HOW TO RECOGNISE AN ONLINE SCAM



A Practical Guide to Spotting Online Scams, Recognising Warning Signs, Protecting Your Money, and Avoiding Internet Fraud

SAM CHOO

How to Recognise an Online Scam
A Practical Guide to Spotting Online Scams, Recognising Warning Signs, Protecting Your Money, and Avoiding Internet Fraud

Author: Sam Choo
Publisher: Hope Publishing, Singapore

Copyright © 2026 Hope Publishing. All rights reserved.

No part of this publication may be reproduced, distributed, or transmitted in any form or by any means without prior written permission from the publisher, except for brief quotations permitted by applicable copyright law.

Disclaimer

This book is intended for general educational and informational purposes only. It does not constitute legal, financial, cybersecurity, or other professional advice.

Scam methods, technologies, laws, and reporting procedures vary across countries and may change over time. Although care has been taken to provide practical and accurate information, the author and publisher make no guarantee that the recommendations in this book will prevent every scam or financial loss.

Readers should independently verify important information and consult qualified professionals, financial institutions, or relevant authorities when necessary.

Any hypothetical examples are provided for illustration and do not describe actual individuals or incidents unless expressly stated.

The author and publisher accept no liability for losses or damages arising from reliance on the information in this publication, to the extent permitted by applicable law.

Email: samchoo@gmail.com

Website: https://payhip.com/samchoo

Contents

Introduction: Could This Be a Scam? 1

Part One: Understanding How Online Scams Work 4

Chapter 1: What Is an Online Scam? 6

Chapter 2: How Scammers Trick People 11

Chapter 3: The Warning Signs of an Online Scam 16

Part Two: Recognising Common Online Scams 20

Chapter 4: Phishing Emails, Text Messages, and Fake Links 22

Chapter 5: Fake Websites and Online Shopping Scams 27

Chapter 6: Bank, Government, and Company Impersonation Scams 33

Chapter 7: Investment and Cryptocurrency Scams 38

Chapter 8: Job, Business Opportunity, and Easy-Money Scams 44

Chapter 9: Social Media, Messaging, and Online Friendship Scams 49

Part Three: The New Generation of Online Scams 55

Chapter 10: AI Scams, Deepfakes, and Fake Voices 57

Chapter 11: Malicious Apps, Remote Access, and Tech Support Scams 62

Part Four: Protecting Yourself Before a Scam Happens 67

Chapter 12: How to Check Whether Something Is a Scam 69

Chapter 13: How to Protect Your Money and Personal Information 74

Part Five: Responding to Scams and Staying Safe 80

Chapter 14: What to Do If You Have Been Scammed 82

Chapter 15: How to Stay Scam-Aware in a Changing Digital World 87

Conclusion: Your Best Protection Is Knowing When to Stop 93

Appendix A: The 30-Point Online Scam Warning Signs Checklist 96

Appendix B: How to Verify a Suspicious Message, Website, or Offer 99

Appendix C: What to Do in the First 30 Minutes After a Scam 102

Appendix D: 25 Common Scam Terms Explained in Simple English 105

Appendix E: 20 Everyday Online Scam Scenarios 108

Introduction: Could This Be a Scam?

Your mobile phone makes a familiar sound. A message has arrived.

It appears to be from a delivery company. According to the message, a parcel cannot be delivered because your address is incomplete. You are asked to click a link and update your details. There is a small delivery fee to pay.

You are expecting a parcel, so the message seems reasonable. The company's name looks familiar. The link appears professional. You might even recognise the logo.

You are about to click when a thought crosses your mind.

Could this be a scam?

That simple question could save you from losing money or revealing personal information to a criminal.

Online scams have become part of everyday life. They appear in emails, text messages, social media advertisements, shopping websites, and messaging applications. Some involve strangers offering attractive

investments. Others involve people pretending to represent banks, government agencies, or well-known companies.

Many scams are carefully designed to resemble ordinary transactions and communications.

A fraudulent website may look almost identical to a genuine one. A message may appear to come from someone you know. Criminals can even use artificial intelligence to imitate voices, create convincing photographs, and produce realistic videos.

Recognising a scam is becoming more challenging, particularly when everything appears legitimate.

Scammers understand how people behave. They know that someone expecting a delivery might respond quickly to a shipping notification. A person worried about a bank account might follow urgent instructions from someone claiming to be a bank officer. Someone looking for additional income might be attracted to an opportunity promising unusually high returns.

These situations involve ordinary human concerns. Scammers deliberately exploit them.

People sometimes assume that scam victims are careless, poorly educated, or unfamiliar with technology. This assumption is misleading. Professionals, business owners, young adults, and experienced internet users have all been deceived. Education and experience can help, but neither provides complete protection.

The good news is that many scams share recognisable warning signs.

Although criminals continually change their methods, their underlying tactics often remain similar. They create urgency, impersonate trusted organisations, make attractive promises, or persuade people to disclose information they would normally keep private.

Learning to recognise these patterns can make a meaningful difference.

This book will help you understand how online scammers operate and identify common forms of internet fraud. You will learn how to examine suspicious messages, recognise fraudulent websites, question unusual financial offers, and verify whether someone is genuinely representing an organisation.

You will also discover practical ways to protect your accounts, personal information, and money. If you have already encountered a scam, you will learn what steps to take and where to seek assistance.

You do not need technical knowledge to benefit from this book. The explanations are written in simple English, with everyday examples and practical advice.

As you read, remember one important habit.

Whenever someone unexpectedly asks you to click a link, share confidential information, transfer money, or make an urgent decision, stop and verify the request through a trusted, independent source.

You can enjoy the convenience of the internet while taking sensible precautions.

Your first line of defence begins with a simple question.

Could this be a scam?

Part One: Understanding How Online Scams Work

Every online scam begins with deception. Someone wants you to believe something that is untrue so that you will take an action that benefits them.

The deception may be simple, such as a fake message asking you to pay a small delivery fee. It may also be elaborate, involving false identities, convincing websites, and conversations that continue for weeks or months.

Understanding how scammers operate is one of the most useful ways to protect yourself.

Scammers often take advantage of ordinary human emotions and behaviour. They may create fear by claiming that your bank account is in danger. They may offer an attractive opportunity that seems too good to miss. Sometimes, they spend considerable time building trust before making their demands.

Their methods differ, but many rely on familiar patterns of manipulation.

In this first part, you will learn what online scams are, why people become targets, and how criminals influence their victims. You will also discover 15 common warning signs that can help you recognise suspicious situations before taking action.

The purpose is to develop your awareness and judgment. Once you understand the methods scammers use, you will be better prepared to recognise them, even when the messages, websites, and stories change.

The more you understand how deception works, the harder it becomes for someone to deceive you.

Chapter 1: What Is an Online Scam?

Understanding Internet Fraud and Why Anyone Can Be Targeted

> "The first step in avoiding a scam is understanding how deception works."

What Makes Something an Online Scam?

An online scam is a deliberate attempt to deceive someone through the internet or digital communication for financial gain or another dishonest purpose.

Imagine receiving an email informing you that you have won a valuable prize. To collect it, you must first pay a processing fee. You send the money, but the prize never arrives. The sender disappears.

The prize never existed. The message was designed to persuade you to part with your money.

Online scams can occur through websites, emails, social media, messaging applications, and online marketplaces. Some involve a single message. Others involve carefully planned conversations lasting weeks or months.

The common element is deception. Someone creates a false impression to persuade another person to do something they would otherwise avoid.

How Online Scams Differ From Ordinary Mistakes

Every disappointing online transaction is not necessarily a scam.

Suppose you order a shirt from an online store. When it arrives, the colour is different from what you expected. The seller may have made a genuine mistake.

If the seller refuses to provide a refund, you may have a consumer dispute. Whether fraud occurred depends on the circumstances and evidence.

Now imagine a website advertising expensive electronic products at unusually low prices. Customers pay, but no products are delivered. The website disappears, and the supposed company never existed.

This suggests deliberate deception.

The distinction matters because genuine businesses sometimes make mistakes, experience delivery problems, or provide poor service. Fraud involves dishonest conduct intended to mislead.

When something goes wrong, examine the available evidence before deciding what happened. If you suspect fraud, preserve transaction records and report your concerns through appropriate channels.

Why Scammers Target Ordinary People

Scammers do not need to know you personally to target you.

Criminals can send thousands of fraudulent messages using automated systems. Even if most recipients ignore them, a small number of successful attempts may generate money.

Some scams are more selective. Criminals may study public social media profiles, professional information, or online activities before approaching someone.

For example, a person who publicly announces that they are looking for employment may receive a fraudulent job offer. Someone discussing investments online may attract a scammer pretending to be a financial adviser.

Scammers also exploit circumstances shared by millions of people. Many people shop online, receive parcels, use banks, and communicate through messaging applications.

These ordinary activities provide opportunities for criminals to create believable stories.

Anyone who uses the internet can encounter a scam attempt.

The Different Things Scammers Want

Money is an obvious target. Scammers may request bank transfers, cryptocurrency payments, gift cards, or fees for services that do not exist.

However, money is only one possible objective.

Some criminals want passwords that allow them to enter email, shopping, or social media accounts. Others seek personal information, including identity numbers, addresses, banking details, or verification codes.

Such information may be used for further fraud or unauthorised account access.

Scammers may also persuade victims to install harmful applications or provide remote access to their computers and phones.

Once access is granted, criminals may attempt to steal information, interfere with accounts, or carry out unauthorised transactions.

A suspicious request for information deserves the same careful attention as a request for money.

Why Intelligent and Careful People Can Be Deceived

People often imagine that they would immediately recognise a scam. Unfortunately, deception can be convincing when it fits someone's circumstances.

A person worried about an elderly relative may react quickly to an emergency message. Someone expecting an important payment may trust a message appearing to come from their bank.

Scammers deliberately create situations that encourage emotional decisions.

Fear can make people act urgently. Trust can reduce suspicion. The hope of solving a financial problem can make an attractive offer seem believable.

These reactions are normal human responses.

Being educated, experienced, or familiar with technology does not eliminate the possibility of deception.

Understanding this helps us approach scam prevention with greater awareness and treat victims with respect.

What You Should Do

Develop one essential habit: independently verify unexpected requests before taking action.

