STAYING SAFE
IN THE DIGITAL AGE

"The prudent see danger and take refuge, but the simple keep going and pay the penalty."

— PROVERBS 22:3

Presented by Philemon Hini | philemon@keyrios.com

WHAT WE'LL COVER TODAY

1. **The Threat Landscape**
   Ghana fraud stats and top 8 threats

2. **Social Engineering**
   Manipulation, urgency, impersonation

3. **Mobile Money Fraud**
   MoMo scams, SIM swap, OTP theft

4. **ATM & Banking Safety**
   Skimmers, card cloning, safe habits

5. **Bank & Identity Fraud**
   Ghana Card scams, forgery, insider fraud

6. **Passwords & 2FA**
   Strong passwords, two-factor authentication

7. **Safe Online Behaviour**
   Phishing links, fake sites, downloads

8. **Crypto & Investment Scams**
   Ponzi schemes, fake platforms

THE THREAT IS REAL

Cyber fraud is rising sharply across Ghana. These numbers affect real people — including our church community.

Business News of Wednesday, 8 October 2025 **Source:** www.ghanaweb.com

Ghana lost over GH¢19 million to cybercrimes in first 9 months of 2025

« Prev | Next » | Comments (2) | Listen to Article Share:

Nearly half of all reported cases this year were linked to online fraud

The Cyber Security Authority (CSA) has disclosed that Ghana has lost over GH¢19 million to cybercrime between January and September 2025.

According to the Senior Manager at the Authority, Isaac Socrates Mensah, the figure reflects a troubling rise in online criminal activity, with online fraud emerging as the most widespread threat.

Speaking at a cybersecurity awareness event organised by the Financial Intelligence Centre and the CSA on Wednesday, October 8, 2025, he explained that nearly half of all reported cases this year were linked to online fraud.

Other forms of cybercrime included shopping scams, fake loan offers, romance and

Source: ghanaweb.com · 8 October 2025

GHS 20M+ — In cyber fraud losses reported in Ghana annually

MOBILE MONEY — A significant share of reported fraud cases

WIDESPREAD — Many Ghanaians report scam attempts on mobile and online channels

⚠ *These aren't just headlines — they're our neighbours, friends, and family members.*

THE 8 THREATS EVERY USER MUST KNOW

Phishing & Smishing

Fake emails, SMS and WhatsApp links stealing your login

Social Engineering

Tricks that manipulate you into sharing PIN, OTP or data

Romance & Investment Scams

Fake relationships and 'too good to be true' returns

Account Takeover

SIM swap, stolen passwords, hijacked WhatsApp

Online Shopping Scams

Fake vendors, non-delivery, counterfeit goods

Fake Apps & Links

Malicious apps, fake websites, spoofed login pages

Identity Theft

Stolen Ghana Card details used to commit fraud

Payment Card Fraud

Card skimming, cloning, unauthorised charges

⚠ **These threats all start with ONE person being tricked — that person could be you.**

01

SECTION 01

Social Engineering

How scammers manipulate people using psychology, not technology

COMMON SOCIAL ENGINEERING TACTICS

Social engineering is when a scammer tricks you into giving away information or money — by exploiting your trust, fear, or kindness rather than hacking your device.

Creating Urgency

1

"Your account will be blocked in 10 minutes!" — Pressure stops you from thinking clearly.

Impersonation

2

Posing as a bank official, MTN agent, pastor, or government worker to gain your trust.

Pretexting

3

Inventing a convincing story ("I'm verifying your account") to extract sensitive details.

Phishing Messages

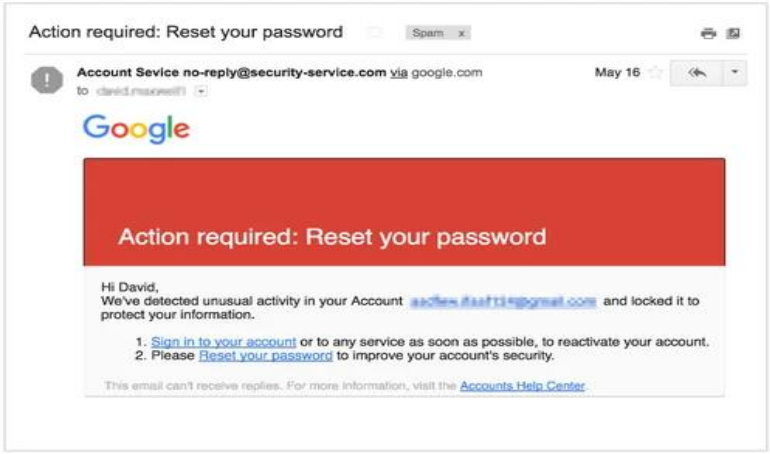
4

Fake SMS, WhatsApp or email with a link designed to steal your login credentials.

