
CYESEC TECH
CYBER SECURITY & ESOLUTIONS

CRYPTOCURRENCY AND BLOCKCHAIN

FRAUD DETECTION MECHANISMS

Dr. Emmanuel O. Okoi

CEO/Faculty: CYESEC TECHNOLOGIES

(Cybersecurity & ESolutions)

Red & Blue Team Lead

Multi-Certified in Offensive & Defensive Cybersecurity

HND ||BSC || MSC|| PhD

|| CCNA || CEH || CCSA || CPENT ||CDFA || CAPIS || ISO/IEC 27003

Cybersecurity & Forensic Analyst

INTRODUCTION

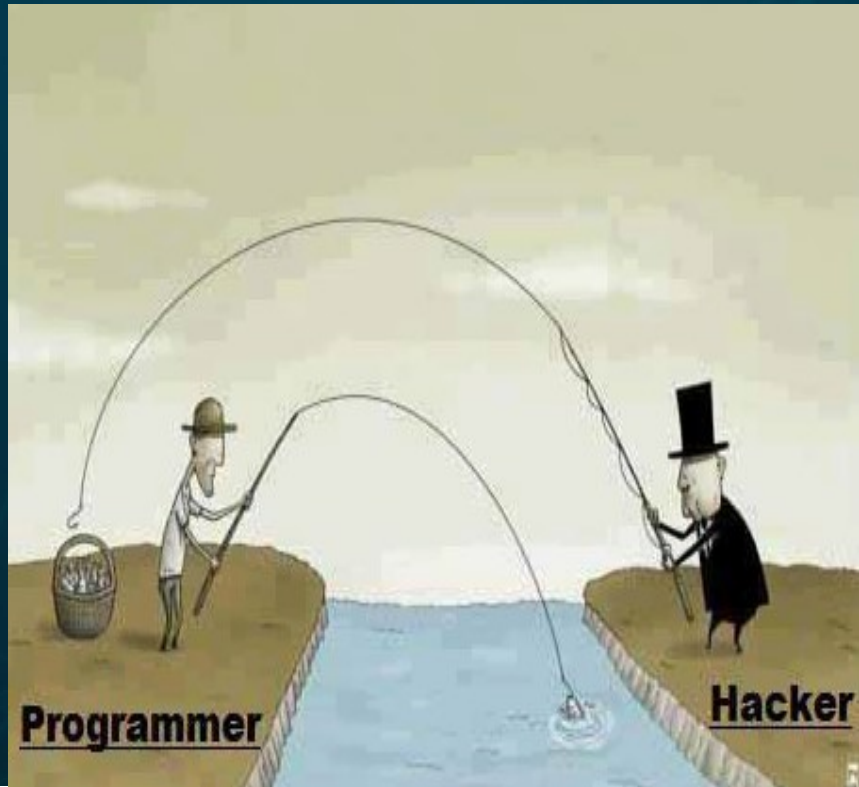
- What is Cryptocurrency?
- What is Blockchain?
- Importance of Forensics in Crypto
- Rise in Crypt-Related Fraud

OBJECTIVES

- Understand the structure of crypto fraud
- Explore cyber tools and techniques
- Evaluate fraud detection strategies
- Recommend future-proof solutions

Common Types of Crypto Fraud.

- Ponzi Schemes
- Rug Pulls
- Phishing & Impersonation
- Money Laundering via Mixers
- Fake ICOs and Token Scams



KEY COMPONENTS OF BLOCKCHAIN TRUST ANALYSIS

Blockchain trust analysis refers to evaluating how much trust can be placed in a blockchain system based on its technical, organizational, and social characteristics.

(1) Decentralization: Distribution of control and decision-making across a network.

- Node distribution
- Geographic dispersion
- Developer control

Trust Implication: High decentralization reduces the risk of collusion and single points of failure,enhancing trust.

(2) Immutability: Once data is recorded on the blockchain, it cannot be altered.
Trust Implication: Ensures data integrity and makes the blockchain a reliable source of truth.

(3) Transparency and Auditability: Transactions and smart contracts are publicly visible and verifiable.

Trust Implication: Enables third-party audits and increases user confidence.

(4) Consensus Mechanism: Determines how agreement is reached on the blockchain.
Types: Proof of Work(PoW),Proof of Stake(PoS),Delegated PoS (DpoS),Practical Byzantine Fault Tolerance(PBFT)
Trust Implication: A more secure and decentralized consensus algorithm fosters higher trust (e.g.,Bitcoin’s PoW is trusted for its security, though it's resource-heavy).