If a message claims to come from your bank, contact the bank using its official application or a telephone number you obtained independently.

If someone claiming to represent a company requests payment, visit the company's official website yourself.

Avoid using contact details supplied in the suspicious message, since those details may lead directly to the scammer.

Whenever a request involves money, confidential information, or access to your device, give yourself time to check its legitimacy.

A few minutes of careful verification may prevent serious financial loss.

Understanding what scammers want and how they approach people is the foundation of protecting yourself online.

Chapter 2: How Scammers Trick People

The Psychology of Fear, Trust, Urgency, and False Promises

> "A scammer's greatest weapon is often the emotion that prevents someone from thinking clearly."

What Is Social Engineering?

Imagine receiving a telephone call from someone claiming to work for your bank. The caller sounds professional and knows your name. You are told that someone has attempted to withdraw money from your account.

The caller offers to help you protect your savings. All you need to do is follow a few instructions.

You feel worried. You want to act quickly.

This is how social engineering works.

Social engineering is the use of psychological manipulation to persuade people to reveal information, transfer money, or perform actions that benefit a scammer.

Instead of relying entirely on technical attacks, criminals exploit human behaviour. They study how people respond to authority, fear, trust, and attractive opportunities.

Understanding these methods helps you recognise manipulation before making a costly decision.

Creating Fear and Urgency

Fear is one of the most common tools scammers use.

You may receive a message claiming that your bank account has been compromised. Another message may warn that your online account will be suspended unless you verify your identity immediately.

Some criminals impersonate government officials and threaten legal action. Others invent emergencies involving family members.

These messages are designed to create emotional pressure.

When people feel frightened, they may concentrate on escaping the apparent danger rather than checking whether the warning is genuine.

Urgency makes the situation more difficult.

A scammer may insist that you must act within ten minutes or risk losing your savings. The deadline is often invented to prevent careful verification.

Legitimate emergencies can occur, but an unexpected demand for immediate payment or confidential information should always be independently checked.

Pretending to Be Someone You Trust

People naturally place confidence in familiar organisations and individuals.

Scammers exploit this by pretending to represent banks, government agencies, delivery companies, employers, or customer support departments.

They may use official-looking logos, convincing email addresses, or professional language.

Sometimes, criminals impersonate someone you know personally.

Imagine receiving a message from a friend's social media account requesting an urgent loan. The message explains that your friend has encountered an emergency and promises to repay you tomorrow.

You may feel comfortable helping because the request appears to come from someone familiar.

However, the account may have been taken over by a criminal.

A familiar name, photograph, or telephone number does not automatically prove someone's identity. Caller identification and sender details can sometimes be falsified.

Independent verification remains essential.

Using Greed, Hope, and Curiosity

Scammers also exploit people's hopes and desires.

Someone struggling financially may be attracted to an investment promising unusually high returns. A person seeking employment may respond to an offer of generous pay for simple online tasks.

Others receive messages claiming that they have won prizes, inherited money, or qualified for exclusive opportunities.

These promises can be persuasive because they offer something the recipient genuinely wants.

Curiosity creates another opening.

A message might say that someone has posted an embarrassing photograph of you. Another may claim that an important document is waiting for your attention.

The purpose is to encourage you to click a link before considering whether the message is trustworthy.

Attractive offers deserve careful examination, particularly when they arrive unexpectedly or require advance payment.

Building Trust Before Asking for Money

Some scammers are patient.

They begin with friendly conversations, helpful advice, or apparently harmless requests. Over time, they create the impression of a genuine relationship.

A fraudulent investment adviser may initially provide general financial information. Later, the adviser introduces an investment platform and encourages a small deposit.

The victim may even receive a modest payment or see apparent profits displayed online.

These early experiences can create confidence.

Once trust develops, the scammer may request larger payments, introduce additional fees, or create an unexpected financial emergency.

This gradual process can make deception difficult to recognise because each individual request may appear reasonable.

A history of pleasant conversations or small successful transactions does not establish that someone is trustworthy.

What You Should Do

Pay attention to your emotional reaction whenever someone asks you to make an important decision online.

If you suddenly feel frightened, excited, pressured, or unusually hopeful, give yourself time to examine the situation.

Ask why the person needs you to act immediately. Consider whether the request is consistent with what you know about the organisation or individual.

Verify unexpected claims using contact information obtained independently.

Avoid making financial decisions while someone is pressuring you to continue a conversation or complete a transaction.

You can also discuss suspicious requests with someone you trust. Another person may notice warning signs that are difficult to recognise when you are emotionally involved.

Scammers depend on influencing your decisions. Recognising that influence gives you an opportunity to regain control.

A calm decision, supported by independent verification, is one of your strongest protections against online fraud.

Chapter 3: The Warning Signs of an Online Scam

15 Red Flags That Should Make You Stop and Check

"A warning sign gives you a chance to check before you trust."

Scams come in many forms, but certain warning signs appear repeatedly. Learning to notice them can help you avoid dangerous decisions. The following 15 red flags are reasons to investigate, even when a message or offer initially seems convincing.

Unexpected Contact and Unusual Requests

1. Someone contacts you unexpectedly. A stranger sends a message about an investment, job, prize, or urgent problem. Unexpected contact alone does not prove fraud, but it deserves caution, especially when money or personal information is involved.

2. You are asked to keep the conversation secret. A caller tells you not to inform your family, bank, or colleagues. Secrecy can prevent others from questioning a dishonest story.

3. The person wants to move the conversation elsewhere. Someone you meet on a shopping platform quickly asks to communicate privately through another application. This may remove the protection or records provided by the original platform.

Pressure and Threats

4. You must act immediately. A message demands payment or verification within minutes. Artificial deadlines leave little time to check the claim.

5. You are threatened with serious consequences. Someone claims that you will be arrested, fined, or locked out of your account unless you obey. Verify such claims directly with the relevant organisation.

6. The person discourages independent checking. A supposed official becomes angry when you say you will call the organisation yourself. Attempts to prevent verification are a major warning sign.

Money and Payment Warning Signs

7. You must pay before receiving a promised benefit. A supposed prize requires a processing fee, or a job offer requires a deposit. Advance payments linked to unexpected rewards deserve scrutiny.

8. Payment must use an unusual method. A stranger insists on gift cards, cryptocurrency, or transfers to a personal account. These methods may make recovery difficult. The payment method should make sense for the transaction.

9. You are told to move money into a safe account. Someone claiming to represent your bank says your savings are at risk and must be transferred immediately. Contact your bank using its official number instead.

Identity and Website Warning Signs

10. A link leads somewhere unexpected. A message appears to come from a familiar company, but its website address contains unfamiliar words or a misleading spelling. Do not assume a page is genuine because it displays a company logo.

11. The person's identity cannot be verified. A caller claims to be an official but refuses to let you confirm their position through the organisation's published contact details.

12. Reviews or endorsements seem suspicious. A product or investment is promoted through glowing testimonials, celebrity photographs, or impressive-looking screenshots. Reviews can be fabricated, and images can be misused or manipulated.

Promises That Are Too Good to Be True

13. Profits are described as guaranteed. An investment promises unusually high returns without risk. Genuine investments involve uncertainty, and guaranteed-profit claims warrant careful investigation.

14. A bargain is unusually generous. An unfamiliar store offers an expensive product for a fraction of its normal price, particularly when payment must be made outside a trusted shopping platform.

15. You have won something you never entered. A message announces a lottery prize, inheritance, or special reward, then asks for your details or money. Unexpected rewards are a common way to attract attention.

What You Should Do

You do not need to identify several warning signs before taking precautions. One serious red flag, such as a demand to disclose a verification code or transfer savings urgently, is enough to stop the interaction.

Avoid clicking links or making payments while checking. Contact the organisation through its official application, a website address you enter yourself, or a number you have independently confirmed. If a friend requests money, contact them through a separate, familiar channel.

Remember that scammers can produce convincing messages without obvious spelling mistakes or suspicious-looking websites. Some fraudulent approaches contain none of the warning signs listed here at first. A polished appearance is never proof of legitimacy.

Treat these signs as prompts to investigate, and make independent verification your normal habit before sharing sensitive information or sending money.

Part Two: Recognising Common Online Scams

Online scams appear in many forms. Some arrive as unexpected emails or text messages. Others appear through shopping websites, social media platforms, investment advertisements, or offers of employment.

Although the methods differ, the underlying purpose is usually similar. Scammers want to persuade you to trust a false story, disclose valuable information, or take an action that benefits them.

The difficulty is that many fraudulent approaches resemble ordinary online activities.

You may receive a delivery notification while waiting for a parcel. A message claiming to be from your bank may arrive shortly after you have made a purchase. An online advertisement may offer a product you have been searching for at an attractive price.

These situations can make suspicious messages appear believable.

In this part, we will examine six common categories of online scams. You will learn how phishing messages attempt to steal personal information,

how fraudulent shopping websites deceive customers, and how criminals impersonate trusted organisations.

We will also explore investment scams, fake employment opportunities, and fraud involving social media and online friendships.

Each chapter will explain how the scam works, identify warning signs, and provide practical steps to help you protect yourself.

You do not need to memorise every possible scam. Criminals continually invent new stories and adapt familiar methods to changing circumstances.

What matters is learning to recognise the patterns behind these attempts.

Once you understand how common scams operate, you will be better prepared to question suspicious requests and make safer decisions when something unexpected appears on your screen.

Chapter 4: Phishing Emails, Text Messages, and Fake Links

How Scammers Steal Passwords, Banking Details, and Personal Information

"A convincing message deserves careful checking when it asks you to reveal something valuable."

What Is Phishing?

Phishing is a form of online fraud in which criminals pretend to be trustworthy individuals or organisations to obtain confidential information.

Imagine receiving an email from your bank warning that your account has been temporarily suspended. The message asks you to click a link and confirm your identity.

The email looks official. It contains the bank's logo and uses professional language. However, the sender is a criminal attempting to steal your banking details.

Phishing can arrive through several communication channels.

Email phishing uses fraudulent emails. SMS phishing, sometimes called smishing, uses text messages. Similar attacks occur through WhatsApp, Telegram, and other messaging applications.

The delivery method may differ, but the intention is often to persuade you to disclose information or visit a fraudulent website.

How Fake Messages Imitate Trusted Organisations

Scammers frequently impersonate organisations that people deal with regularly.