SOCIAL ENGINEERING

Two Faces of the Same Trick

PHISHING EMAIL



Fake "reset password" email pressures you to click before thinking

WHATSAPP TAKEOVER

Scammers steal your WhatsApp by tricking you into sharing the 6-digit code

Both attacks rely on trust and urgency — slow down, verify before you click, tap, or share a code.

WHATSAPP ACCOUNT TAKEOVER — THE 6-DIGIT CODE SCAM

WhatsApp Message

"Hi, sorry, I accidentally sent you a 6-digit code via SMS. Can you forward it to me? It's urgent! 🙏"

⚠ THIS IS A SCAM — DO NOT FORWARD THE CODE

WHAT HAPPENS NEXT

- You are completely locked out of WhatsApp
- Scammer messages your family & church contacts as 'you'
- They claim to be in emergency and beg for MoMo transfers
- Contacts lose money before realising it was not you

HOW THE ATTACK WORKS — STEP BY STEP

1. **Code arrives on YOUR phone —**
   WhatsApp sends a 6-digit login code to your number as a real SMS.
2. **Scammer asks you to forward it —**
   A message arrives claiming it was sent 'by mistake.' It may even look like a trusted contact.
3. **You share the code —**
   The moment you send it, the scammer uses it to log into your WhatsApp from their device.
4. **Your account is hijacked —**
   You are locked out. The scammer now controls your account, contacts, and profile photo.

PREVENTION & RECOVERY

- NEVER share any 6-digit code with anyone — not even a 'friend'
- Enable WhatsApp 2-Step Verification: Settings → Account → Two-Step Verification
- If taken over: email support@whatsapp.com immediately to recover your account
- Warn your contacts via call/SMS/Facebook so they don't send money to the scammer

The 6-digit code is your KEY — sharing it is the same as handing someone your house keys.

02

SECTION 02

Mobile Money Fraud

MoMo scams, SIM swap attacks, and OTP theft in Ghana

HOW MOBILE MONEY SCAMS WORK

1

Fake Agent / Wrong Transfer

- Caller claims to have sent money to you by mistake
- Asks you to 'refund' via MoMo
- No money was actually sent — it's a trick
- Alternatively pretends to be an MTN/Telecel agent

2

SIM Swap Fraud

- Scammer convinces your network to transfer your SIM
- They receive all your calls & OTP messages
- Can access your MoMo & bank accounts
- Often done with your stolen personal details

3

OTP / PIN Theft

- Scammer calls pretending to be from your network
- Claims to 'verify' or 'upgrade' your account
- Asks for the code sent to your phone (OTP)
- That code gives them full access to your wallet

REAL FRAUD CASES — HOW SCAMMERS OPERATE (1 & 2)

MO 1: Fake MoMo Screenshot Scam

HOW IT WORKS

- Scammer shows a fake MoMo payment screenshot via WhatsApp or in person
- Vendor releases goods/services before receiving the official network SMS
- No real money ever arrives — the wallet balance never changed
- Often uses a rider/dispatch to collect goods quickly and disappear

PREVENTION

ALWAYS wait for the official SMS from MTN/Telecel before releasing goods. Verify balance via *170# (MTN) or *110# (Telecel). A screenshot is NOT proof of payment.

MO 2: Wrong Transfer / Reversal Scam

HOW IT WORKS

- Caller claims to have 'mistakenly' sent a large sum to you
- They plead urgently for you to send it back ('my mother is sick / I'll lose my job')
- Moments later a real USSD authorisation prompt appears on your phone
- If you approve or follow their instructions, real funds leave your account

PREVENTION

NEVER act on calls asking you to return money. Check your real balance yourself via USSD. Only your network can reverse a genuine wrong transfer — not you.

