DIGITAL SAFETY HUB

with Abinyoh

SCAM-PROOF

PLAYBOOK

Your complete step-by-step guide to staying safe online

No Tech Language • Real Examples • Step-by-Step Guides

Welcome to the Scam-Proof Playbook

This playbook was created for one reason: to protect everyday people from scammers.

You do not need to be a tech expert. You do not need special tools. Everything in this guide is written in plain language with real examples — the kind of thing a trusted friend would explain to you over coffee.

Scammers are professional criminals. They are not targeting stupid people — they are targeting everyone. Smart people, careful people, educated people lose money to scams every day. It is not your fault. But it is in your power to make yourself a much harder target.

How to use this playbook:

1. Read the 5 Golden Rules first — they protect you from 90% of all scams.

2. Work through each section and tick the checkboxes as you go.

3. Share this with your family, friends, and anyone you care about.

4. Keep it somewhere easy to find — return to it whenever something feels suspicious.

★★★★★

I forwarded this to my entire WhatsApp contact list. Three people called me the same day to say they had nearly fallen for exactly the scams described.

A

Amara K.

Accra, Ghana

✓ Verified

What Is Your Scam Risk Score?

Answer 5 questions honestly — then check your score below

Circle or tick ONE answer per question. Add up your points at the end.

Question 1

Circle ONE answer · Add up your points

You get a WhatsApp from an unknown number: 'Hi Mum, I broke my phone, this is my new number. I need $300 urgently. Don't call my old number.' What do you do?

- **A** Send the money — my child might really need help [3 pts]
- **B** Ask them questions over chat to check it's really them [2 pts]
- **C** Call my child's OLD saved number to verify [1 pt]
- **D** ✓ **BEST ANSWER** Ignore it — I would never send money without a voice or video cal [0 pts]

✓ **Correct answer: D**

The right answer is D. Calling the real saved number is the only way to confirm identity. A message alone — no matter how personal it sounds — is never enough proof to send money.

Question 2

Circle ONE answer · Add up your points

An email says your Gmail account will be deleted in 24 hours unless you click a link and verify. What do you do?

- **A** ✓ **BEST ANSWER** Delete the email — Google never sends threats like this [0 pts]
- **B** Reply to the email asking if it is real [2 pts]
- **C** Go directly to gmail.com myself and check my account [1 pt]
- **D** Click the link immediately — I don't want to lose my email [3 pts]

✓ **Correct answer: A**

The right answer is A. Google never threatens account deletion with a 24-hour deadline. If worried about your Gmail, go directly to gmail.com yourself — never through a link in an email.

Question 3

Circle ONE answer · Add up your points

You are at a mall and connect to the free Wi-Fi. You then open your banking app. Is this a problem?

- **A** No — free Wi-Fi is the same as home Wi-Fi [3 pts]
- **B** Maybe, but I will be quick so it should be fine [2 pts]
- **C** ✓ BEST ANSWER
  Yes — I never open my banking app on public Wi-Fi [0 pts]
- **D** I am a bit unsure — I will look into it later [1 pt]

✓ **Correct answer: C**

The right answer is C. Public Wi-Fi can be monitored by anyone on the same network including fake hotspots. Being quick does not reduce the risk. Always switch to mobile data for banking.

Question 4

Circle ONE answer · Add up your points

A stranger on Instagram has been messaging you for 3 weeks. They are kind and romantic. Now they say they are in trouble and need money via bank transfer. What do you do?

- **A** Help them — we have built a real connection over these weeks [3 pts]
- **B** ✓ BEST ANSWER
  Block and report immediately — this is a romance scam [0 pts]
- **C** Ask for more details and proof before I decide [2 pts]
- **D** Tell a family member and ask their opinion first [1 pt]

✓ **Correct answer: B**

The right answer is B. Scammers invest weeks or months building trust specifically so sending money feels correct. Asking for proof will produce convincing fake documents. Block first, then report.

Question 5 Circle ONE answer · Add up your points

Do you use two-step verification (2FA) on your email and WhatsApp?

- **A** No — I have never heard of it [3 pts]
- **B** I think I do but I am not really sure [2 pts]
- **C** On some accounts but not all of them [1 pt]
- **D** ✓ **BEST ANSWER** Yes — all my important accounts have it turned on [0 pts]

✓ **Correct answer: D**
The right answer is D. Two-step verification (2FA) is one of the most powerful protections available. Even if a scammer steals your password, they still cannot get in without the code sent to your phone.