A fake delivery message may claim that your parcel cannot be delivered until you update your address or pay a small fee.

A fraudulent bank notification may warn about an unauthorised transaction and ask you to verify your account immediately.

Another message may appear to come from a government agency, claiming that you have an unpaid fine or an important document awaiting your attention.

These messages exploit familiar situations. Someone expecting a parcel may respond without questioning the delivery notification. A person worried about financial security may react quickly to a banking alert.

Criminals may copy logos, colours, and wording from genuine organisations to make their messages appear authentic.

The familiar appearance of a message does not establish that its sender is genuine.

How Fraudulent Links and Login Pages Work

Many phishing messages contain links that lead to fraudulent websites.

Suppose you receive a message asking you to update your banking password. Clicking the link opens a page that looks almost identical to your bank's official website.

You enter your username and password. The page may then request a one-time password, commonly called an OTP.

Unfortunately, the information is being collected by criminals.

An OTP is a temporary security code used to confirm certain account activities. If a scammer obtains it, the code may help them complete an unauthorised login or transaction.

Some fraudulent websites also request credit card numbers, identity details, or other confidential information.

A website can look professional and display a padlock symbol while still being fraudulent. The padlock generally indicates an encrypted connection, not that the business or website is trustworthy.

Warning Signs in Emails and Messages

Phishing messages often contain clues that something is wrong.

The sender's email address may differ from the organisation's genuine domain name. A domain name is the main address identifying a website, such as example.com.

A fraudulent message may contain a link with an unfamiliar spelling or additional words designed to resemble a legitimate address.

Unexpected attachments deserve caution because they may contain harmful software.

Be particularly careful when a message requests passwords, verification codes, banking details, or urgent payments.

However, spelling mistakes and awkward language are no longer reliable indicators. Criminals can produce polished messages that look convincing.

Even a message displaying a familiar sender name or telephone number may be deceptive because sender information can sometimes be falsified.

What If You Already Clicked?

If you have clicked a suspicious link, the next steps depend on what happened.

If you only opened a webpage without entering information or downloading anything, close the page. Keep your browser and device updated, and remain alert for unusual activity. Simply opening a page does not automatically mean your accounts have been compromised.

If you entered a password, change it immediately through the genuine website or application. Change it anywhere else you reused it, and enable additional account protection.

If you disclosed banking details or verification codes, contact your bank immediately using its official contact information.

If you installed an unfamiliar application or granted remote access, stop using the affected device for banking until it has been checked and secured. Use a separate trusted device to contact your bank.

Acting promptly can reduce further harm.

What You Should Do

Treat unexpected messages containing links or requests for confidential information with caution.

Instead of following the supplied link, open the organisation's official application or type its known website address directly into your browser.

If necessary, contact the organisation using a telephone number obtained independently.

Avoid opening unexpected attachments or sharing verification codes with someone who contacts you.

When a message claims that urgent action is required, verify the situation before responding.

Phishing succeeds when people trust a message without checking its source. Developing the habit of independent verification makes these attempts easier to recognise and avoid.

Chapter 5: Fake Websites and Online Shopping Scams

How to Identify Fraudulent Stores, Sellers, Advertisements, and Payment Requests

> "A good bargain becomes expensive when the seller never intended to deliver."

How Fake Online Stores Operate

Imagine finding an advertisement for a popular smartphone at half its usual price. The advertisement leads to an attractive online store with product photographs, customer reviews, and a professional-looking checkout page.

You place an order and make payment. Days pass, but the smartphone never arrives. Your messages go unanswered. Eventually, the website disappears.

You may have encountered a fake online store.

Fraudulent stores are websites created to collect payments or personal information without providing the advertised products.

Some scammers copy genuine retailers' websites. Others create entirely fictional businesses. Social media advertisements help them reach shoppers who may never have heard of their stores.

Fraud can also occur on legitimate marketplaces when dishonest sellers advertise products they do not intend to deliver.

Common Shopping Scam Tactics

One common tactic is offering expensive products at unusually low prices.

Scammers know that attractive discounts can encourage people to purchase quickly, particularly when the products are popular or difficult to obtain.

Another tactic is creating false scarcity.

A website may display messages claiming that only two items remain or that a special discount expires within minutes. These claims may be designed to discourage careful checking.

Some fraudulent sellers insist on advance payment through bank transfers or other methods offering limited buyer protection.

After receiving payment, they may disappear or demand additional money for delivery, insurance, or customs clearance.

Be especially cautious when a seller unexpectedly changes the agreed payment method or asks you to complete a transaction outside the shopping platform.

How to Examine a Website or Seller

Before purchasing from an unfamiliar store, examine its website address carefully.

Scammers sometimes use domain names that resemble established retailers, with additional words or slightly different spellings.

Look for clear business information, including a physical address, customer service details, and understandable return policies.

However, remember that these details can be invented or copied.

Search independently for information about the business. Look for reviews on established platforms and complaints from previous customers.

Check whether the seller has a meaningful transaction history. On online marketplaces, examine account age, customer feedback, and previous sales where such information is available.

A recently created account selling expensive products at unusually low prices deserves additional scrutiny.

You can also compare the advertised price with those offered by established retailers.

No single check guarantees that a seller is genuine. Several independent checks provide a stronger basis for deciding whether to proceed.

Why Reviews and Professional Designs Can Be Misleading

Many people judge an online store by its appearance.

Unfortunately, creating a professional-looking website has become relatively easy. Fraudulent stores can use attractive templates, convincing photographs, and familiar payment symbols.

Customer reviews are not always reliable either.

Scammers may fabricate testimonials, purchase favourable reviews, or copy comments from legitimate businesses.

Some fraudulent websites display photographs of satisfied customers who have never purchased anything from the store.

Even genuine-looking social media accounts can be misleading. Followers, likes, and comments may be artificially generated.

Look beyond the store's own promotional material. Independent evidence is more valuable than testimonials controlled by the seller.

Safer Ways to Pay Online

Your choice of payment method can affect your ability to recover money when something goes wrong.

Credit cards often provide mechanisms for disputing eligible fraudulent or undelivered purchases, although protections vary by country, card issuer, and circumstances.

Established shopping platforms may offer buyer protection when payments are completed through their approved systems.

Direct bank transfers to unfamiliar individuals can be particularly risky because recovering transferred funds may be difficult.

Be cautious when sellers request cryptocurrency, gift cards, or payments to unrelated personal accounts.

Avoid saving payment details on unfamiliar websites unless necessary.

Before paying, confirm the total amount, recipient, and payment conditions.

Remember that using a protected payment method reduces certain risks but cannot guarantee that every loss will be recovered.

What You Should Do

Develop a simple checking routine whenever you encounter an unfamiliar online seller.

First, compare the advertised price with established retailers. An unusually generous offer deserves investigation.

Next, examine the website address and look for independently verifiable business information.

Search for customer experiences outside the seller's own website. Check the seller's history if purchasing through a marketplace.

Choose a payment method that offers appropriate buyer protection, and keep the transaction within the platform whenever possible.

Save your order confirmation, payment receipt, and communications with the seller.

If something feels suspicious, delay the purchase until you have verified the business.

A genuine bargain should remain worthwhile after careful checking. Protecting your money is more important than securing a discount that may never have existed.

Chapter 6: Bank, Government, and Company Impersonation Scams

Recognising Fake Officials, Fraud Alerts, and Urgent Demands for Money

> "An official-sounding voice does not make a stranger trustworthy."

How Impersonation Scams Begin

Your telephone rings. The caller introduces himself as an officer from your bank's fraud department. He knows your name and warns that suspicious transactions have been detected.

He sounds professional and offers to help protect your savings.

What you do next could determine whether your money remains safe.

Impersonation scams occur when criminals pretend to represent trusted organisations or individuals. They may contact victims through telephone calls, emails, text messages, or messaging applications.

Scammers sometimes use official-looking documents, familiar logos, and convincing language. They may also manipulate caller identification so that a call appears to come from a recognised number.

Their objective is to gain your confidence before requesting money, information, or access to your accounts.

Fake Bank Security Alerts

Bank impersonation scams frequently begin with alarming claims about account security.

A caller may say that criminals are attempting to withdraw your savings. You might be instructed to transfer your money into a supposedly protected account while the bank investigates.

The account actually belongs to the scammer or someone assisting the fraud.

Other criminals send messages containing links to fraudulent banking websites. These pages may request usernames, passwords, or one-time verification codes.

Some callers even claim that bank employees are involved in criminal activity and warn you against contacting your usual branch.

This instruction is designed to prevent independent verification.

If someone unexpectedly tells you to transfer savings to protect them, end the conversation and contact your bank directly.

Fake Government and Law Enforcement Officials

Criminals also impersonate government officers, police investigators, tax authorities, and immigration officials.

You may receive a call claiming that your identity has been linked to criminal activity. The caller threatens arrest unless you cooperate with an investigation.

Another message may demand immediate payment of an unpaid tax, fine, or administrative charge.

Some scammers send forged documents bearing official seals or identification numbers.

They may transfer the call between several accomplices pretending to represent different departments. This creates the impression of a genuine investigation.

Official procedures differ between countries, but threats of immediate arrest combined with demands for secret payments or personal banking credentials are serious warning signs.

Contact the relevant agency independently before taking action.

Company and Customer Support Impersonation

Impersonation scams also involve familiar commercial organisations.

A message may claim to come from an online shopping platform, telecommunications provider, technology company, or subscription service.

For example, you might receive an email warning that your account has been suspended because of suspicious activity.

The message directs you to a website where you must enter your login credentials.

Other scams begin with fake customer support telephone numbers displayed in online advertisements or search results.

When victims call these numbers, criminals may request payment, confidential information, or permission to control their devices remotely.

Some scammers contact customers through social media while pretending to resolve complaints.

A familiar company name does not guarantee that the person contacting you is authorised to represent it.

How to Verify an Official Request

Independent verification is your strongest protection against impersonation.

If someone claims to represent your bank, end the call and contact the bank using the number printed on your bank card or published in its official application.

For government agencies, locate the official website yourself and use its published contact details.

Avoid relying on telephone numbers, website links, or email addresses supplied by the suspicious caller.

If you receive an unexpected customer support message, sign in through the company's genuine application or website to check for notifications.