GOLDEN RULES FOR MOBILE MONEY SAFETY

NEVER share your PIN or OTP

No legitimate MTN, Telecel, or AirtelTigo agent will ever ask for your PIN or OTP. Hang up immediately.

NEVER 'refund' a wrong transfer

Call your network's official line to verify before doing anything. Genuine mistakes are handled by the operator.

NEVER click unknown MoMo links

Scam websites mimic official MoMo portals. Only use the official app or USSD (*170# for MTN, *110# for Telecel).

Report suspicious calls instantly

Report to MTN: 100 | Telecel: 200 | AirtelTigo: 444. Also report to the Cyber Crime Unit: 18555.

SECTION 03

ATM & Banking Safety

Protecting yourself at the ATM and on your banking app

03

BANK FRAUD MO 1 — ATM CARD SKIMMING

BANK MO 1: ATM / Card Skimming & Cloning

HOW IT WORKS

- Skimming devices on ATM slots or handheld readers at POS capture card data
- Hidden camera or fake keypad records your PIN
- Card is cloned; rapid cash withdrawals or online purchases follow

PREVENTION

Shield your PIN. Inspect the slot. Enable SMS alerts.

REAL DEVICE

A skimmer clipped over the real card slot — almost invisible to a quick glance.

SECTION 03b

Bank & Identity Fraud

Ghana Card scams, ATM cloning, forgery, and insider fraud — what the data shows

03b

MO 5: GHANA CARD LINKING / IMPERSONATION SCAM

HOW THIS SCAM WORKS — STEP BY STEP

1. **Fake SMS arrives**
   "Your Ghana Card must be linked to your bank account for security. An agent will call you." — Looks official.
2. **Professional call follows**
   A scammer calls immediately, posing as a bank or MTN agent ready to 'assist with the linking process.'
3. **PII is requested**
   They ask for: Ghana Card number, date of birth, bank account/card number, card expiry, CVV, and the OTP sent to your phone.
4. **Accounts are hijacked**
   With your details they link your Ghana Card to a fraudulent wallet, take over existing accounts, or open loans in your name.
5. **Money disappears fast**
   Funds are transferred via MoMo wallets, layered rapidly, and withdrawn before you notice. Reversals are nearly impossible.

PREVENTION CHECKLIST

- Banks/telcos NEVER call to ask for your Ghana Card number, CVV, or OTP
- Hang up — call your bank's official number from the back of your card
- Verify 'linking' requests in the official app or at a branch only
- Enable daily transaction alerts to catch unauthorized activity fast

"The Ghana Card is a powerful protection — but it becomes a weapon when its details are shared carelessly."

STAYING SAFE AT THE ATM & WITH BANKING APPS

ATM SAFETY

- ✓ Shield keypad with your hand when entering PIN
- ✓ Check for card skimmer devices on the slot
- ✓ Use ATMs in well-lit, busy locations
- ✗ Never accept 'help' from strangers at ATM
- ✗ Never share card details or PIN via phone/SMS

BANKING APP SAFETY

- ✓ Only download banking apps from official app stores
- ✓ Enable login notifications / transaction alerts
- ✓ Always log out after using the banking app
- ✗ Never use public Wi-Fi for banking transactions
- ✗ Never save your password in the browser

04

SECTION 04

Passwords & Account Security

How to create strong passwords and enable 2-Factor Authentication

CREATING STRONG PASSWORDS

✗ WEAK PASSWORDS (Avoid these!)

- `123456`
- `password`
- `kofi2000`
- `church123`
- `ghana2026`

✓ STRONG PASSWORD TIPS

- At least 12 characters long
- Mix of UPPERCASE & lowercase
- Include numbers e.g. 7, 23
- Include symbols e.g. @, #, !
- Use a passphrase: "God_Saves_ME_2025!"

Use a different password for each account — especially your email, bank, and MoMo app.

TWO-FACTOR AUTHENTICATION (2FA) — YOUR EXTRA LOCK

2FA adds a second layer of protection. Even if someone steals your password, they still cannot get in without your phone.

1

Enter your password

You log in to your account with your username and password as usual.

