GSM INTELIGENCE; GOOGLE, ERICSSON, KPIIOS ANALYSIS. NOTE: PENETRATION FIGURES ARE FOR TOTAL POPULATION (ALL AGES).



Hootsuite™

we are social

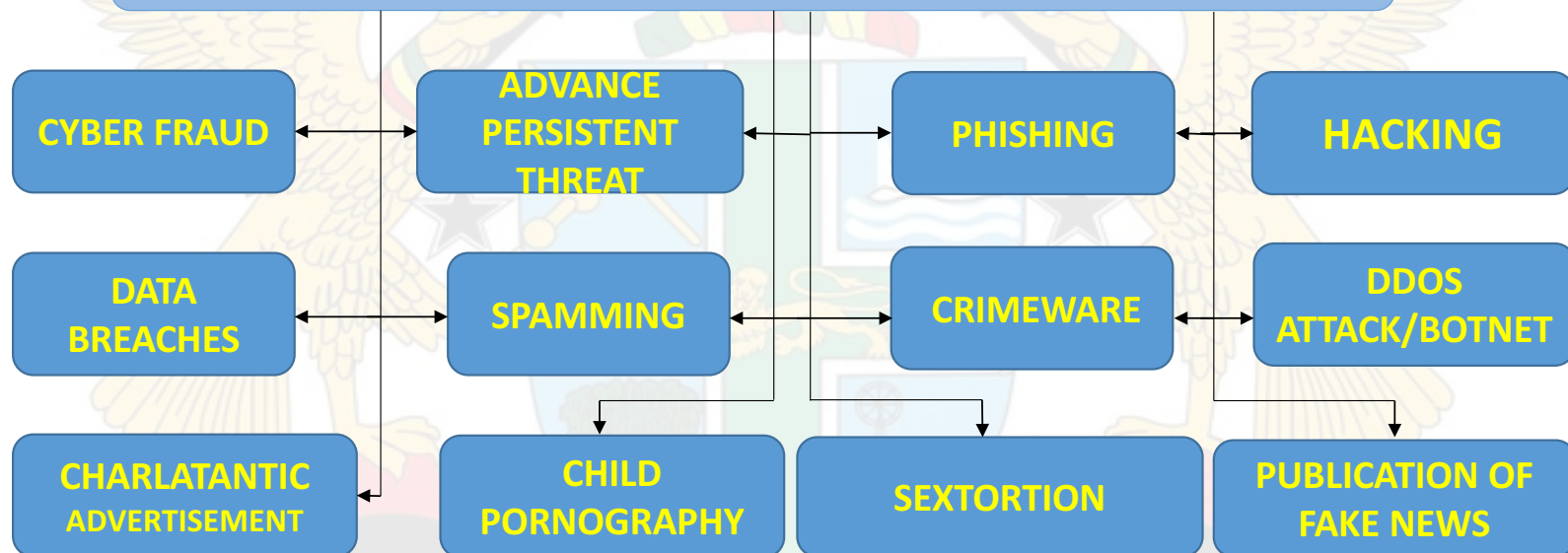


NATIONAL CYBER SECURITY CENTRE

Securing Ghana's Digital Journey

AND

# CYBER CRIME LANDSCAPE





## PREVALENT CYBERCRIME CASES

- **PHISHING AND SPEAR PHISHING**
- **CYBER FRAUD**
- **SEXTORTION**
- **RANSOMWARE**



## PHISHING

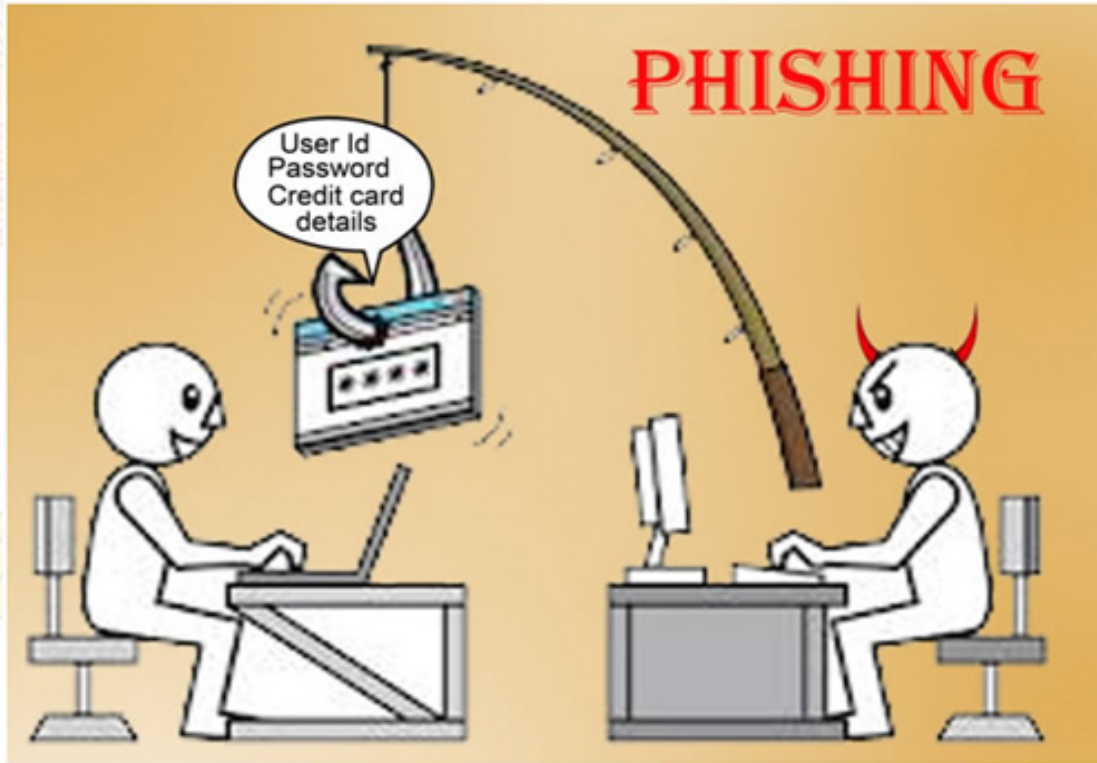
**Phishing** is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

**Communications purporting to be** from social web sites, auction sites, banks, online payment processors or IT administrators are often used to lure victims.