My Total Score: ________ / 15 points

What does your score mean?

0 – 3 points
WELL PROTECTED
You already have strong instincts against scams. Complete the full checklist to close any remaining gaps — then share this playbook with everyone you love.

4 – 8 points
SOME RISK AREAS
You are doing some things right, but there are gaps scammers could exploit. Work carefully through WhatsApp, Gmail Security, and Passwords sections.

9 – 15 points
HIGH RISK — ACT TODAY
You are currently vulnerable to several common scam types. Start with WhatsApp Privacy, then Gmail Security, then Passwords. Work through every section today.

Your Master Protection Checklist

Complete these actions once and you will be dramatically safer online. Tick each box as you finish it. Work through them in order.

GOLDEN RULES

[ ] **I have read and understood the 5 Golden Rules**

[ ] **I have shared the Golden Rules with at least one family member**

[ ] **My family has agreed on a secret safe word for emergencies**

WHATSAPP

[ ] **I have set WhatsApp groups to 'My Contacts' or 'Nobody'**

[ ] **I have set WhatsApp calls to 'My Contacts' only — strangers cannot call me**

[ ] **I have set my WhatsApp profile photo and info to 'My Contacts' only**

[ ] **I have turned on WhatsApp two-step verification (2FA)**

[ ] **I know never to share a 6-digit SMS code with anyone**

EMAIL & GMAIL

[ ] **I have turned on Gmail 2-Step Verification**

[ ] **I have checked 'Your devices' and removed unknown ones**

[ ] **I have removed unknown third-party apps from my Google account**

[ ] **I have added a recovery phone number and backup email to Gmail**

SOCIAL MEDIA

[ ] **I have set my Facebook personal info to 'Friends only' or 'Only me'**

[ ] **I have turned on Facebook two-factor authentication**

[ ] **I know how to reverse image search a suspicious profile photo**

[ ] **I understand that all celebrity giveaways online are fake**

PASSWORDS

[ ] **My email has a unique password used nowhere else**

[ ] **My bank app has a unique password used nowhere else**

[ ] **My social media accounts each have their own unique password**

[ ] **I have written my passwords in a private notebook kept safely at home**

PHONE & APPS

- [ ] **All my apps are updated to the latest version**
- [ ] **My phone's operating system is fully updated**
- [ ] **I have removed apps I have not used in the last 3 months**
- [ ] **I have reviewed app permissions and removed unnecessary ones**
- [ ] **I have set up Private DNS (dns.google) on my Android phone**

PUBLIC WI-FI

- [ ] **I never open my banking app on public Wi-Fi**
- [ ] **I always confirm the exact Wi-Fi name with staff before connecting**
- [ ] **I forget public Wi-Fi networks after leaving a location**

IF IT HAPPENS

- [ ] **I know to call my bank immediately using the number on my card**
- [ ] **I know to change my email password first if scammed**
- [ ] **I know the reporting site for my country (ecrime.ae / Action Fraud / FTC)**
- [ ] **I know that 'recovery scams' are a second scam — I will ignore them**

★★★★★

I shared it with my whole family on WhatsApp. My dad had no idea about the AI voice clone scam. We set up a family safe word the same evening. This should be mandatory reading.

P

Priya M.
London, UK

✓ Verified

★

The 5 Golden Rules

These cover 90% of all scams — read them first

Read these 5 rules. Remember them. Share them with everyone you love.

[ ] **1. If it feels urgent — SLOW DOWN**

Scammers always create panic. 'Act NOW or lose your account.' 'Send money in the next hour or your son is arrested.' Real banks, real governments, and real family members never demand you decide in minutes. The moment you feel rushed, that is your signal to stop, breathe, and call someone you trust. Urgency is the scammer's only real weapon — taking your time destroys it completely.

[ ] **2. Never send money to someone you have not met in person**

Gift cards, bank transfers, crypto, Western Union — it doesn't matter how they ask. If you have never physically met the person, do not send them money under any circumstances. Scammers build relationships over weeks or months before asking. No real emergency requires a stranger to send you money.

[ ] **3. Always verify by calling directly — using YOUR saved number**

Your bank calls about fraud? Hang up. Find the number on the back of your card and call that. Someone messages claiming to be your child? Call their real saved number. A link tells you to log in? Open the app yourself — never through a link someone sent you. This single habit stops almost every impersonation scam.