3 ADVPHISH INSTALL/RUN

INSTALLATION

```
└──── $ git clone https://github.com/Ignitetch/AdvPhishing.git
└──── $ cd AdvPhishing/
└──── $ chmod 777 *
└──── $ ./Linux-Setup.sh
└──── $ ./AdvPhishing.sh
```

AVAILABLE TUNNELLING OPTIONS

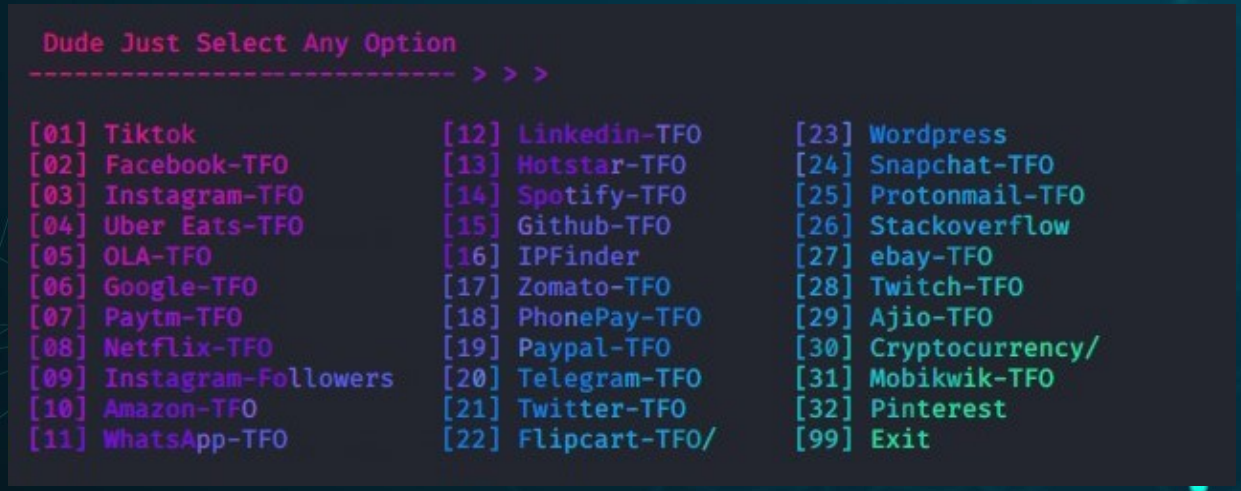
LOCALHOST
NGROK (https://ngrok.com/)

TO BE USED FOR EDUCATIONAL PURPOSES ONLY

3 PHISHING

- **Tool :AdvPhishing**

As the name implies, it's one of the most Advance phishing tools because of it extra features which includes {Phishing, IPGrabbing & Information Gathering, OTP Phishing}. It's also known to have a more updated login pages of over 32 social media and payment platforms.



(5) Smart Contract Reliability: **A**utomated contracts that execute without intermediaries.

Trust Implication: **B**ugs or vulnerabilities in smart contracts (e.g., DAO hack) can compromise trust; formal verification and audits enhance reliability.

(6) Governance Model: **T**he rules and structure for decision-making on protocol upgrades and dispute resolution.

Types: On-chain governance and Off-chain governance

Trust Implication: Transparent and inclusive governance enhances long-term system credibility.

7. Legal and Regulatory Compliance etc.

FRAUD DETECTION SYSTEMS BUILT ON BLOCKCHAIN.

(1)Transaction Transparency

(2).Public Ledgers as Evidence

(3). Wallet Tracing and Entity Clustering

We would demonstrate how Bitcoin transactions are traced!

FRAUD DETECTION MECHANISMS

- Anomaly Detection in Transactions
- Address Clustering & Behavior Analytics
- Smart Contract Auditing
- Pattern Recognition in Mixing Services
- Machine Learning for Risk Scoring

CHALLENGES IN CRYPTO & BLOCKCHAIN

- Unprepared Users Education
- Use of Privacy Coins (e.g., Monero)
- Cross-border Investigations
- Limited Technical Expertise

RECOMMENDATIONS

- Capacity Building & Training
- Public-Private Partnerships
- **Consult Cyber and Forensic Experts Before Investing**
- Stronger Regulatory Compliance

IS MY LINK SAFE?