Phishing emails may contain **links to websites that are infected with malware.**



# PHISHING







## PHISHING



Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

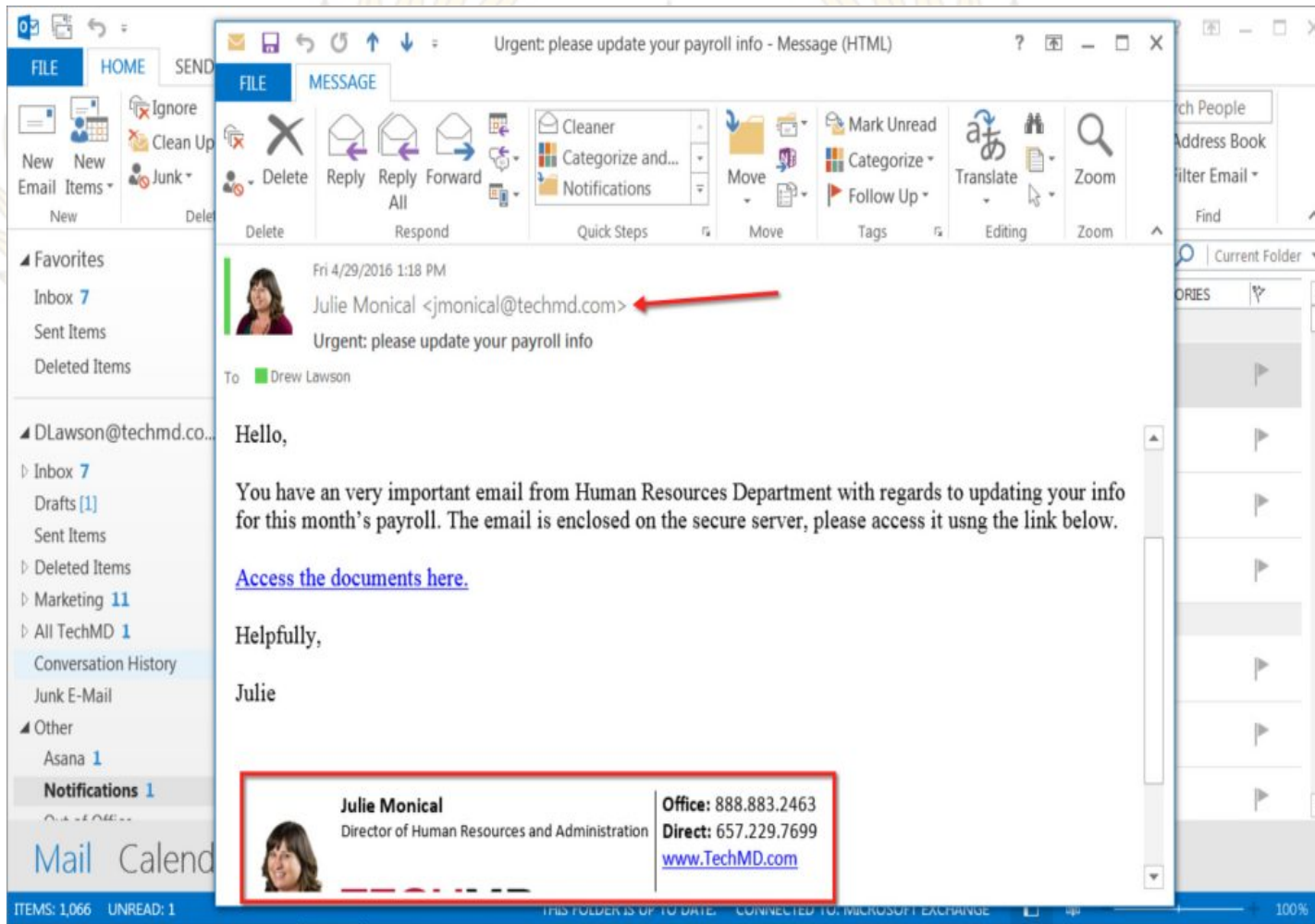
Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,  
TrustedBank