Be aware that scammers may know genuine details about you. Your name, address, or recent purchases may have been obtained from public information or compromised records.

Knowledge of personal details does not prove someone's identity.

What You Should Do

When an unexpected caller claims to represent an authority, remain calm and avoid making immediate decisions.

Do not transfer money, reveal passwords, disclose verification codes, or install software simply because someone claims that urgent action is necessary.

You can end the conversation without seeking the caller's permission.

Contact the organisation independently and explain what happened. If the request was genuine, the organisation should be able to advise you through its established channels.

If you have already disclosed sensitive information or transferred money, contact your bank immediately and follow its security instructions.

Preserve relevant messages, telephone numbers, and transaction records for reporting.

Scammers depend on the authority of the organisations they impersonate. By verifying requests independently, you can prevent a convincing stranger from gaining control over your decisions.

Chapter 7: Investment and Cryptocurrency Scams

How Fake Profits, Guaranteed Returns, and Fraudulent Trading Platforms Deceive Investors

> "The promise of easy money deserves careful examination, especially when someone wants your money first."

How Fake Investment Opportunities Attract Victims

Imagine seeing a social media advertisement promising unusually high investment returns. The advertisement features a successful businessperson who appears to recommend a trading platform.

You click the advertisement and join a messaging group. Members share screenshots showing impressive profits. A friendly adviser offers to help you begin investing.

Everything appears convincing.

Unfortunately, the advertisement, testimonials, and adviser may be part of an elaborate scam.

Investment scammers frequently approach people through social media, messaging applications, online advertisements, and unsolicited telephone calls.

Some impersonate financial professionals or well-known companies. Others create investment groups where accomplices pretend to be satisfied investors.

Their objective is to persuade victims to transfer money into fraudulent schemes.

The Promise of Easy or Guaranteed Profits

A common warning sign is the promise of unusually high returns with little or no risk.

An investment opportunity might claim that you can earn substantial profits every week through cryptocurrency trading, foreign exchange transactions, or automated investment software.

The promoter may insist that losses are impossible because the system uses advanced technology or artificial intelligence.

These claims deserve serious scrutiny.

Legitimate investments involve risks. Their value can rise or fall, and past performance cannot guarantee future returns.

Scammers sometimes create artificial urgency by claiming that an exclusive opportunity is available for only a short period.

They may also discourage independent financial advice, insisting that outsiders do not understand the opportunity.

Whenever someone promises guaranteed profits or pressures you to invest immediately, investigate before committing money.

Fake Trading Platforms and Account Balances

Some investment scams involve sophisticated-looking websites or mobile applications.

After depositing money, victims receive access to an online account displaying their supposed investments.

The dashboard may show rising balances, profitable transactions, and impressive investment growth.

However, these figures can be entirely fabricated.

The money may never have been invested. Instead, it may have been transferred directly to accounts controlled by criminals.

Scammers can manipulate the displayed figures to encourage additional deposits.

A victim who believes an investment has doubled may feel confident enough to contribute more savings.

The appearance of profits on a screen does not establish that genuine investments exist.

Why Scammers Sometimes Allow Small Withdrawals

One particularly deceptive tactic involves allowing victims to withdraw small amounts of money.

Suppose you deposit $500 into an unfamiliar trading platform. After several days, your account displays a profit.

You request a withdrawal of $100, and the money arrives in your bank account.

This experience may convince you that the platform is legitimate.

Encouraged by the apparent success, you invest several thousand dollars.

When you eventually attempt a larger withdrawal, the platform demands additional payments for taxes, processing fees, or account verification.

You may discover that your remaining money cannot be withdrawn.

The earlier payment was part of the deception. Scammers sometimes sacrifice small amounts to gain access to much larger sums.

A successful initial withdrawal is therefore insufficient proof that an investment platform is trustworthy.

How to Check an Investment Provider

Before investing, establish whether the company and individuals involved are authorised to provide the services they advertise.

Many countries maintain official registers of licensed or regulated financial institutions.

In Singapore, investors can consult the Monetary Authority of Singapore's Financial Institutions Directory and Investor Alert List.

In the United States, relevant resources include the Securities and Exchange Commission's investor information services and FINRA's BrokerCheck.

Other countries provide similar regulatory registers and investor warning lists.

Visit these resources independently rather than following links supplied by investment promoters.

Check the exact company name, website address, and contact details. Scammers sometimes impersonate genuinely licensed businesses.

Remember that appearing on a register does not guarantee investment safety. An absence from a warning list also does not establish legitimacy.

What You Should Do

Never transfer investment funds simply because someone approaches you with an attractive opportunity.

Investigate the provider through official regulatory sources and verify its identity independently.

Be cautious about investment advice from strangers in messaging groups, particularly when they promise exceptional returns.

Avoid installing unfamiliar trading applications or sending cryptocurrency to wallets controlled by unknown individuals.

Never borrow money or use essential savings because someone promises quick profits.

If a platform refuses withdrawals and demands additional fees, stop making payments. Contact your financial institution promptly and report suspected fraud to the relevant authorities.

Investment scams succeed by making imaginary profits appear real.

Protect your savings by verifying the people, organisations, and arrangements involved before committing money.

Chapter 8: Job, Business Opportunity, and Easy-Money Scams

Recognising Fake Employment Offers, Paid Tasks, and False Income Opportunities

> "A genuine opportunity should withstand careful questions about how the money is earned."

How Fake Job Offers Reach Victims

Imagine receiving a WhatsApp message from someone claiming to be a recruitment officer. The message offers flexible work from home, generous daily earnings, and no experience requirements.

The recruiter explains that you can begin immediately. There is no formal interview, and the work takes only an hour each day.

For someone seeking additional income, the offer may sound attractive.

Unfortunately, fake employment offers are a common form of online fraud.

Scammers advertise through social media, job websites, messaging applications, and unsolicited text messages. Some impersonate established recruitment agencies or legitimate companies.

They may use stolen company logos, fabricated employee profiles, and professional-looking employment documents.

Their purpose is often to obtain money or personal information from people who believe they are applying for genuine employment.

Task Scams and Paid Online Activities

Task scams involve apparently simple online activities that promise easy commissions.

A supposed employer may ask you to rate products, like social media posts, review hotels, or complete online orders.

Initially, the tasks appear harmless.

You might receive a small payment after completing several activities. This creates confidence that the work is genuine.

Later, the platform introduces tasks requiring you to deposit money before earning larger commissions.

The recruiter explains that the deposit is temporary and will be returned together with your earnings.

As you continue, the required payments increase.

When you attempt to withdraw your money, the platform may demand additional deposits or claim that you must complete another task first.

The displayed earnings may be fictional, and the promised commissions may never be paid.

A job requiring workers to deposit their own money to unlock wages or commissions is a serious warning sign.

Work-From-Home and Business Opportunity Scams

Not every fraudulent income opportunity is presented as employment.

Some scammers advertise home-based businesses, online franchises, automated stores, or income-generating systems.

They promise that participants can earn substantial money with minimal effort.

A promoter may request an upfront payment for training, software, equipment, or membership.

After payment, the promised support may disappear. The business may produce little income, or the opportunity may never have existed.

Some fraudulent schemes also use fabricated testimonials showing impressive earnings.

Legitimate businesses can charge reasonable fees for products or training, but such charges do not establish that an income opportunity is genuine.

Before paying, examine what you will actually receive, whether the earnings claims are supported, and whether the company can be independently verified.

Money Mule Recruitment

Some fake jobs involve receiving money into your personal bank account and transferring it elsewhere.

The recruiter may describe the work as payment processing, financial administration, or international transaction support.

You are promised a commission for each transfer.

However, the money may come from criminal activities, including scams against other victims.

A person who receives or transfers funds on behalf of criminals may become a money mule.

Participating in these transactions can expose you to serious legal consequences, depending on your knowledge, actions, and local laws.

Scammers may also request access to your bank account or ask you to open new accounts for business purposes.

Never allow an unfamiliar employer to use your personal account to receive or move money for unknown parties.

How to Verify an Employer or Opportunity

Begin by checking whether the company genuinely exists.

Visit its official website independently and look for the advertised position through established recruitment channels.

If someone claims to represent a known company, contact its human resources department using published contact details.

Check whether the recruiter's email address belongs to the company's genuine domain.

Be cautious if communication takes place entirely through messaging applications and the recruiter refuses a reasonable identity check.

Examine the job description carefully. Genuine employment offers should explain the responsibilities, payment arrangements, and employment conditions.

A company registration number alone does not prove legitimacy because scammers can misuse genuine business details.

What You Should Do

Before accepting an unfamiliar job or income opportunity, investigate the employer and understand exactly how you will be paid.

Avoid opportunities promising unusually high earnings for trivial activities.

Never pay deposits to unlock commissions or withdraw supposed wages.

Protect your identity documents and banking information until you have verified the employer and established a legitimate reason for sharing them.

Refuse requests to receive or transfer money for strangers through your personal accounts.

If you have already transferred money or disclosed sensitive information, contact your bank promptly and report the suspected scam.

A genuine employment opportunity should provide understandable work arrangements and withstand independent verification.

Your desire to earn an income should never require you to surrender control of your money or financial accounts.

Chapter 9: Social Media, Messaging, and Online Friendship Scams

How Criminals Exploit Online Connections, Fake Profiles, and Hijacked Accounts

"A familiar face on a screen is not always the person behind the message."

How Scammers Approach People on Social Media

Social media allows us to reconnect with old friends, meet new people, and communicate across the world. Unfortunately, scammers use these same platforms to find potential victims.

Imagine receiving a friendly message from someone who shares your interests. The person's profile contains attractive photographs, thoughtful posts, and several mutual connections.

You begin chatting. The conversation seems natural, and the person appears genuinely interested in getting to know you.

However, the profile may be fake.

Scammers create false identities using stolen photographs, invented personal histories, and misleading information. Some impersonate professionals, celebrities, or ordinary individuals.

They may approach people through Facebook, Instagram, TikTok, LinkedIn, Telegram, WhatsApp, or other platforms.

An unexpected friendship request is not necessarily suspicious, but caution is appropriate when someone quickly requests personal information or introduces financial opportunities.

When a Friend's Account Has Been Hijacked

Sometimes, a suspicious message appears to come from someone you already know.