PLATFORMS TO CONFIRM IF A LINK IS SAFE

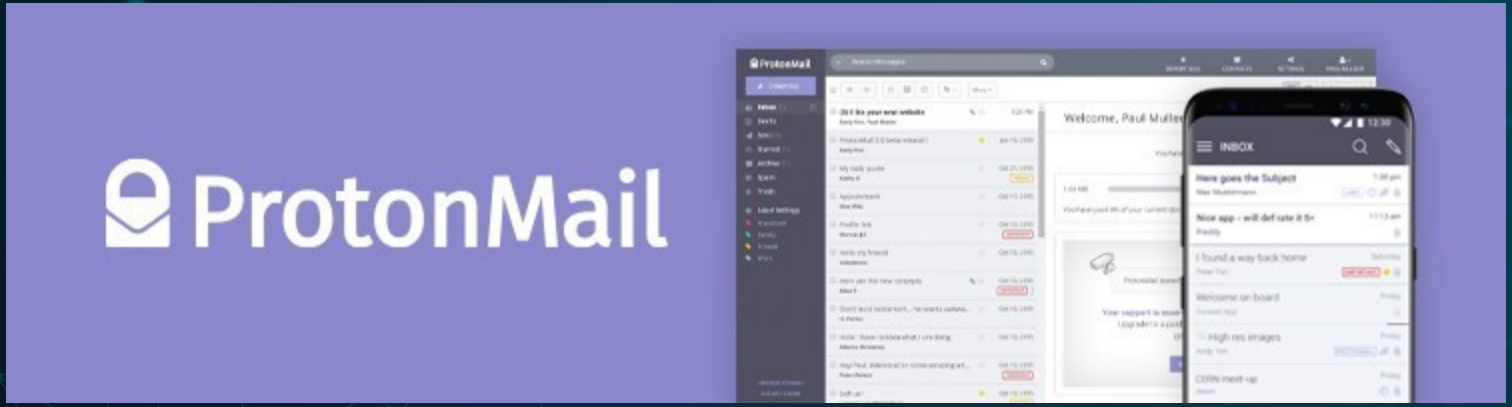
- Virustotal (analyze files & URLs to detect types of malware)
- urlvoid.com
- https://safeweb.norton.com/
- https://scanurl.net/
- https://www.phishtank.com/ (Phishing link checker)
- https://www.psafe.com/dfndr-lab/
- https://transparencyreport.google.com/safe-browsing/search

"the results are captured by Google's web crawlers and inform you if the site can be trusted."

TOP 5 SECURE MAIL PROVIDERS

2 **Email Security**

1. ProtonMail - best ratio between price and privacy



Pros

No-logs policy
Encrypted messages to anyone CSV contact import
Self-destructing emails Over 20 account languages

2. CounterMail - strongest security features

Pros

Anonymous payment
Security-first
RAM-only servers
MITM-attack protection
Safebox storage