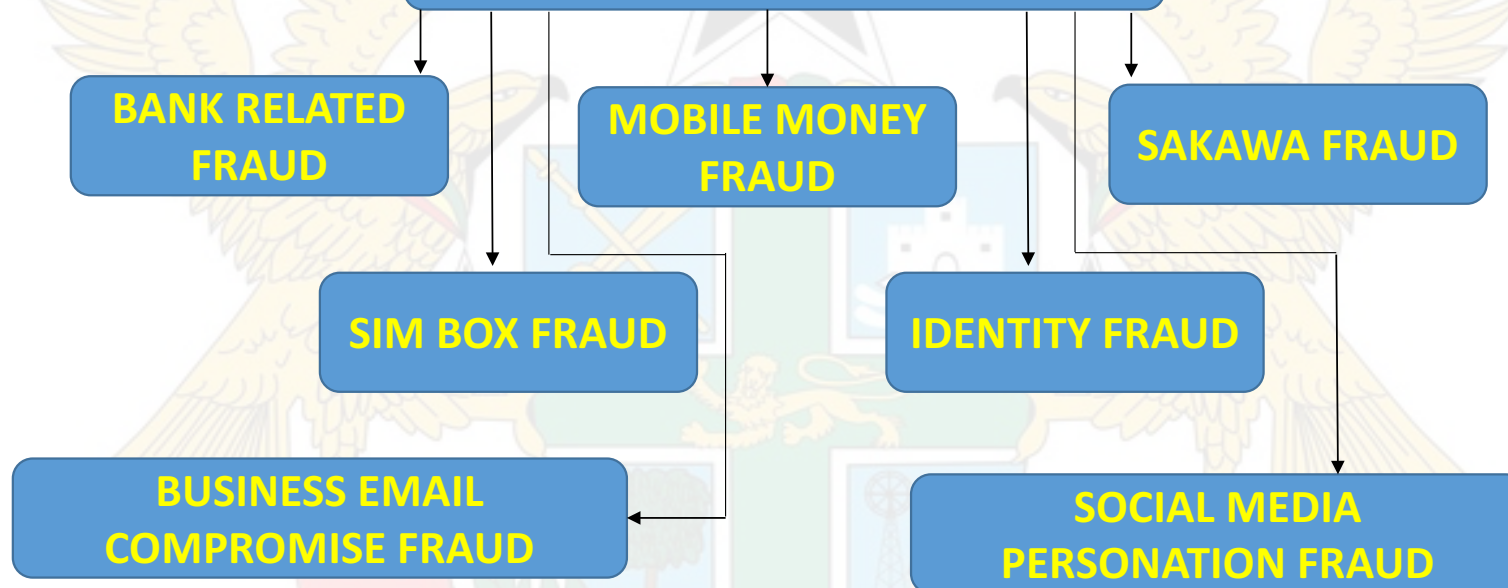


## SPEAR PHISHING

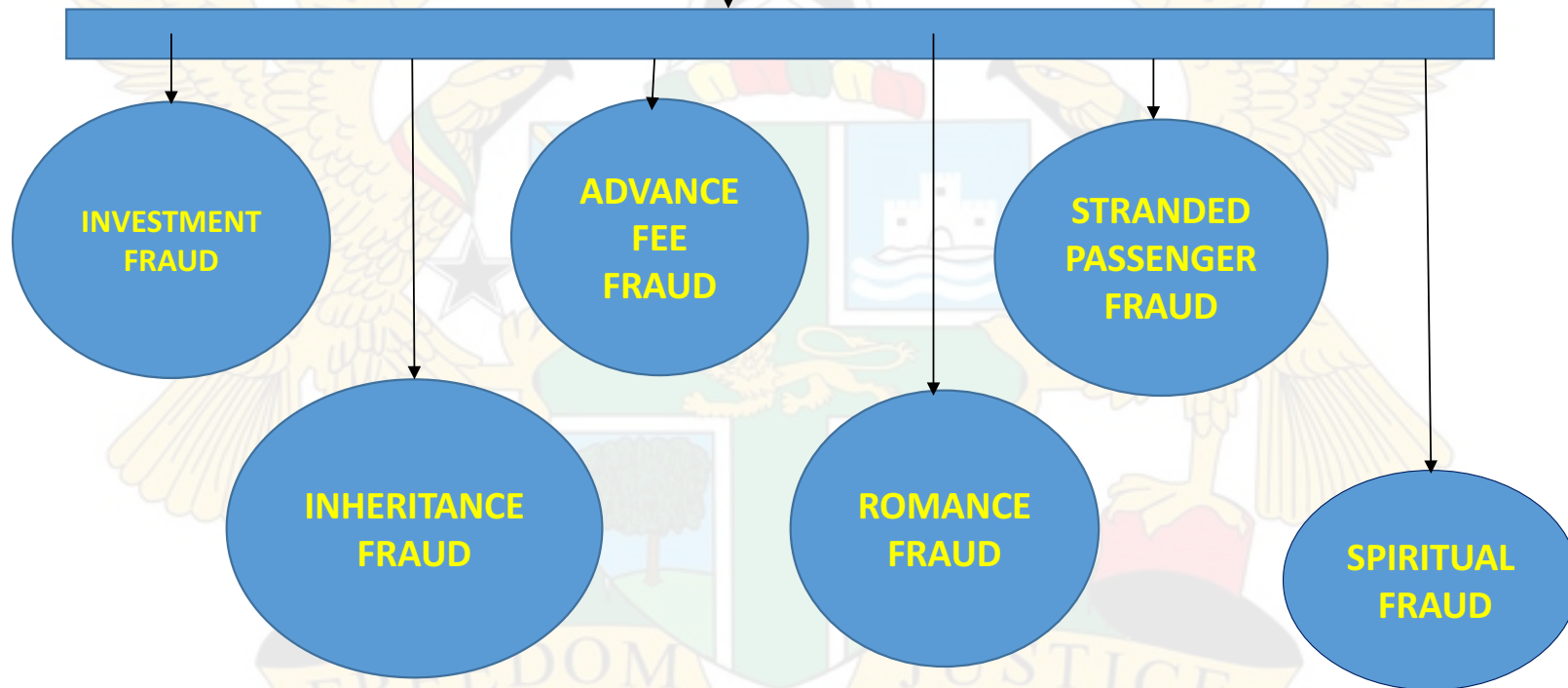
- Spear-phishing is a more targeted form of phishing.
- Whereas ordinary phishing involves malicious emails sent to any random email account, spear-phishing emails **are designed to appear to come from someone the recipient knows and trust**
- such as a colleague, business manager or human resources department—and can include a subject line or content that is specifically tailored to the victim's known interests or industry