Imagine receiving a message from an old friend asking for an urgent loan. Your friend explains that a banking problem has left them temporarily unable to access their money.

The message arrives through the same social media account you have used to communicate with that person for years.

You may naturally assume the request is genuine.

However, scammers sometimes gain unauthorised access to legitimate accounts. Once inside, they can send fraudulent messages to the account owner's contacts.

These messages may request emergency loans, verification codes, or assistance with supposed financial difficulties.

Because the request comes from a familiar account, recipients may lower their guard.

Before sending money, contact your friend through a different, established communication channel. A direct telephone conversation can help confirm whether the request is genuine, although a familiar voice alone should not be treated as conclusive proof.

Fake Giveaways and Influencer Endorsements

Social media scams also appear through advertisements, competitions, and promotional posts.

A fraudulent account may claim that a popular company is giving away expensive products. Participants are asked to click a link, complete a form, or pay a small delivery fee.

The promised giveaway may never have existed.

Other scammers misuse photographs or videos of celebrities and online influencers to promote fraudulent investments or products.

Some advertisements falsely suggest that a well-known personality has personally endorsed an opportunity.

The account displaying the promotion may closely resemble an official profile.

Be cautious about competitions requiring banking details, passwords, or advance payments.

Verify promotions through the organisation's independently located official website or established communication channels.

Online Friendships Used for Financial Exploitation

Online friendships can develop into meaningful relationships. However, criminals sometimes use friendly conversations to establish trust before requesting money.

A scammer may communicate regularly, remember personal details, and offer emotional support.

Over time, the person may introduce an investment opportunity, request a temporary loan, or describe an unexpected financial emergency.

The request can seem reasonable because a relationship has already developed.

Some scammers gradually isolate victims from people who might question their stories.

They may discourage discussions with family members or become upset when asked for independent verification.

Genuine friendships should allow reasonable questions about financial requests.

Never feel obligated to send money simply because someone has spent considerable time communicating with you.

How to Check Whether a Profile Is Genuine

Start by examining the account's history.

Look for meaningful activity over time, consistent information, and interactions that appear natural.

A recently created profile with limited activity may deserve additional scrutiny, although established accounts can also be compromised.

You can use reverse image searching to investigate whether profile photographs appear elsewhere under different identities.

However, photographs may be stolen, altered, or artificially generated, so image searches cannot establish authenticity.

If someone claims to represent an organisation, verify their identity through its official channels.

For people you know personally, contact them through a separate, familiar method when an unusual request appears.

Remember that followers, mutual connections, and professional-looking photographs are not reliable proof of identity.

What You Should Do

Protect your social media accounts with strong, unique passwords and additional login security.

Review privacy settings and limit unnecessary public access to personal information.

Avoid sharing verification codes, banking details, or identity documents with online contacts whose identities have not been independently established.

Be cautious when someone unexpectedly introduces financial opportunities or requests urgent assistance.

If a friend's account appears compromised, inform them through another communication channel.

Report suspicious profiles and fraudulent messages to the relevant platform.

Online connections can enrich your life. A little independent verification helps ensure that the people requesting your trust are genuinely who they claim to be.

Part Three: The New Generation of Online Scams

Technology has changed the way we communicate, work, shop, and manage our money. Unfortunately, it has also given criminals new ways to deceive people.

In the past, fraudulent messages were sometimes easier to recognise because of poor spelling, awkward language, or suspicious-looking websites. Today, scammers can create professional messages, realistic images, and convincing online identities with relatively little effort.

Artificial intelligence has made some forms of impersonation particularly difficult to detect. Criminals can generate realistic voices, manipulate videos, and create false appearances that resemble people we know or trust.

Other scams involve harmful applications, fake technical support services, and software that allows criminals to access computers or mobile phones remotely.

These methods can be especially dangerous because victims may believe they are communicating with genuine people or receiving legitimate technical assistance.

In this part, we will examine two important areas of modern online fraud.

First, we will explore how artificial intelligence, deepfake technology, and voice cloning are being used to create convincing impersonations.

Next, we will examine malicious applications, remote access scams, and fraudulent technical support schemes that can expose personal information and financial accounts.

You do not need advanced technical knowledge to understand these threats or protect yourself.

The most important lesson is that appearances can be manipulated. A familiar voice, realistic video, professional website, or convincing application does not automatically establish trustworthiness.

As technology continues to develop, the ability to verify information independently becomes increasingly valuable.

Understanding these newer methods will help you approach unfamiliar digital situations with greater awareness and confidence.

Chapter 10: AI Scams, Deepfakes, and Fake Voices

How Artificial Intelligence Makes Impersonation More Convincing

"When technology can imitate someone you trust, verification becomes more important than recognition."

How AI Is Changing Online Fraud

Imagine receiving a video message from a familiar business leader recommending an investment. The person's face, voice, and manner of speaking appear genuine.

You might reasonably believe that the recommendation is authentic.

However, the video could have been created using artificial intelligence.

Artificial intelligence, commonly called AI, allows computers to generate text, images, voices, and videos. Although this technology has many legitimate uses, criminals can exploit it to make fraudulent communications more convincing.

Scammers can produce professional emails, create realistic photographs, and personalise messages using information gathered online.

They can also imitate people whom victims already know or trust.

These capabilities make some scams harder to recognise through appearance alone.

What Are Deepfakes?

A deepfake is an artificially generated or manipulated recording that makes someone appear to say or do something they never actually said or did.

Deepfakes can involve video, photographs, or audio.

For example, a criminal might create a video showing a well-known person promoting a fraudulent investment platform.

The person's facial movements and speech may appear realistic, even though the endorsement never happened.

Some deepfakes alter genuine recordings, while others generate entirely artificial content.

The technology can also create fictional people who appear to exist in real life.

A convincing photograph or video should therefore be treated as information requiring verification, particularly when it accompanies a request for money.

Voice Cloning and Fake Emergency Calls

Voice cloning uses artificial intelligence to generate speech resembling a particular person's voice.

Criminals may obtain short voice recordings from social media videos, public interviews, or other accessible sources.

Imagine receiving a telephone call from someone who sounds exactly like your adult child.

The caller is crying and claims to have been involved in an accident. Money is urgently needed to resolve the situation.

The familiar voice makes the emergency seem genuine.

However, the voice could be artificially generated.

The United States Federal Trade Commission has warned that scammers can use voice cloning to impersonate relatives during fabricated emergencies.

The safest response is to end the call and contact your relative through a telephone number you already know.

If you cannot reach them, contact another trusted family member to verify the situation.

Fake Celebrity Endorsements and Investment Videos

Scammers also exploit public trust in celebrities, business leaders, and respected professionals.

A social media advertisement may feature a famous actor appearing to recommend a cryptocurrency investment.

Another video may imitate a television interview in which a public figure supposedly reveals a profitable trading opportunity.

These promotions can be entirely fabricated.

Australia's Scamwatch has documented fraudulent investment advertisements using deepfake celebrity videos and fake news articles.

The apparent endorsement is intended to make the opportunity seem credible.

Before trusting such claims, investigate the investment provider independently and check whether the endorsement appears through the public figure's verified official channels.

Even a genuine celebrity endorsement cannot guarantee that an investment is safe.

Why Appearance and Voice Are No Longer Reliable Proof

People naturally rely on familiar faces and voices to recognise others.

AI-generated impersonations make this increasingly risky.

Some manipulated videos contain unusual facial movements, inconsistent lighting, or unnatural speech. However, these imperfections are not always present.

High-quality synthetic content may appear convincing to ordinary viewers.

Trying to identify every deepfake through visual inspection is therefore unreliable.

A video call also does not automatically establish someone's identity because visual and audio content can sometimes be manipulated.

The more dependable approach is to verify unexpected requests through separate, trusted communication channels.

What You Should Do

Whenever a familiar voice or face makes an unexpected request involving money or confidential information, stop and verify the situation.

End suspicious calls and contact the person using a telephone number you already have.

For requests supposedly made by company executives or officials, use established organisational contact procedures.

Consider agreeing on a private family verification phrase for emergencies. Keep it confidential and use it alongside independent contact, since phrases can also be disclosed.

Avoid making financial decisions based solely on videos, audio recordings, or online endorsements.

If someone pressures you to act immediately, explain that you need to verify the request first.

AI technology will continue to improve, and fraudulent impersonations may become increasingly convincing.

Your strongest protection is a verification habit that remains useful even when artificial content looks and sounds completely real.

Chapter 11: Malicious Apps, Remote Access, and Tech Support Scams

How Scammers Gain Access to Your Devices, Accounts, and Money

> "Protecting your money also means protecting the devices that give you access to it."

How Fraudulent Apps and Software Are Used

Imagine purchasing something through a social media advertisement. The seller asks you to install a special application to complete payment or arrange delivery.

You follow the instructions because the application appears necessary for your purchase.

Unfortunately, the software may be malicious.

Malicious software, commonly called malware, is designed to perform harmful activities on computers or mobile devices. It may steal information, monitor activity, or allow criminals to interfere with accounts.

Some fraudulent applications imitate genuine shopping, banking, or delivery services.

Others are disguised as useful tools.

Once installed, harmful software may attempt to obtain passwords, intercept messages, or access financial information.

The danger increases when users grant applications unnecessary permissions.

Fake Technical Support Warnings

You are browsing the internet when a warning suddenly fills your screen.

It claims that your computer has been infected with dangerous viruses. A telephone number appears, accompanied by instructions to contact technical support immediately.

The message may even display the logo of a familiar technology company.

This could be a technical support scam.

Criminals create frightening pop-up messages to convince people that their devices require urgent repairs.

When victims call the displayed number, scammers impersonate technical support employees.

They may demand payment for unnecessary services or ask victims to install software.

The United States Federal Trade Commission warns that genuine security pop-ups do not ask users to telephone a support number.

If an unexpected warning appears, avoid calling the displayed number. Close the suspicious page and seek assistance through official support channels.

Remote Access Scams

Remote access software allows someone to operate a computer or mobile device from another location.

This technology has legitimate uses, including technical assistance and workplace support.

However, scammers can exploit it.

A fraudulent technician may ask you to install a remote access application, claiming that it is necessary to remove viruses or repair your device.

Once connected, the person may be able to view your screen, operate applications, or access sensitive information.

Some criminals persuade victims to open online banking applications while remote access remains active.