2

Receive a one-time code

A 6-digit code is sent to your phone via SMS or an authenticator app.

3

Enter the code to get in

Only someone with both your password AND your phone can log in.

Enable 2FA on: WhatsApp · Facebook · Gmail · Your bank app · MoMo wallet

05

SECTION 05

Safe Online Behaviour

Spotting scam links, fake websites, dangerous downloads & romance fraud

SPOTTING SCAM LINKS & ONLINE THREATS

RED FLAGS — STOP & DON'T CLICK

- Link asks for your PIN, password or OTP
- "You have won GHS 5,000! Claim now!"
- URL looks odd: g00gle.com, m-t-n.gh.site
- Message creates URGENCY or FEAR
- Sent via WhatsApp, not official website
- Asks you to share with 10 friends to qualify
- Sends a photo of your Ghana Card, passport, or driver's licence
- Asks for voice notes or short videos of you — even casual ones

✓ SAFE HABITS TO PRACTISE

- Verify links before clicking — type the address yourself
- Official sites end in .gov.gh or .com — check carefully
- Never download apps from links in WhatsApp messages
- If in doubt, ask a trusted family member or friend
- Use Google to look up the real contact of any company
- Screenshot & report scam messages to Cyber Crime Unit
- Never share a photo of your Ghana Card — name, DOB, and ID are all on it
- AI can clone your voice from 10 seconds of audio — limit what you post

06

SECTION 06

Crypto & Investment Scams

Recognising fake investment platforms and Ponzi schemes

INVESTMENT SCAM RED FLAGS

Guaranteed high returns

"Double your money in 7 days!" No legitimate investment can guarantee huge returns. If it sounds too good to be true — it is.

Pressure to recruit others

Schemes where you must bring in friends & family to earn are classic Ponzi/pyramid structures. You will likely lose everything.

Unregistered platforms

Always check with the Securities & Exchange Commission (SEC Ghana) at sec.gov.gh before investing. Unregistered = illegal.

Crypto "opportunities"

Fake celebrities promote bogus crypto coins on social media. Once you invest, the scammer disappears with your money ('rug pull').

Remember: God's blessing does not come through schemes that exploit others. Be wise with what He has given you.

DATA PRIVACY & MOBILE SECURITY

Screen Lock

Always lock your phone with a PIN, fingerprint, or face ID. Set auto-lock to 30 seconds. Your phone is a digital wallet — protect it.

App Permissions

Review what apps can access: camera, contacts, location, SMS. A torchlight app does NOT need your contacts. Revoke unnecessary access.

Software Updates

Install Android/iOS updates promptly. Updates fix security holes. Scammers exploit outdated software to access your phone.

Public Wi-Fi Risks

Never do banking or MoMo transactions on public Wi-Fi (cafes, churches, markets). Use your mobile data for financial transactions.

YOUR 5-POINT ACTION PLAN

Do these 5 things this week — they can save you from losing your savings.

1. **Change your MoMo & bank PIN**

   Use a unique PIN that nobody can guess. Don't use your birthday or 1234.

2. **Enable 2FA on WhatsApp & email**

   Settings → Account → Two-Step Verification. Takes 2 minutes.

3. **Set a screen lock on your phone**

   Settings → Security → Screen Lock. Enable fingerprint or PIN.

4. **Save official fraud hotlines in your phone**

   MTN: 100 | Telecel: 200 | Cyber Crime Unit: 18555 | Bank of Ghana: 0800-111-4898

5. **Share this with your family today**

   Show your parents, spouse, and children. Warn them about MoMo scam tactics.

HOW TO REPORT CYBER FRAUD IN GHANA

Ghana Cyber Crime Unit

Call: 18555
Email:
cybersecurity@police.gov.gh
Report online:
cybercrime.ghanapolice.info

Bank of Ghana

Toll-free: 0800-111-4898
Email:
fraudreport@bog.gov.gh
For banking & fintech fraud

Network Operators

MTN: 100 | Telecel: 200 |
AirtelTigo: 444
For SIM swap, MoMo fraud
& account theft

Always take a screenshot of the scam message before reporting it. This helps investigations.

Questions & Discussion

Thank you for your time and attention.

”…Be as shrewd as snakes and as innocent as doves." — Matthew 10:16