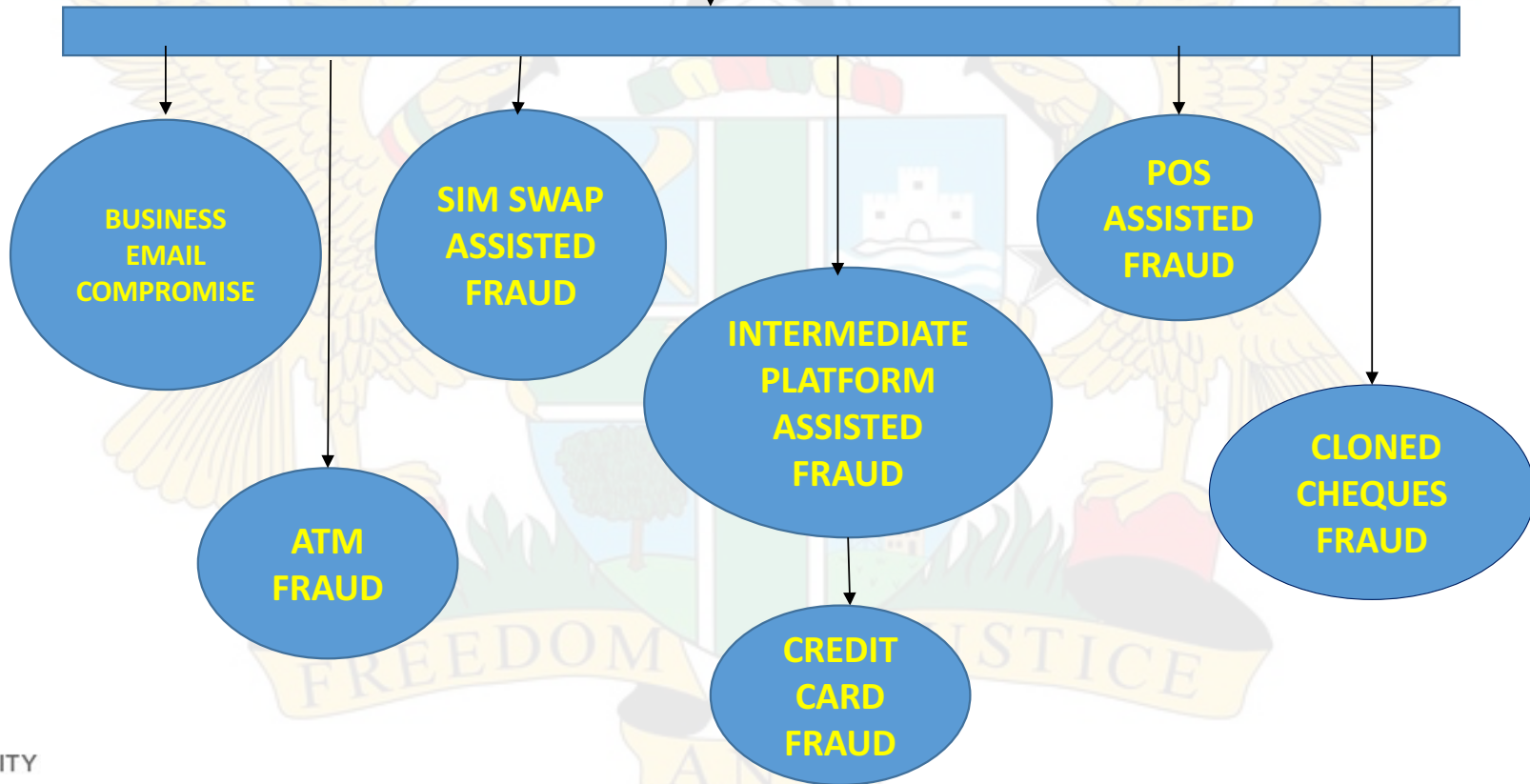
# CYBER FRAUD



# SAKAWA FRAUD



# BANK RELATED FRUAD





# Business Email Compromise

A **business email compromise** (BEC) is an exploit in which the attacker gains access to a corporate **email** account and spoofs the owner's identity to defraud the company or its employees, customers or partners of money



# Business Email Compromise

- Account intercepted using social engineering
- Accounts intercepted using malware via phishing emails
- Using spoofed emails- they obtain a domain to mimic the targets email address
- Creating email address to mimic the email of the target using free Web-based e-mail service
  - [smartamfo@yahoo.com](mailto:smartamfo@yahoo.com) ✓
  - [smartarnfo@yahoo.com](mailto:smartarnfo@yahoo.com) ✗
- Using anonymous remailer websites to create email address similar to that of their target



# MOBILE MONEY FRUAD

## SCHEMES EMPLOYED



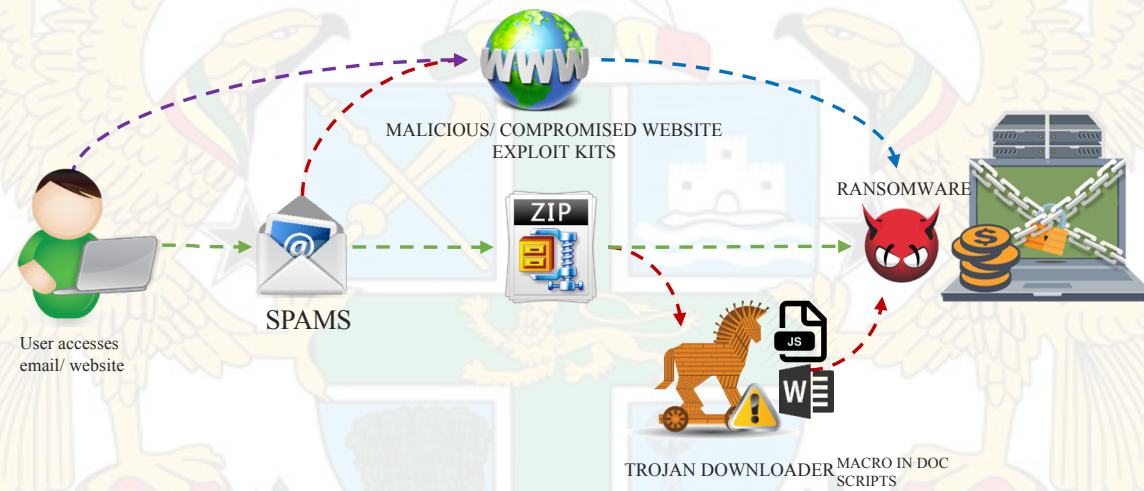


# RANSOMWARE

- Ransomware is a malware that targets your critical data and systems for the purpose of extortion
- Victim's computer is infected with malware
- Malware encrypts the victim's data and /or computer making them unreadable
- Attacker demands a ransom before the files/system/network is decrypted
- Payment is usually demanded through Bitcoins
- Ransomware is frequently delivered through **spear phishing e-mails**

# RANSOMWARE

## Deployment models





# WANNACRY RANSOMWARE

Recent wannacry attacks targeted organization, government and end users, making awareness and training a critical preventive measure.

**Wannacry** is a ransomware **CRYPTOWORM**, which targets computers running the Microsoft Windows operating system that have not been updated with recent security updates

**Global impact** – victims spread over around 200 countries

**Maximum diffusion** – The malicious code is automatically copied onto each PC in the same network who presents the same vulnerability



# WANNACRY RANSOMWARE

Wana Decrypt0r 2.0

**Oops, your files have been encrypted!** English



**What Happened to My Computer?**  
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**  
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**  
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

**Payment will be raised on**  
5/16/2017 00:47:55  
Time Left  
02:23:57:37

**Your files will be lost on**  
5/20/2017 00:47:55  
Time Left  
06:23:57:37

[About bitcoin](#)  
[How to buy bitcoins?](#)  
[Contact Us](#)

**Send \$300 worth of bitcoin to this address:**  
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw Copy

**Check Payment** **Decrypt**





# SEXTORTION

**Sextortion** is a form of sexual exploitation that employs non-physical forms of coercion to extort sexual favors from the victim

**Sextortion** also refers to a form of blackmail in which sexual information or images are used to extort sexual favors, money or information from their victim.