This may expose account information or enable unauthorised transactions.

Never grant remote access to someone who contacts you unexpectedly and claims that your device requires repairs.

Dangerous App Permissions

Applications sometimes request permission to access particular features of your device.

A navigation application may reasonably need location information. A camera application may require access to your camera.

However, certain permissions can create serious risks when granted to malicious software.

Accessibility permissions, designed to help people operate their devices, can sometimes allow applications to observe screen content or control interactions.

Screen-sharing permissions may expose messages, passwords, and financial information displayed on your device.

Other sensitive permissions include access to text messages, notifications, and stored files.

Before approving a request, consider whether the application genuinely needs that access.

An unfamiliar shopping application requesting extensive control over your phone should raise suspicion.

Warning Signs of Device Compromise

A compromised device may behave differently from normal.

You might notice unfamiliar applications, unexpected account notifications, or security settings that have changed without your permission.

Other possible signs include unusual pop-ups, unexplained financial transactions, or login alerts from unfamiliar locations.

However, these symptoms can also have innocent explanations.

A slow device or rapidly draining battery does not automatically indicate malware.

Some infections produce no obvious warning signs.

If you suspect unauthorised access, check your financial accounts using another trusted device.

Contact your bank immediately if you discover suspicious transactions.

What You Should Do

Install applications through official app stores whenever possible, and verify the developer before downloading.

Official stores reduce certain risks but cannot guarantee that every application is safe.

Keep your operating system, browser, and applications updated. Use reputable security software where appropriate.

Avoid installing software through unexpected messages or granting unnecessary permissions.

If you suspect that a malicious application has been installed, disconnect the affected device from mobile data and Wi-Fi.

Use another trusted device to contact your bank and secure important accounts.

Seek assistance from a reputable technical professional. A seriously compromised device may require a factory reset or professional examination.

If someone has obtained remote access, disconnect immediately and treat sensitive information accessed during the session as potentially exposed.

Protecting your devices is an essential part of protecting your personal information and money.

Part Four: Protecting Yourself Before a Scam Happens

Recognising a suspicious message is an important first step. Knowing what to do next can prevent a costly mistake.

Many people encounter situations where they are uncertain whether something online is genuine. A message may appear to come from their bank. An unfamiliar website may offer an attractive bargain. Someone claiming to represent a trusted organisation may request personal information.

In such situations, uncertainty is normal. You cannot always determine whether something is fraudulent simply by examining its appearance.

Fortunately, you can develop practical habits that reduce your exposure to online scams.

The most important habit is independent verification. Before responding to an unexpected request, you can check the person's identity, confirm the organisation's contact details, and investigate the claims being made.

You can also strengthen the security of your financial accounts, personal information, and digital devices.

These precautions do not require advanced technical knowledge. Many involve simple actions, such as using strong passwords, enabling additional account protection, and checking payment details before transferring money.

In this part, you will learn a practical method for investigating suspicious messages, websites, and offers. You will also discover everyday security measures that can make it more difficult for criminals to gain access to your accounts or misuse your personal information.

The aim is to make safer online behaviour part of your normal routine.

You cannot control every scam attempt that reaches you. However, you can improve how you respond to unexpected requests and reduce opportunities for criminals to exploit your trust.

A few sensible precautions, practised consistently, can provide valuable protection long before a scam occurs.

Chapter 12: How to Check Whether Something Is a Scam

A Practical Verification Method for Suspicious Messages, Websites, People, and Offers

> "When you are unsure whether something is genuine, you do not have to make a decision immediately."

Start by Stopping

Imagine receiving a message claiming that your bank account will be suspended within thirty minutes unless you verify your identity.

The message contains a link and warns that failure to respond could result in serious inconvenience.

Your first instinct may be to act quickly.

However, the safest response is to stop.

Scammers frequently create urgency because they want people to act before checking the facts.

When something unexpected requires immediate action, allow yourself time to investigate.

Do not click suspicious links, send money, or disclose personal information while feeling pressured.

A genuine organisation should have an established way for you to verify an important request independently.

Identify Exactly What You Are Being Asked to Do

Before deciding whether a message is genuine, examine what the sender wants.

Are you being asked to transfer money, provide banking details, reveal a password, or share a verification code?

Perhaps someone wants you to install an application, grant remote access, or visit an unfamiliar website.

These requests deserve particular caution because they can expose your money, accounts, or devices.

Consider the reason given for the request.

A supposed bank employee may claim that your money must be transferred to a temporary account for protection.

A recruiter may demand a deposit before releasing your earnings.

A stranger may offer an unusually profitable investment.

Write down the request in simple terms. Understanding exactly what you are being asked to do makes it easier to recognise unnecessary risks.

Verify the Person or Organisation Independently

Independent verification means checking information through a source that the suspicious sender does not control.

Suppose someone calls claiming to represent your bank.

Do not rely on the telephone number displayed during the call. Caller identification can be falsified.

End the conversation and telephone your bank using the number printed on your bank card, shown in its official application, or obtained from its independently located website.

If someone claims to represent a government agency, contact that agency through its established public channels.

For an unexpected request from a friend, use a telephone number or communication method you already know.

Do not use contact details supplied exclusively in the suspicious message.

The purpose is to reach the genuine person or organisation without depending on information provided by the possible scammer.

Check Websites, Offers, and Payment Details

When investigating a website, examine its full address carefully.

Scammers sometimes create addresses resembling those of legitimate organisations, with additional words or altered spelling.

A padlock symbol or an address beginning with HTTPS indicates an encrypted connection. It does not prove that the website is trustworthy.

For online shopping, investigate the seller's reputation through independent sources. Check the return policy, contact information, and payment arrangements.

Be cautious when a seller insists on an unusual payment method or asks you to transfer money to an unrelated personal account.

For investment opportunities, check the provider's authorisation with the appropriate financial regulator in your country.

For employment offers, contact the company's official recruitment department.

Always verify payment instructions independently, especially when bank account details have unexpectedly changed.

Recognise When Verification Is Inconclusive

Sometimes, your investigation produces information that appears reassuring but does not establish legitimacy.

A website may contain positive customer reviews. However, reviews can be fabricated or purchased.

A business may display registration documents that belong to another organisation.

Search engine results may contain advertisements leading to fraudulent websites.

A convincing photograph, professional-looking email, or official-looking document can also be misleading.

Even a genuine company's existence does not prove that the person contacting you represents it.

When you cannot independently confirm a request, treat it as unverified.

You do not need to prove that something is fraudulent before deciding not to proceed.

What You Should Do

Develop a simple verification routine whenever you encounter an unexpected request.

First, stop and avoid taking immediate action.

Next, identify what the person wants from you and what you could lose by complying.

Then, independently contact the supposed sender through a trusted channel.

Check the website, company, offer, and payment instructions using reliable sources.

If the information cannot be confirmed, do not send money, disclose sensitive details, or grant device access.

You can seek advice from someone you trust or consult an official scam reporting service.

Remember that verification is not about becoming suspicious of everyone.

It is about making important decisions using information you have checked for yourself.

The more consistently you practise this routine, the easier it becomes to recognise situations that deserve caution.

Chapter 13: How to Protect Your Money and Personal Information

Simple Security Habits That Reduce Your Risk of Online Fraud

> "Good security habits protect you even before you realise someone is trying to deceive you."

Use Strong, Unique Passwords

Imagine using the same password for your email, online shopping, and banking accounts.

If criminals obtain that password from one compromised service, they may try it on your other accounts.

This is why every important account should have a different password.

Choose long passwords that are difficult to guess. Avoid using your birthday, telephone number, or other easily discovered personal information.

A password manager can help.

A password manager is an application that creates and securely stores passwords. Instead of remembering dozens of passwords, you remember one strong master password.

Choose a reputable password manager and protect it with additional authentication.

Never share your passwords with someone claiming to provide technical support.

Turn On Additional Account Protection

Passwords alone may not provide sufficient protection.

Two-factor authentication adds another step when someone attempts to access your account.

For example, after entering your password, you may need to approve the login through an authentication application or use a security key.

This makes unauthorised access more difficult, even when someone knows your password.

Where available, authentication applications and security keys generally provide stronger protection than text-message codes against certain attacks.

Passkeys offer another option.

A passkey allows you to sign in using a trusted device, often with a fingerprint, facial recognition, or device PIN.

Properly implemented passkeys help protect against fraudulent login websites because they are linked to the genuine service.

Enable the strongest practical authentication methods offered by your important accounts.

Never disclose a login verification code to someone who contacts you unexpectedly.

Protect Banking and Payment Accounts

Your banking accounts deserve particular attention.

Enable transaction notifications so you can learn quickly about payments or transfers you did not authorise.

Review your account activity regularly, including transactions involving small amounts.

Where available, consider setting daily transfer limits appropriate to your normal financial needs.

Some banks offer additional security controls, including temporary account locks, payment restrictions, or emergency reporting features.

Familiarise yourself with these options before an emergency occurs.

Avoid saving unnecessary payment information on unfamiliar websites.

When making payments, check the recipient's details carefully.

If your bank offers a separate method for confirming important transactions, use it.

Remember that a transaction you personally authorise under deception may not be treated the same way as an unauthorised transaction. Prevention remains important.

Keep Devices and Applications Updated

Software updates are not merely about introducing new features.

Many updates repair security weaknesses that criminals could exploit.

Keep your mobile phone, computer, web browser, and important applications updated.

Enable automatic security updates whenever practical.

Install applications from official stores or verified developer websites.

Avoid downloading software from links sent by strangers.

Remove applications you no longer need, especially those with access to sensitive information.

Protect your devices with a screen lock and avoid leaving them unattended while unlocked.

If a device is no longer receiving security updates, consider replacing it or limiting its use for sensitive activities.

Limit Unnecessary Personal Information Sharing

Scammers often collect information from public websites and social media profiles.

Details such as your birthday, workplace, family relationships, and travel plans can help criminals create convincing messages.

Review your social media privacy settings.

Consider limiting who can view your posts, contact information, and friends list.

Avoid publishing photographs of identity documents, bank cards, or official correspondence.

Before submitting personal information through an online form, consider whether the organisation genuinely needs it.

Be especially cautious when someone requests copies of identity documents through an unexpected message.

Personal information can be misused for impersonation or fraudulent account applications.