[ ] **4. If it sounds too good to be true — it is**

Free iPhone. Lottery you didn't enter. A job paying thousands a week from home. A celebrity giving away money. None of these exist. Real opportunities don't land in your inbox out of nowhere. Any message promising something amazing — especially if you need to pay a fee first — is a trap.

[ ] **5. Talk to someone before you act**

Scammers want you alone and in secret. 'Don't tell anyone — this is confidential.' Before clicking a link, sending money, or sharing personal information — tell a family member or close friend what's happening. Just saying it out loud often breaks the spell. The people who love you would far rather you call them.

WhatsApp Safety

Scams · Know the warning signs · Key settings

SCAM MESSAGE	REAL MESSAGE
Unknown number: 'Hi Mum, broke my phone, this is my new number. Need $400 urgently. Don't call old number.' ■ Urgency + unknown number + tells you NOT to verify + asks for money = SCAM	From saved contact: 'Hey Mum, it's me — I'll call you in 10 mins from a friend's phone.' ✓ No money request. Offers to call. No pressure to act immediately.

[ ] **Always call back on a saved number before sending money**
No matter how convincing the message, dial the real person's saved number yourself. If they answer and confirm it's real. If not, it was a scam. This one step stops the 'Hi Mum' scam completely.

[ ] **Never share a 6-digit code you receive by SMS with anyone**
When someone tries to steal your WhatsApp, they make WhatsApp send a code to your phone — then they call pretending to be support asking for that code. The moment you share it, your account is gone. WhatsApp will NEVER call and ask for a code.

[ ] **Block unknown people from adding you to groups**
Go to WhatsApp → Settings → Privacy → Groups → change from 'Everyone' to 'My Contacts'. Strangers can no longer add you to scam investment groups silently.

HOW TO: Stop strangers adding you to WhatsApp groups

1. **Open WhatsApp**
Find WhatsApp on your phone and tap it to open.

2. **Go to Settings**
Tap the three dots (Android) or 'Settings' tab (iPhone).

3. **Tap 'Privacy'**
Find and tap Privacy from the settings menu.

4. **Tap 'Groups'**
Scroll down until you see Groups and tap it.

5. **Select 'My Contacts' or 'Nobody'**
Change from 'Everyone' to My Contacts. Only people you know can add you to groups.

6. **Done — you are protected**
Strangers can no longer silently add you to scam groups.

Want the full step-by-step guides? The Premium Edition includes complete visual how-to guides for: turning on WhatsApp 2FA · stopping unknown callers · locking your profile photo · securing Gmail · setting up Private DNS · password creation · app updates · and more — with full explanations for every step.

Social Media Scams

Facebook · Instagram · Fake profiles · Romance scams

SCAM MESSAGE	REAL MESSAGE
Account created 2 weeks ago. Very attractive photos. Military officer or engineer 'working abroad.'	Account exists for years. Real photos over time. Mutual friends you actually know.
Messages you out of nowhere. Very romantic very quickly. Avoids video calls.	Happy to video call without hesitation. Has never asked for money.
■ New account. No mutual friends. Eventually asks for money or gift cards.	✓ Long history. Consistent. No financial requests.

[ ] **Reverse image search profile photos of strangers**

If someone you don't know sends a friend request, save their photo and go to images.google.com. Upload the photo and search. If it appears on many websites with different names, it is stolen. This takes 30 seconds and instantly reveals most fake profiles.

[ ] **Celebrity giveaways are always fake — 100% of the time**

No celebrity gives away money by contacting random followers. No real competition requires you to pay to claim a prize. Before sharing any giveaway, ask: can I find this confirmed on their official verified account?

[ ] **Check your Facebook privacy settings today**

Your public profile may show your birthday, phone number, home city, employer, and family members — all of which scammers use to impersonate you. Go to Settings → Privacy and set personal information to 'Friends only' or 'Only me.'

[ ] **Be careful with Marketplace — pay safely**

Warning signs: price far below market value, seller insists on bank transfer only, they claim to be overseas and will 'ship' the item, want payment before you see it in person. Always meet in public, inspect before paying, use payment with buyer protection.

Phone Call Scams

Fake banks · Government threats · AI voice clones

SCAM MESSAGE	REAL MESSAGE
'This is your bank's fraud department. We detected suspicious activity. To protect your account we need your card number and PIN right now.'	'We're calling about a blocked transaction. We will never ask for your PIN. Please call us back on the number on your card to discuss.'
■ Unsolicited. Urgent. Asks for card details. Real banks NEVER ask for your PIN.	✓ Asks YOU to call back. Never requests PIN or full card number.