# SEXTORTION

## How images and videos are acquired

- Relationship-freewill sharing (mostly with unknown partners online) and through secret recording during video chat
- Phone repairers
- Seeking help from technologically savvy friends
- WhatsApp web and other forms of intrusion methods
- Losing digital devices through stealing or any other means particularly with no security
- Improper Idle time setting
- Cracking passwords
- Use of female criminal syndicate



# Ghana Cybercrime Statistics

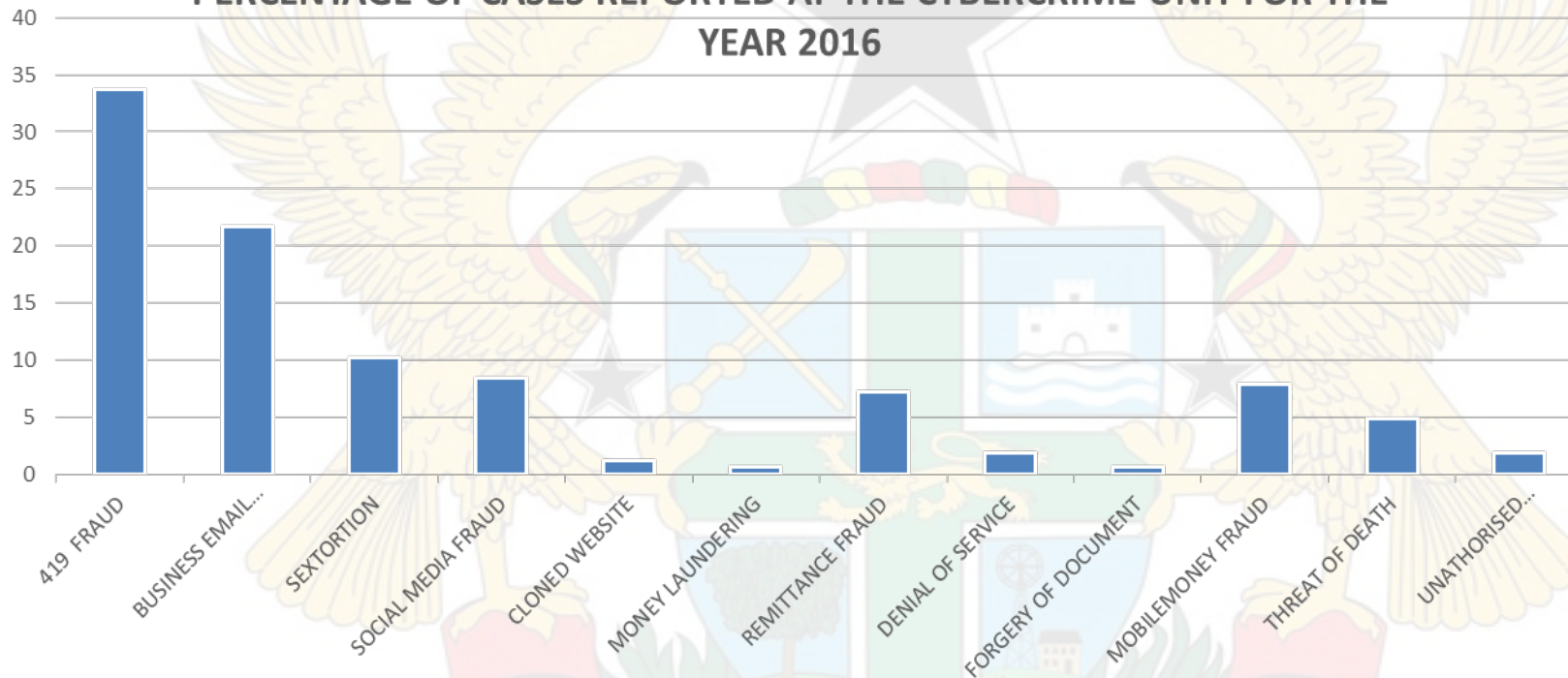


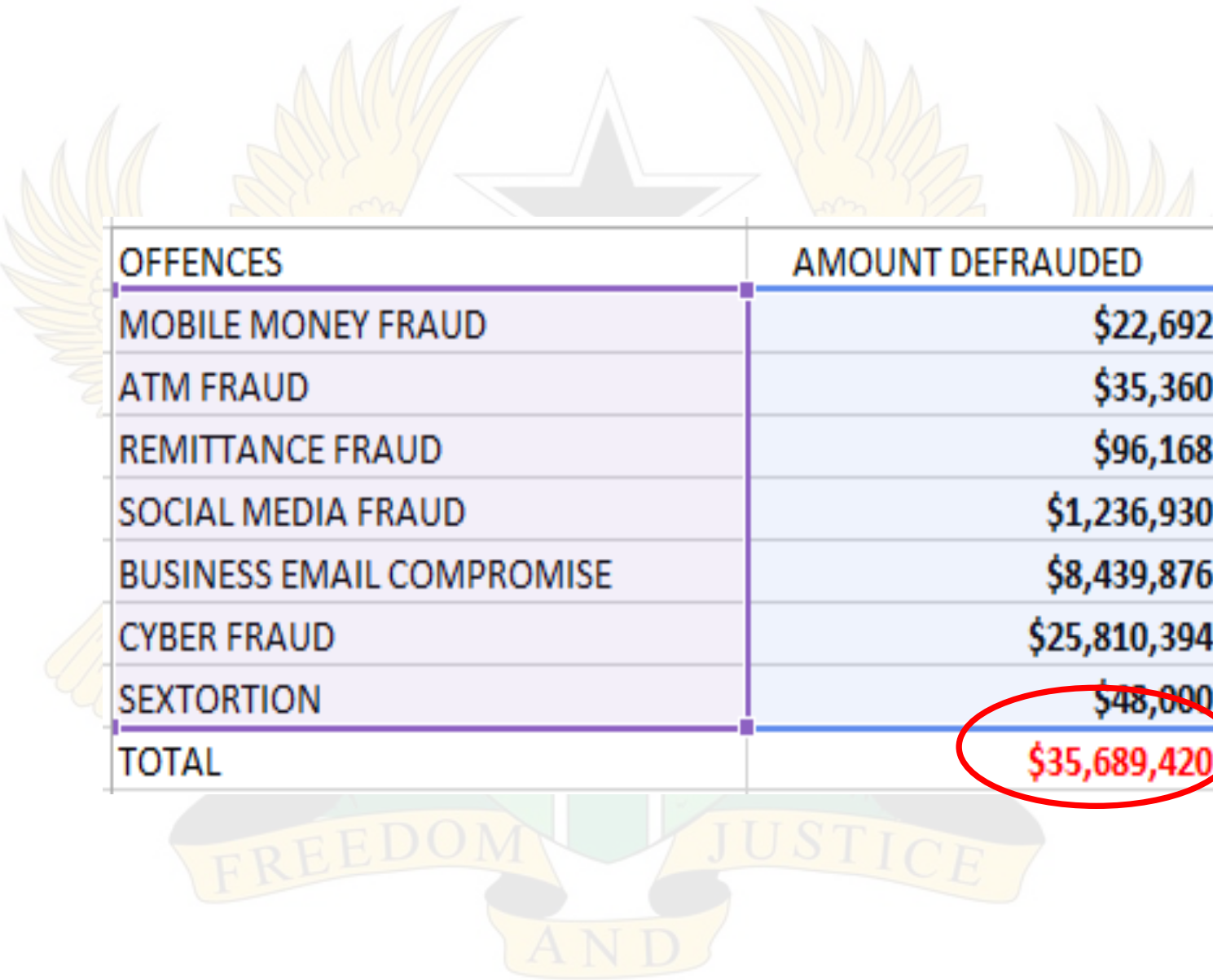
**GHANA**

50



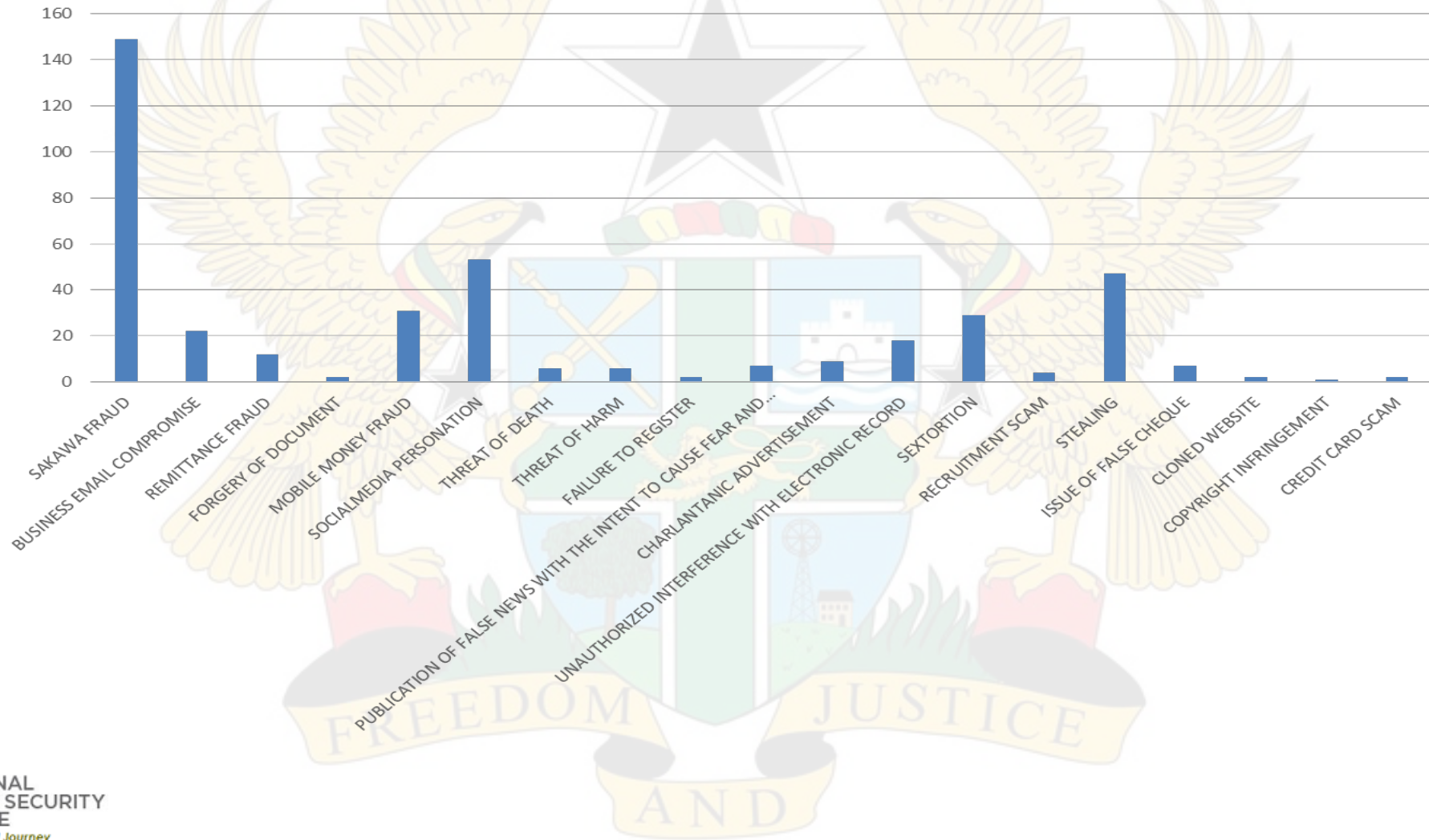
## PERCENTAGE OF CASES REPORTED AT THE CYBERCRIME UNIT FOR THE YEAR 2016



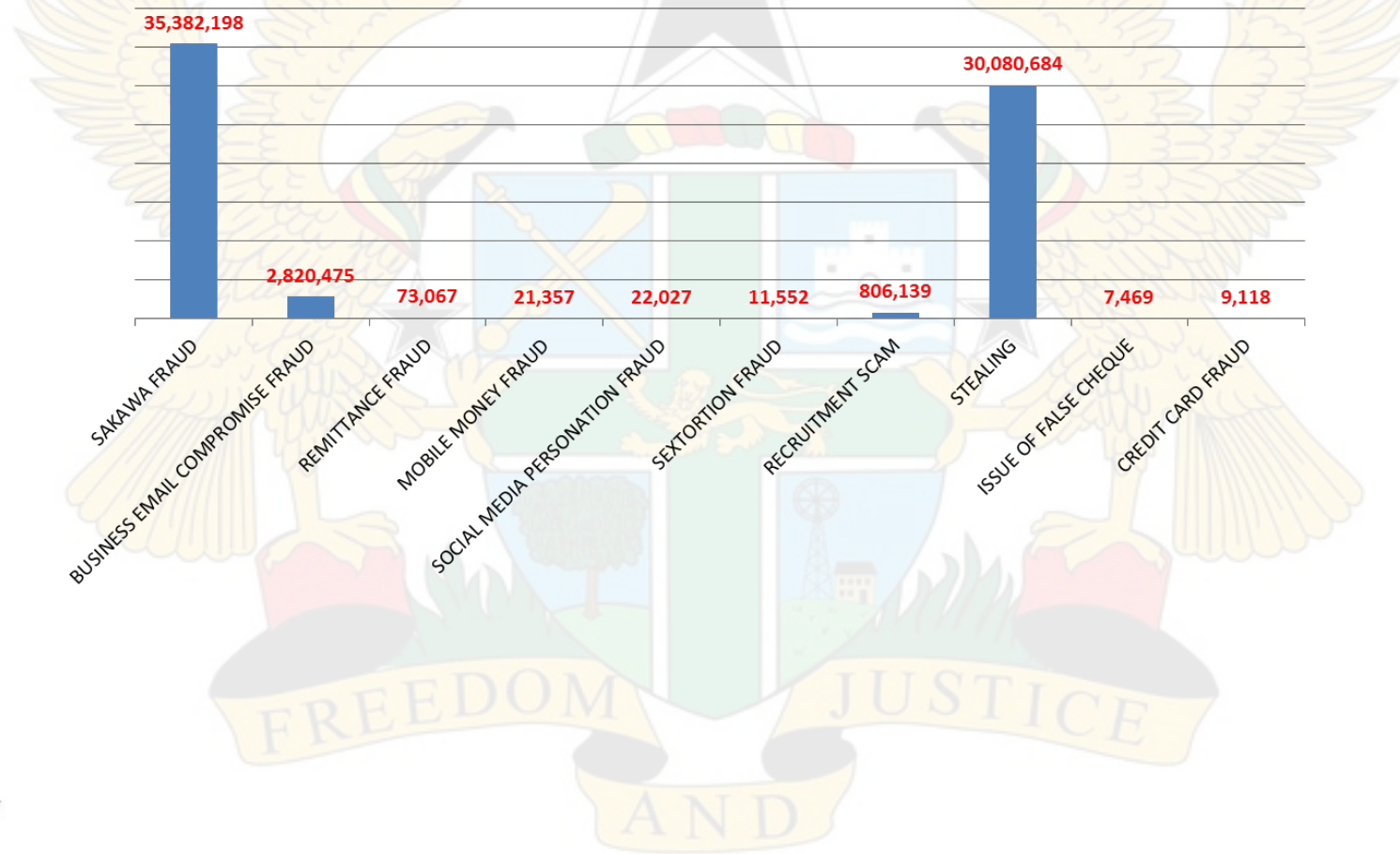


OFFENCES	AMOUNT DEFRAUDED
MOBILE MONEY FRAUD	\$22,692
ATM FRAUD	\$35,360
REMITTANCE FRAUD	\$96,168
SOCIAL MEDIA FRAUD	\$1,236,930
BUSINESS EMAIL COMPROMISE	\$8,439,876
CYBER FRAUD	\$25,810,394
SEXTORTION	\$48,000
<b>TOTAL</b>	<b>\$35,689,420</b>

Cases Received at Cybercrime Unit in the year 2017



**Graph Showing Types of Cases and Amount Lost to Criminals(\$) for the Year 2017**



TYPE OF CASE	AMOUNT(\$)
SAKAWA FRAUD	35,382,198
BUSINESS EMAIL COMPROMISE FRAUD	2,820,475
REMITTANCE FRAUD	73,067
MOBILE MONEY FRAUD	21,357
SOCIAL MEDIA PERSONATION FRAUD	22,027
SEXTORTION FRAUD	11,552
RECRUITMENT SCAM	806,139
STEALING	30,080,684
ISSUE OF FALSE CHEQUE	7,469