3. Tutanota - Best secure email for any device

Pros

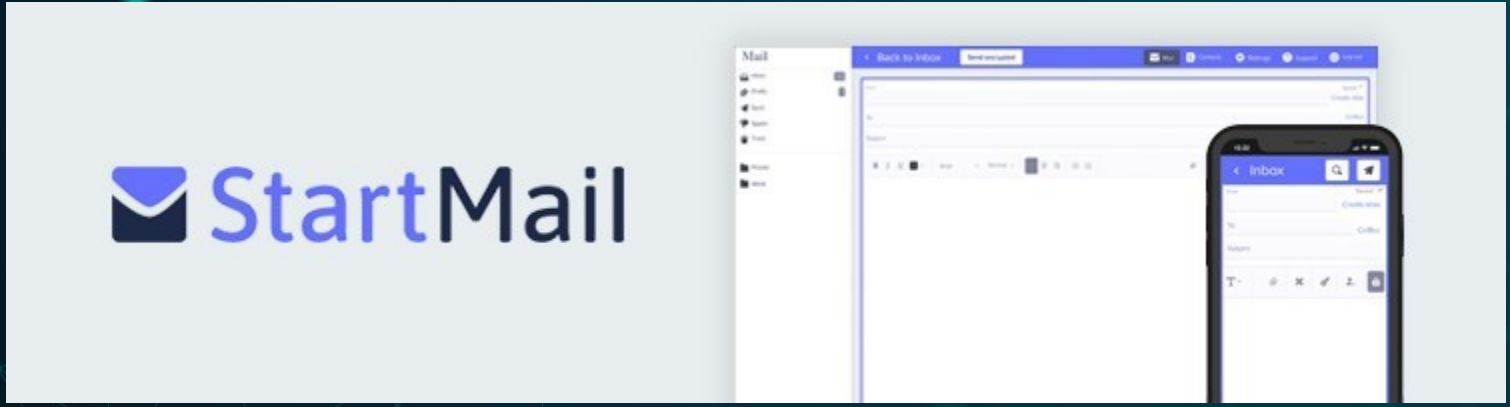
Cheap

No-logs policy Spam filter

20+ supported languages

Encrypted calendar

4. Startmail – best email for desktop-only users



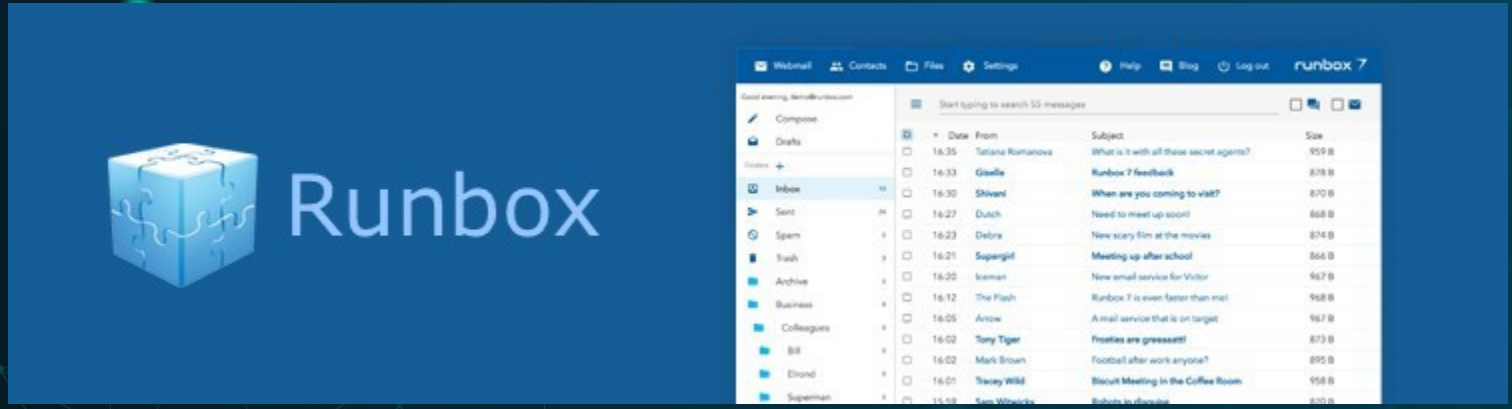
Pros

Supports PGP

Can add multiple aliases IMAP/SMTP support

10 GB of encrypted cloud storage

5. Runbox – private email service with a lot of quality of life features



Pros

Accepts cryptocurrencies

SMTP/POP/IMAP support No ads

Intuitive UI

2 **Email Security**

WHAT TO DO IF YOUR EMAIL IS HACKED ?

1. Run a Quick Recovery check
2. Check your recent email activity to see if anything was sent that you were not aware of
3. Change your password
4. Commit to Multi Factor Authentication
5. Use different passwords for every account
6. Start using a password manager to generate random, complex passwords
7. Update your system to the latest OS and update your security software
8. Change Your Security Question
9. Run your antivirus and malware detection programs

For further protection from email hacks, it's advisable to make use of temporary mails for online registration and otp confirmation on unimportant or non trusted sites and form fills.

Temporary Mails - No Login Required

http://www.20minutemail.com/ https://burnermail.io/
http://www.yopmail.com/en/ https://tempmailo.com/
https://www.guerrillamail.com/ https://getnada.com/ http://temp-mail.org/ https://maildrop.cc/ http://www.e4ward.com/
http://www.throwawaymail.com/ https://mytemp.email/
https://tempemailco.com/

3 Mobile Security

Tips you can use to prevent your phone from being hacked:

1)Avoid sharing passwords with friends or family
2)Avoid using the same passwords for all devices and accounts.
3)Do not open links or download attachments sent in text messages and emails without checking or confirming the source.
4)Install anti-malware software on your devices.
5)Regularly check the applications installed on your phone and remove suspicious ones
6)Ensure you have your 2fa fixed for your iCloud and all online accounts.
7)Regularly update the applications and OS of your phone.
8)Avoid connecting your device to a public Network or Wi-Fi without using a VPN.
9)Avoid visiting unsecured sites

CONCLUSION

- Cryptocurrency and blockchain technology is vital in the fight against digital fraud.
- Tools exist, but must be combined with policy and human capacity
- The future of finance requires proactive fraud detection

THANKS!

Do you have any questions?

www.cyesec.com.ng
+2347036740799