Protecting your privacy reduces the information available to people attempting to deceive you.

What You Should Do

Make personal security a regular habit rather than something you consider only after receiving a suspicious message.

Begin with your email account because it is often used to reset passwords for other services.

Create unique passwords for important accounts and consider using a password manager.

Enable two-factor authentication or passkeys wherever available.

Activate banking transaction alerts and review your transfer limits.

Keep your devices updated and remove unfamiliar or unnecessary applications.

Check your privacy settings and reduce the personal information publicly available online.

Finally, learn how to contact your bank quickly if you suspect fraud.

You do not need to complete every improvement in one day.

Start with your most important accounts and gradually strengthen the others.

These habits cannot eliminate every scam risk, but they can make it considerably harder for criminals to gain access to your money and personal information.

Part Five: Responding to Scams and Staying Safe

Even when you understand how online scams work and take precautions to protect yourself, you may still encounter a convincing attempt at fraud.

Scammers constantly change their methods. They exploit new technologies, imitate trusted organisations, and create situations that pressure people into making quick decisions.

Sometimes, a person recognises the danger before anything happens. At other times, the warning signs become clear only after money has been transferred or personal information has been disclosed.

If you discover that you may have been scammed, what you do next matters.

Acting promptly can help limit further financial losses, protect your accounts, and preserve information that may assist an investigation.

It is also important to understand that being deceived does not mean someone is foolish or careless. Criminals deliberately manipulate trust,

emotions, and ordinary human behaviour. Anyone can encounter a convincing scam.

In this final part, we will examine the practical steps to take when you suspect that a scam has occurred. You will learn how to respond to suspicious transactions, protect compromised accounts, preserve evidence, and report fraud through appropriate channels.

We will also explore how to remain informed as online scams continue to evolve.

You do not need to memorise every type of scam or understand every new technology. What matters is developing habits that help you recognise unusual requests, verify information independently, and respond appropriately when something goes wrong.

Staying safe online is an ongoing process.

The knowledge you have gained throughout this book can help you make more informed decisions, protect your financial security, and share useful precautions with people around you.

The aim is not to become fearful of the internet. It is to use it with greater awareness, confidence, and control.

Chapter 14: What to Do If You Have Been Scammed

Immediate Steps to Protect Your Accounts, Report Fraud, and Seek Help

> "When you discover a scam, the next important decision is how to protect what remains."

Stop Contact and Prevent Further Losses

Discovering that you have been scammed can be frightening. You may feel embarrassed, angry, or uncertain about what to do.

The first priority is to prevent further harm.

Stop communicating with the suspected scammer. Do not send additional money, even if the person promises to return your previous payments.

Scammers may claim that you must pay a processing fee, outstanding tax, or account verification charge before receiving your money.

These demands may be attempts to obtain more money.

Avoid clicking further links or installing applications suggested by the person.

Do not delete conversations immediately. They may contain useful evidence.

If someone is threatening you, preserve the messages and seek assistance from the appropriate authorities.

Contact Your Bank or Payment Provider Immediately

If you have transferred money, contact your bank or payment provider as soon as possible.

Use its official telephone number or application rather than contact details supplied by the scammer.

Explain what happened, identify the transactions, and ask what protective actions are available.

Your bank may be able to block further transactions, secure your account, or attempt to recall transferred funds.

If you paid by card, ask whether the transaction qualifies for a dispute or chargeback.

If you used a payment application or cryptocurrency service, report the incident to that provider promptly.

Recovery is not guaranteed.

The possibility of recovering money depends on the payment method, how quickly you report the incident, the location of the funds, and applicable procedures.

Nevertheless, early reporting may improve the chances of limiting further losses.

Secure Your Accounts and Devices

The next steps depend on what information or access the scammer obtained.

If you disclosed a password, change it immediately using the genuine website or application. Change passwords on other accounts where you reused it.

Enable additional login protection and review recent account activity.

If you revealed banking details or card information, ask your financial institution whether your card or account needs to be blocked or replaced.

If you installed a suspicious application or granted remote access, stop using the affected device for banking.

Disconnect it from the internet and seek assistance from a reputable technical professional.

Use another trusted device to secure important accounts.

If identity documents were exposed, contact the relevant issuing authority or identity protection service to ask about available safeguards.

Preserve Evidence and Report the Incident

Keep records of everything connected with the suspected scam.

Useful evidence includes messages, email addresses, telephone numbers, website links, payment receipts, transaction references, and screenshots.

Record the dates and amounts of payments.

Preserve the original messages where possible because screenshots may not capture every useful detail.

Report the incident to your local police or designated fraud reporting authority.

In Singapore, you can seek guidance through ScamShield and report suspected criminal activity to the Singapore Police Force.

In other countries, use the relevant national fraud reporting service or consumer protection authority.

You should also report fraudulent profiles, advertisements, or accounts to the platforms involved.

Official reports may assist investigations, even when immediate financial recovery is not possible.

Watch Out for Recovery Scams

Unfortunately, some criminals target people who have already lost money.

A person may contact you claiming to be a lawyer, investigator, government official, or specialist recovery agent.

They promise to retrieve your lost funds in exchange for an upfront payment.

Some claim that your money has already been located but requires a release fee.

These offers may be another scam.

Criminals sometimes use information from the original fraud to make their claims convincing.

Do not trust someone simply because they know details about your previous loss.

Verify any organisation independently before providing information or paying fees.

Be particularly cautious of guaranteed recovery promises.

What You Should Do Next

After taking urgent protective steps, review your financial accounts regularly for unfamiliar activity.

Keep a written record of reports submitted, organisations contacted, and actions taken.

Follow up with your bank and relevant authorities using official channels.

Consider reviewing your account security and adjusting payment limits.

If the incident has affected your confidence or emotional wellbeing, speak with someone you trust.

Financial fraud can cause considerable distress, especially when savings or borrowed money are involved.

You may also benefit from professional financial or emotional support.

Avoid making rushed financial decisions while trying to replace lost money.

Recovery can take time, and some losses may be permanent.

Focus on protecting your remaining resources, understanding what happened, and rebuilding your financial security.

Being scammed does not prevent you from making safer decisions in the future.

Chapter 15: How to Stay Scam-Aware in a Changing Digital World

Building Everyday Habits That Help You Recognise New Scams

> "You cannot predict every new scam, but you can develop habits that help you recognise danger."

Why Scam Methods Continue to Change

Online scams will continue to evolve because technology and everyday habits are constantly changing.

When more people began shopping online, criminals developed fraudulent shopping websites. As digital payments became popular, scammers found new ways to impersonate banks and payment providers.

Today, artificial intelligence allows criminals to create convincing messages, voices, and videos.

Tomorrow, new technologies may introduce different opportunities for fraud.

Scammers also study how people behave. They take advantage of popular shopping seasons, employment trends, major news events, and changes in financial services.

A scam that worked several years ago may reappear with a different name or delivery method.

This means that memorising a list of known scams is not enough.

The better approach is to understand the methods criminals use to gain trust and persuade people to act without verification.

Learn From Official Scam Alerts

Government agencies, police departments, financial regulators, and consumer protection organisations regularly publish information about emerging scams.

These alerts can help you recognise unfamiliar techniques before encountering them personally.

In Singapore, ScamShield and the Singapore Police Force provide scam-related information.

In the United States, the Federal Trade Commission publishes consumer fraud warnings.

Australia's Scamwatch and the Canadian Anti-Fraud Centre also provide useful guidance.

Readers elsewhere should identify the equivalent official services in their countries.

You do not need to read every warning.

Occasionally reviewing official alerts can help you understand which scams are becoming more common and what precautions are recommended.

Whenever possible, obtain information directly from an agency's official website rather than relying entirely on forwarded messages.

Build a Personal Verification Routine

The most useful protection is a routine you can follow without having to think too hard.

Whenever someone unexpectedly asks for money, sensitive information, or access to your device, stop before responding.

Consider whether the request is reasonable.

If the person claims to represent an organisation, contact that organisation independently.

If the request comes from someone you know, verify it through another established communication channel.

Before making an unfamiliar payment, check the recipient's details and investigate the transaction.

These steps should become normal habits, much like checking that your front door is locked before leaving home.

A routine is particularly valuable when you are busy, distracted, or emotionally unsettled.

You may not recognise every new scam, but you can still refuse to act on an unverified request.

Discuss Scams With People You Trust

Scammers often benefit when victims feel unable to discuss suspicious situations with others.

Someone who is embarrassed about an investment decision may hesitate to ask for advice.

A person who has developed an online friendship may fear being judged for trusting a stranger.

Open conversations can make it easier to recognise problems early.

Discuss unusual messages or financial requests with trusted relatives, friends, or colleagues.

Encourage others to ask questions without fear of ridicule.

If someone tells you that they may have been scammed, listen carefully before offering advice.

Avoid blaming them for what happened.

A supportive conversation may help the person take protective action sooner.

Sharing experiences can also make everyone more aware of unfamiliar scam methods.

Share Warnings Responsibly

When you encounter a possible scam, you may want to warn other people immediately.

This can be helpful, but inaccurate warnings can create unnecessary confusion.

Social media posts sometimes circulate outdated information, fabricated incidents, or misleading photographs.

A forwarded message claiming that a particular company is fraudulent may itself contain false information.

Before sharing an alert, check whether it comes from a credible source.

Look for confirmation from official agencies or the organisation involved.

Avoid forwarding unverified accusations against individuals or businesses.

If you are uncertain, explain that the information has not been confirmed.

Responsible sharing helps others stay informed without spreading unnecessary fear or misinformation.

What You Should Do

Create a manageable routine for staying scam-aware.

Once a month, visit an official scam information website and review recent warnings relevant to your activities.

Keep your devices and important applications updated.

Review your banking notifications and account security settings periodically.

Whenever you encounter an unfamiliar financial request, use the verification method described earlier in this book.

Discuss suspicious situations with someone you trust, especially when substantial money is involved.

If you discover a genuine scam warning, share the official information with people who may benefit.

You do not need to become an expert in every form of online fraud.

A small amount of regular attention, combined with careful verification, can make a meaningful difference.

The digital world will continue changing. Your protective habits can remain dependable even as new scams appear.

Conclusion: Your Best Protection Is Knowing When to Stop

The internet has become an essential part of everyday life. We use it to communicate with people we love, manage our money, purchase products, find employment, and discover new opportunities.