CREDIT CARD FRAUD	9,118
<b>TOTAL</b>	<b>69,234,085</b>





## CHALLENGES WITH CYBERCRIME INVESTIGATIONS

### Global Nature - Multiple territorial connections

- **The action of the criminals reach computers and victims in countries other than their countries**
- Evidence may be found in different jurisdictions
  - Gmail/Yahoo Webmails
- National law enforcement agencies are limited to their geographical borders while criminals have unlimited borders?
  - International assistance in criminal investigations require proper legal channels?
  - Mutual legal assistance Treaty (MLAT) Required



## CHALLENGES WITH CYBERCRIME INVESTIGATIONS

- **Evidence is volatile**
- States, citizens and economies depend internet creating heavy network traffic and huge amounts of data generated. Data is easily overwritten as result
- Security vs. business challenge (collaborating with Telecommunication companies)



## CHALLENGES WITH CYBERCRIME INVESTIGATIONS

### **Investigation units are understaffed and not adequately trained/ skilled**

- Increasing number of cases which makes investigators ineffective
- Huge backlog of computers to be examined
- Understanding changing Modus Operandi and knowing what evidence to collect
- Investigations into possible forms of Organized Crime vs. Single criminal





## CHALLENGES WITH CYBERCRIME INVESTIGATIONS

### Coping with new technological paradigms

**New illegal activities** are being “invented” everyday

#### Hacking as a service

- Outsourcing of a complete cyber-enabled attack
- Technical support for cybercrime activities

#### Crimeware as a service

- Sophisticated exploit kits and other malware for rent
- Development of malware for niche markets

#### Research-as-a-service

- Legal or illegal collection of information on victims ▪
- Resale of stolen personal data or email addresses

#### Infrastructure as a service

- Hosting of malware on secure networks
- Rental of established botnets for Distributed Denial-of-Services



## CHALLENGES WITH CYBERCRIME INVESTIGATIONS

### Coping with new technological paradigm





## CHALLENGES WITH CYBERCRIME INVESTIGATIONS

### Coping with new technological paradigms

- TOR Networks provides anonymity and privacy by shielding them from LEA
- Darkweb refers to websites on a darknet





## CHALLENGES WITH CYBERCRIME INVESTIGATIONS

### Coping with new technological paradigms

- Cloud Computing – “Evidence in the Cloud”
- Cryptocurrency provides anonymous transaction eg Bitcoin
  - Digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.
  - Monies obtain through crime are laundered through bitcoins
- Anonymous remailers help spoof email
  - An anonymous remailer is specialized kind of mail server designed to send e-mail messages without identifying the sender. Many of them are provided as a free service.



