

DIGITAL SAFETY HUB

with Abinyoh

---



# SCAM-PROOF STARTER GUIDE

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

No Tech Language



Real Examples



Step-by-Step Guides

# What's Inside This Guide

Six essentials to get you protected today

## 1 The 5 Golden Rules

The foundation. Read this first.

---

## 2 What Is Your Scam Risk Score?

A 5-question quiz to find your gaps

---

## 3 Master Protection Checklist

Every setting to change, once

---

## 4 WhatsApp Safety

Scams, group settings, 2FA setup

---

## 5 Deepfakes & AI Scams

Fake videos, cloned voices, family safe word

---

## 6 I Was Scammed. Help!

Your 60-minute emergency action plan

---

**Want more?** The Premium Edition covers 61 pages across 11 complete sections, plus 5 exclusive bonus guides, at [getdigitalsafetyhub.com](https://getdigitalsafetyhub.com).

New free guides are published regularly too, covering social media scams, phone call scams, online shopping, and more, at [getdigitalsafetyhub.com/guides](https://getdigitalsafetyhub.com/guides)

# Welcome to the Scam-Proof Starter Guide

---

This guide exists for one simple reason: to protect everyday people from scammers.

You don't need to be a tech expert, and you don't need any special tools. Everything here is written in plain language with real examples, the kind of thing a trusted friend would walk you through over coffee.

Scammers are professional criminals, and they're not just targeting careless people. They target everyone. Smart, careful, educated people lose money to scams every day. That's not a reflection on you. What matters is that you now have the power to make yourself a much harder target.

## How to use this guide

1. **Start with the 5 Golden Rules.** They protect you from most scams on their own.
2. **Work through each section** and tick the boxes as you go.
3. **Share it** with your family and anyone you care about.
4. **Keep it somewhere easy to find**, and come back whenever something feels off.

What Is Your Scam Risk Score?

## ■ 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** Ask them to send a voice note to prove it's them [ 1 pt ]
- D** ✓ **BEST ANSWER**  
Call my child's old saved number to check it's really them [ 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 you're worried about your Gmail, go directly to gmail.com yourself, never through a link in an email.

What Is Your Scam Risk Score?

## 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, and some hotspots are fake. 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 right. If you ask for proof, they'll send convincing fake documents. Block first, then report.

What Is Your Scam Risk Score?

## 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'm 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 guide 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 the WhatsApp section and the checklist.

9 – 15 points

**HIGH RISK: ACT TODAY**

You are currently vulnerable to several common scam types. Start with the WhatsApp section, then work through the checklist 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'
- ☐ I have turned on 'Silence unknown callers' in WhatsApp
- ☐ 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, and I will ignore them

THESE COVER 90% OF ALL SCAMS

# The 5 Golden Rules

---

Read these five 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 gets arrested." Real banks, governments, and family members never demand you decide in minutes. The moment you feel rushed is exactly when you should stop, breathe, and call someone you trust. Urgency is the scammer's only real weapon, and taking your time destroys it completely.

## ❑ 2. Never send money to someone you haven't met in person

Gift cards, bank transfers, crypto, wire services. It doesn't matter how they ask. If you've never physically met the person, don't send them money, no matter the story. Scammers build relationships over weeks or months specifically so the request feels earned. No real emergency requires you to send money to a stranger.

## ❑ 3. Always verify by calling directly, using your own saved number

Your bank calls about fraud? Hang up, then call the number on the back of your card. Someone messages claiming to be your child? Call their real saved number. A link asks you to log in? Open the app yourself, never through a link someone sent you. This one habit stops almost every impersonation scam on its own.

## ❑ 4. If it sounds too good to be true, it is

A free iPhone. A lottery you never entered. A job paying thousands a week from home. A celebrity giving away money. None of it is real. Genuine opportunities don't land in your inbox out of nowhere, and anything that asks you to pay a fee first is a trap.