[ ] **Hang up and call back on the official number**
If any caller claims to be your bank, police, or government — hang up. Find the official number yourself (on your card, their website, or a previous letter) and call that. Scammers can fake the phone number shown on your screen — this is called number spoofing.

[ ] **The government will never threaten you over the phone**
Police do not call demanding payment to avoid arrest. Tax authorities send letters, not threatening calls. Immigration services do not demand gift cards. If you receive a threatening call — hang up. This scam targets elderly people and immigrants.

[ ] **AI voice clones can sound exactly like your family — create a safe word**
AI can clone any voice from just a few seconds of audio. You may receive a call that sounds perfectly like your child or spouse saying they are in danger and need money urgently. Agree on a secret family safe word now. If a 'family member' cannot say it — hang up.

[ ] **Never allow remote access to your phone or computer**
'Tech support' calls asking you to install an app so they can fix a virus remotely are scams. That app gives them complete control — they can see your banking app and transfer money while you watch. Legitimate tech support does not call you unsolicited.

★★★★★

I nearly accepted a fake job offer that would have given scammers access to my bank account. This playbook has a whole section on exactly that scam. I shared it with everyone in my graduate program.

J

Jordan T.

Atlanta, USA

✓ Verified

■

Deepfakes & AI Scams

Fake videos · Cloned voices · AI-generated content

SCAM MESSAGE	REAL MESSAGE
Face looks blurry around edges. Mouth movement doesn't match words perfectly. Eyes don't blink naturally. Background flickers or looks too smooth. ■ Test: ask them to turn sideways or read a random word. A deepfake can't respond naturally.	Natural eye blinking. Consistent lighting. Can respond to unexpected questions. Comfortable turning head in any direction. Background makes sense. ✓ Genuine reactions. No lag. Natural imperfections. Happy to do surprise requests.

[ ] **Shocking videos of celebrities or leaders may be completely fake**

AI can put any words into any person's mouth convincingly. Before believing or sharing a shocking video — search the news on BBC, Reuters, or the person's official account. If it really happened, it will be widely reported. Sharing a deepfake makes you part of the scam.

[ ] **Real-time video calls can be faked too**

Warning signs: slight delay, unnaturally smooth skin, flickering at face edges, reluctance to turn sideways. Ask them to do something unexpected: wave with a specific hand, hold up a random number of fingers. Deepfakes struggle with spontaneous requests.

[ ] **Create a family emergency safe word right now**

Sit down with your family and agree on one secret word only you all know. Something random. If anyone calls claiming to be a family member in an emergency, they must say the safe word. If they cannot — hang up and call the real person on their saved number. Do this today.

Secure Your Accounts

Two-step verification for Gmail · WhatsApp · Facebook

What is two-step verification (2FA)? It is a second lock on your account. Even if a scammer steals your password, they still cannot get in without a code sent to your phone. Think of it as a deadbolt on top of your regular door lock. Takes 5 minutes. Stops most takeovers.

[ ] **Turn on 2FA for Gmail — do this today**
Your Gmail is the master key to all your other accounts — protect it first. See the full Gmail security guide in Section 3.

[ ] **Turn on 2FA for WhatsApp**
Settings → Account → Two-step verification → Enable. See the full guide in Section 2.

[ ] **Turn on Facebook two-factor authentication**
Facebook → Menu → Settings & Privacy → Settings → Security and Login → Use two-factor authentication → turn it on and choose SMS codes.

[ ] **Review which apps have access to your Google or Facebook account**
Go to Google account Security settings → Third-party apps with account access. Remove anything you don't recognise. Do the same in Facebook under Apps and Websites in Settings. Each unknown connection is a potential backdoor into your account.

[ ] **Check logged-in devices on all accounts**
On Gmail, Facebook, and WhatsApp you can see every device currently logged in to your account. If you see a device or location you don't recognise — remove it immediately and change your password.

★★★★★

A video of a famous journalist told me I was owed money from a government program. It looked completely real. I almost clicked the link. This playbook showed me exactly how to spot a deepfake — I now send it to every new person I meet at university.

L

Lucas M.
São Paulo, Brazil

✓ Verified

I Was Scammed — Do This Now

Your 60-minute action plan. Stay calm. Act fast.

You are not stupid. These are professional criminals who deceive millions of smart, careful people every single day. What matters now is the next 60 minutes. You can limit the damage. Follow these steps in order.