## CHALLENGES WITH CYBERCRIME INVESTIGATIONS

### Coping with new technological paradigms

- Use of technology including VPN and Proxy poses a challenge
  - A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet.
  - A proxy or proxy server is basically another computer which serves as a hub through which internet requests are processed. By connecting through one of these servers, your computer sends your requests to the proxy server which then processes your request and returns what you were wanting



## CHALLENGES WITH CYBERCRIME INVESTIGATIONS

### Coping with new technological paradigm

- **IoT – Internet of things**
  - Every device is connected to the Internet and addressable via its' own IP address
  - Devices communicate with their owners and with each others
- **Challenges**
  - These devices become targets because the product have security vulnerabilities.
  - Many of these devices are compromised and used as be used as botnets
- **Technical knowledge** is required to investigate such cases hence difficult for an average investigator



## CHALLENGES WITH CYBERCRIME INVESTIGATIONS

- **Instant Messaging and Social Networking site** have taken over as the communications tool of choice in recent years with many well known examples providing instant and user friendly access by the use of encryption technology which reduce the chances of detection
- Request for Content requires MLAT which takes months/year





## CHALLENGES WITH CYBERCRIME INVESTIGATIONS

### ENCRYPTION CHALLENGE

The intentional storage of information in encrypted form on devices of victims, witnesses or suspects.

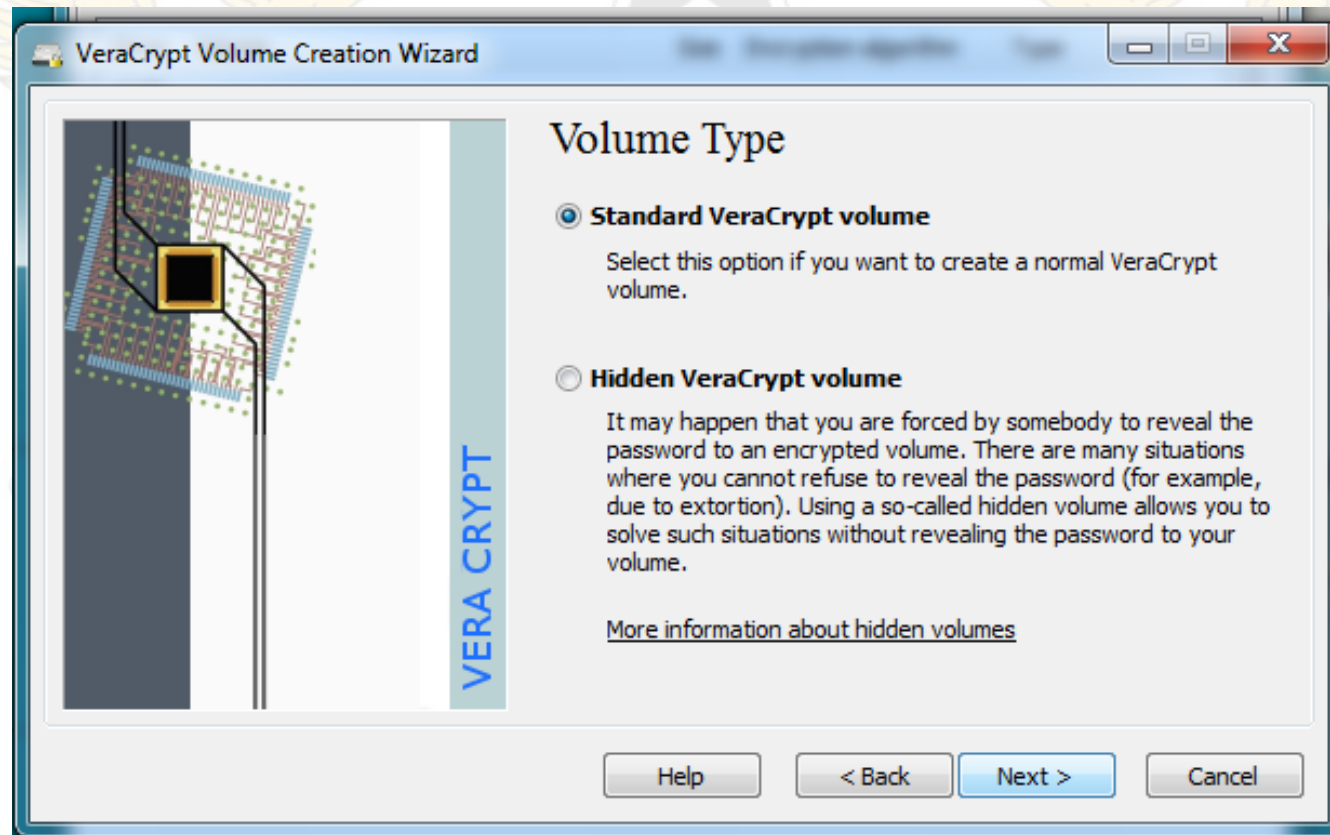






## CHALLENGES WITH CYBERCRIME INVESTIGATIONS

### ENCRYPTION CHALLENGE





## CHALLENGES WITH CYBERCRIME INVESTIGATIONS

**Limited technical capabilities** to support a successful investigation

Digital forensics laboratories outdated

Malware forensics and reverse engineering capacities

Collaboration with local telecommunication service providers (understanding their operation)

**International cooperation**

Police to Police

International Judicial Cooperation

Interactions with international large service providers (Social Networks, etc.)



## CHALLENGES WITH CYBERCRIME INVESTIGATIONS

- Different countries with different cultures, with different legal tradition and different criminal law frameworks see these criminal activities different
- **Cybercrime legislation – Harmonization**  
Definition of cybercrimes  
Where was Crime Committed? Which Country has jurisdiction?  
Need to adopt global standards, International Treaties
- **Lack of common understanding** on cybercrime amongst the criminal justice authorities



## CONCLUSION

- Requires local and international Collaboration
- Comprehensive programme to train all Law Enforcement Officer, Prosecutors and Judges .
- Technical Capacity Built
- Increase Awareness Creation
- International legal instrument required
- Strengthen our laws to be in harmony with international Legal Instrument



# Questions