## ❑ 5. Talk to someone before you act

Scammers want you isolated. "Don't tell anyone, this is confidential." Before you click a link, send money, or share personal information, tell a family member or close friend what's happening. Saying it out loud often breaks the spell completely. The people who love you would always rather you called.

# WhatsApp Safety

| SCAM MESSAGE                                                                                                 | REAL MESSAGE                                                                               |
|--------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Unknown number: "Hi Mum, broke my phone, this is my new number. Need \$400 urgently. Don't call old number." | From saved contact: "Hey Mum, it's me, I'll call you in 10 minutes from a friend's phone." |
| Urgency + unknown number + tells you not to verify + asks for money = scam                                   | 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 sounds, dial the real person's saved number yourself. If they say they never sent it, it's a scam. This one step alone stops the "Hi Mum" scam completely.
- ☐ **Never share a 6-digit code you receive by SMS**  
When someone tries to steal your WhatsApp, they trigger a code to be sent to your phone, then call pretending to be support and ask you to read it back. 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, and change it from "Everyone" to "My Contacts." Strangers can no longer silently add you to scam investment groups.

## How to: Stop strangers adding you to WhatsApp groups

- Open WhatsApp** and tap the three dots (Android) or the Settings tab (iPhone).
- Tap Privacy**, then scroll down and tap Groups.
- Select "My Contacts."** Only people you know can add you now.

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, creating passwords, updating apps, and more.

# Deepfakes & AI Scams

| DEEPPFAKE SIGNS                                                                                                      | REAL VIDEO SIGNS                                                                                  |
|----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Face looks blurry around edges. Mouth movement doesn't quite match. Eyes don't blink naturally. Background flickers. | Natural blinking. Consistent lighting. Responds to unexpected questions. Turns their head freely. |

☐ **Shocking videos of celebrities or leaders may be entirely fake**

AI can now put convincing words into anyone's mouth. Before believing or sharing a dramatic video, check the news on a source like BBC or Reuters, or the person's own verified account. If it really happened, it will be reported. Sharing a deepfake makes you part of spreading it.

☐ **Real-time video calls can be faked too**

Watch for a slight delay, unnaturally smooth skin, or flickering around the face. Ask the person to do something unexpected, like waving with one hand or holding up a random number of fingers. Deepfakes struggle badly with spontaneous requests.

☐ **Set up a family safe word today**

Sit down with your family and agree on one word only you all know. Make it random enough that it would never come up by chance. If anyone calls claiming to be a family member in an emergency, they need to say it. If they can't, hang up and call the real person's saved number.

## YOUR 60-MINUTE ACTION PLAN

# I Was Scammed, Do This Now

---

You're not stupid. These are professional criminals who deceive millions of smart, careful people every 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 profile right now. Don't try to get your money back through them. They'll only scam you again with a fake "recovery" promise.
2. **Call your bank right away if money was sent.** Use the number on the back of your card. Tell them what happened and ask them to freeze or reverse the transfer.
3. **Change your passwords, starting with email.** Email first, then your bank app, then social media. Change them from a device the scammer has never touched.
4. **Check whether your accounts are still yours.** Look for messages you didn't send, unfamiliar login locations, or changed settings.
5. **Tell a family member or trusted friend right now.** Don't hide this out of shame. Scammers count on people staying silent.
6. **Report it and keep every piece of evidence.** Save every message, screenshot, and transaction record. UAE: [ecrime.ae](https://ecrime.ae) or call 992. UK: Action Fraud, 0300 123 2040. US: [reportfraud.ftc.gov](https://reportfraud.ftc.gov). Australia: [scamwatch.gov.au](https://scamwatch.gov.au).
7. **Watch out for "recovery scams."** Someone may contact you claiming they can get your money back for a fee. That's a second scam. Ignore them and report it.

Learning how to protect yourself is already the right move. Share this guide with everyone you love. Every person who knows the signs is one less person a scammer can trick.