1 **Stop all contact with the scammer immediately**

Block their number, email, and social media profile right now. Do not try to get your money back through them — they will only scam you further with a fake 'recovery' promise.

2 **Call your bank right now if money was transferred**

Use the number on the back of your bank card. Tell them you have been scammed. Ask them to freeze or reverse the transfer. Banks can sometimes stop payments if contacted quickly enough.

3 **Change your passwords — starting with your email**

Your email first, then bank app, then social media. Change passwords from a device the scammer has never touched. Never reuse old passwords.

4 **Check if your WhatsApp or social accounts are still yours**

Log in and check for unfamiliar messages sent, login locations, or changed settings. If you can't log in, use the account recovery option with your backup email or phone.

5 **Tell a family member or trusted friend right now**

You need support — emotional and practical. Do not hide this out of shame. Scammers rely on victims staying silent. Telling someone is one of the bravest things you can do.

6 **Report it to the authorities — keep all evidence**

Save every message, screenshot, email, and transaction record. UAE: ecrime.ae or call 992 | UK: Action Fraud 0300 123 2040 US: reportfraud.ftc.gov | AUS: scamwatch.gov.au

7 **Watch out for 'recovery scams'**

Someone may contact you claiming they can recover your money for a fee. This is a SECOND scam. No legitimate service guarantees fund recovery. Ignore and report them.

You are already doing the right thing by learning how to protect yourself. Share this playbook with everyone you love — a friend who is protected is a friend who cannot be taken from you by scammers.

Share this playbook freely. Print it. Send it. It could save someone's savings — or their life.

Online Shopping Scams

Know the 3 red flags before you buy anything online

■ **Scam**

Price is 80% below market
No reviews or fake reviews
Only accepts bank transfer
No return address listed

✓ **Real**

Price is competitive, not extreme
Hundreds of verified reviews
Accepts card or PayPal
Clear returns & contact info

Red Flag 1 — Price too good to be true

If a product is 70-90% cheaper than everywhere else, the store is likely fake. Scammers use impossibly low prices to create urgency. Check the same product on 2-3 trusted sites first.

Red Flag 2 — No secure checkout

Before entering your card details check the web address starts with https:// and shows a padlock icon. If it says http:// only — leave immediately. Your card details are not protected.

Red Flag 3 — Untraceable payment only

Legitimate stores accept credit cards or PayPal — both have buyer protection. If a seller insists on bank transfer, Western Union, or crypto only, it is almost certainly a scam.

■■ **Always search the store name + 'scam' or 'review' on Google before buying from a site you** don't recognise.

QR Code Scams

One rule that stops every QR code scam instantly

■ Scam

QR code stuck over real one
Links to unfamiliar website
Asks for card details to proceed
Found in public places, parking meters

✓ Real

QR code printed directly on material
Links to known official website
No payment details requested upfront
Comes from trusted official source

The One Rule:

Before scanning any QR code — check if it is a sticker

Peel or scratch the corner. If it comes off — do not scan. Someone placed it there.

Never scan QR codes from strangers or unexpected messages

WhatsApp messages, emails, or texts containing QR codes asking you to verify your account or claim a prize are scams. Scan QR codes only when you initiated the interaction yourself.

After scanning — check the URL before tapping anything

When you scan a QR code your phone shows you the link first. Read it carefully. If it does not match the business name exactly — close it immediately without tapping.

■■ QR code scams are now in restaurants, parking meters, ATMs and public notice boards. Alway
s check before you scan.

Subscription Traps

The one habit that stops hidden charges before they start

■ Scam

'Free trial' — card required
Cancellation buried in settings
Charges begin after 3 days
No reminder email sent

✓ Real

Free trial clearly explained
Easy cancel in one click
Charges only after clear notice
Reminder email before billing

The Golden Rule — Always read what happens after the free trial

Every free trial that requires your card will charge you automatically when it ends. Before entering your card ask: How much? When? How do I cancel? If you cannot find clear answers — do not sign up.

Use a separate card or virtual card for free trials

Many banks offer virtual card numbers. Use one for free trials with a low spending limit. When the trial ends you simply delete the virtual card and no charge can go through.

Check your bank statement every month for unknown subscriptions

Look for small charges of $5-20 you do not recognise. Scammers charge small amounts hoping you will not notice. One unknown charge per month is $240 per year leaving your account silently.

■ Search your email inbox for 'subscription' and 'trial' to find services you may have forgo
tten about and are still paying for.