These benefits are worth enjoying. Unfortunately, criminals use the same digital services to deceive people.

Throughout this book, you have learned how online scams operate, why they can be convincing, and what warning signs deserve your attention.

You have also discovered an important principle: You do not need to recognise every type of scam to protect yourself.

What matters is knowing when to stop and verify.

When someone unexpectedly asks for money, take time to investigate. When a message requests confidential information, confirm the sender's

identity independently. When an unfamiliar website offers something unusually attractive, examine the offer before making a payment.

Do not allow urgency, fear, excitement, or personal affection to replace careful judgment.

Scammers deliberately exploit ordinary human reactions. They understand that people want to help their families, protect their savings, find good opportunities, and trust those who appear sincere.

These are normal human qualities.

If you have been deceived, it does not mean you lack intelligence or good character. What happened deserves a practical response, not personal condemnation.

Take appropriate steps to protect your accounts, report the incident, and seek support when necessary.

For everyone else, prevention begins with small habits practised consistently.

Use strong passwords. Protect your devices. Monitor your financial accounts. Question unexpected requests. Verify important information through trustworthy channels.

You do not have to become suspicious of every person you encounter online.

You simply need to recognise that trust should be supported by reasonable verification, especially when money or sensitive information is involved.

Technology will continue changing. New scams will appear, and some will be difficult to recognise.

However, the basic principles of protecting yourself will remain useful.

You can pause before acting. You can ask questions. You can check independently. You can refuse a request that cannot be verified.

Above all, remember that you are allowed to walk away from any online interaction that makes you uncomfortable or uncertain.

Continue using the internet to learn, communicate, work, and enjoy life.

Do so with confidence, supported by the knowledge and habits you have developed.

Your best protection begins with a simple decision: Stop, check, and only then decide what to do.

Appendix A: The 30-Point Online Scam Warning Signs Checklist

Use this checklist whenever a message, website, person, or offer seems suspicious. One warning sign does not automatically prove fraud, but it is a reason to investigate.

Suspicious Communications

1. An unexpected message asks you to act immediately.

2. Someone threatens consequences unless you respond.

3. A stranger sends an unfamiliar link or attachment.

4. A caller pressures you to keep the conversation secret.

5. Someone requests a password or verification code.

6. A message asks you to install an unfamiliar application.

Suspicious Identity Claims

1. Someone claims to represent your bank without independent verification.
2. A supposed official refuses reasonable identity checks.
3. A familiar contact suddenly requests money.
4. A caller's identity depends entirely on a familiar-sounding voice.
5. A social media profile has an inconsistent history.
6. Someone discourages you from contacting their organisation directly.

Suspicious Payment Requests

1. You are asked to transfer money to protect your savings.
2. A payment must go to an unrelated personal account.
3. Someone demands payment using gift cards or cryptocurrency.
4. You must pay before withdrawing supposed earnings.
5. Additional fees appear after you have already paid.
6. A stranger asks to use your bank account for transfers.

Suspicious Websites

1. A website address imitates a familiar organisation.
2. Contact information is missing or unverifiable.
3. Prices are unusually low without a credible explanation.
4. The website requests unnecessary personal information.
5. A payment page redirects you to an unfamiliar destination.
6. Reviews appear fabricated or cannot be independently confirmed.

Suspicious Online Offers

1. An investment promises guaranteed high returns.
2. A job offers exceptional pay for trivial tasks.
3. An employer demands deposits before paying wages.
4. A giveaway requires an unexpected payment.
5. A promoter pressures you to decide immediately.
6. An opportunity cannot be independently verified.

Remember: Stop, check independently, and refuse requests you cannot verify.

Appendix B: How to Verify a Suspicious Message, Website, or Offer

Use this simple process whenever you receive an unexpected message, encounter an unfamiliar website, or consider an online offer.

Step 1: Stop Before Responding

Do not click links, download files, send money, or disclose personal information until you have checked the request.

Urgency is a reason to be more careful.

Step 2: Identify the Sender

Ask yourself who is contacting you and what they want.

Do not assume that a familiar name, photograph, telephone number, or email address proves someone's identity.

These details can be falsified.

Step 3: Verify Independently

Contact the person or organisation using information you already trust.

For banks and government agencies, use their official applications or independently located websites.

Do not rely on contact details supplied in the suspicious message.

Step 4: Examine the Website

Check the complete website address for unusual spelling or additional words.

Look for reliable contact information and independently confirmed business details.

Remember that HTTPS and a padlock symbol do not guarantee legitimacy.

Step 5: Investigate the Offer

Consider whether the promised benefits are realistic.

Check employment claims, investment providers, and business opportunities through appropriate official channels.

Be cautious about guaranteed profits and unusually easy earnings.

Step 6: Verify Payment Instructions

Confirm the recipient's identity and payment details independently.

Question unexpected changes to bank account numbers or requests for unusual payment methods.

Never transfer money merely because someone pressures you.

Step 7: Make Your Decision

Proceed only when you understand the request and have reasonable independent confirmation.

If important details remain uncertain, do not proceed.

Seek advice from someone you trust or consult an official scam prevention service.

Remember: You do not need proof of fraud to decline an unverified request.

Appendix C: What to Do in the First 30 Minutes After a Scam

If you suspect that you have been scammed, act immediately. The first 30 minutes are a guide to prioritising urgent action, not a period you should wait through.

First Priority: Stop Further Losses

1. Stop communicating with the suspected scammer.

2. Do not send additional payments, even if promised a refund.

3. Avoid opening further links or installing applications.

4. Do not delete messages or transaction records.

Second Priority: Contact Your Bank

1. Telephone your bank or payment provider immediately using its official contact details.

2. Explain what happened and identify suspicious transactions.

3. Ask about blocking accounts, cards, or further transfers.

4. Request an urgent payment recall or dispute where available.

Recovery is uncertain, but prompt reporting may help limit losses.

Third Priority: Secure Your Accounts

1. If passwords were exposed, change them using a trusted device.

2. Enable additional login protection.

3. Review important accounts for unfamiliar activity.

4. Contact relevant providers if identity or payment information was disclosed.

Fourth Priority: Protect Your Devices

1. If you installed malicious software or granted remote access, disconnect the affected device from the internet.

2. Stop using that device for banking.

3. Seek reputable technical assistance before using it for sensitive activities again.

Fifth Priority: Preserve Evidence and Report

1. Save messages, screenshots, payment receipts, website addresses, and contact details.

2. Record transaction amounts, dates, and reference numbers.

3. Report the incident to your local police or official fraud reporting authority.

4. Report fraudulent accounts to the relevant online platforms.

After the Immediate Emergency

Continue monitoring your accounts. Keep records of your reports and follow-up actions.

Beware of strangers promising to recover your money for an upfront fee.

Remember: Act as soon as you recognise the scam. You do not need to complete these steps in exactly 30 minutes.

Appendix D: 25 Common Scam Terms Explained in Simple English

1. **Phishing**: Fake messages designed to steal personal information or passwords.

2. **Smishing**: Phishing carried out through text messages.

3. **Vishing**: Fraudulent telephone calls used to obtain information or money.

4. **Spoofing**: Disguising a sender's identity, telephone number, or website address.

5. **Malware**: Harmful software designed to steal information or damage devices.

6. **Spyware**: Software that secretly monitors a user's activities.

7. **Ransomware**: Malware that locks files or systems and demands payment.

8. **Deepfake**: Artificially created or altered video, images, or audio.

9. **Voice Cloning**: Technology that imitates someone's voice.

10. **Artificial Intelligence (AI)**: Computer technology that performs tasks associated with human intelligence.

11. **Cryptocurrency**: Digital assets transferred through computer networks, often using blockchain technology.

12. **Blockchain**: A shared digital record of transactions.

13. **OTP**: One-time password used for a particular login or transaction.

14. **Two-Factor Authentication (2FA)**: Account protection requiring two different types of verification.

15. **Passkey**: A secure login method using cryptographic technology, often unlocked through your device.

16. **Password Manager**: Software that securely stores and generates passwords.

17. **Identity Theft**: Misusing someone's personal information to impersonate them.

18. **Impersonation Scam**: Fraud involving someone pretending to be a trusted person or organisation.

19. **Investment Scam**: Fraud involving false or misleading investment opportunities.

20. **Task Scam**: Fake work involving simple activities and demands for deposits.

21. **Money Mule**: Someone who receives or transfers money for criminals.

22. **Remote Access**: Technology allowing someone to control a device from elsewhere.

23. **Social Engineering**: Manipulating people into revealing information or taking harmful actions.

24. **Recovery Scam**: Fraud promising to retrieve previously lost money.

25. **Chargeback**: A card payment reversal requested through the card issuer, subject to applicable rules.

Appendix E: 20 Everyday Online Scam Scenarios

Fictional learning exercises. These situations illustrate possible scam attempts and appropriate precautions. They are not accounts of actual incidents.

1. **Bank Alert**: A message says your account is frozen. Contact your bank independently.

2. **Delivery Fee**: A courier message requests payment through an unfamiliar link. Check the official delivery service.

3. **Friend's Emergency**: A friend suddenly requests money. Telephone them using a known number.

4. **Cheap Smartphone**: An online seller offers an unusually low price. Investigate the seller before paying.

5. **Easy Job**: A recruiter promises generous earnings for simple tasks. Verify the employer.

6. **Paid Reviews**: A platform demands deposits before releasing commissions. Stop paying.

7. **Investment Guarantee**: Someone promises risk-free profits. Treat the guarantee as a warning sign.

8. **Government Official**: A caller threatens arrest unless you transfer money. Contact the agency independently.

9. **Technical Warning**: A browser pop-up displays a support number. Do not call it.

10. **Remote Repair**: A stranger requests control of your computer. Refuse access.

11. **Celebrity Video**: A famous person appears to endorse an investment. Verify the claim independently.

12. **Family Emergency**: A familiar-sounding voice urgently requests money. Call your relative directly.

13. **Online Friendship**: A new friend asks for financial assistance. Avoid sending money.

14. **Prize Notification**: A supposed winner must pay a collection fee. Investigate before responding.

15. **Password Reset**: An unexpected email requests your password. Visit the service independently.

16. **Verification Code**: Someone asks you to forward an OTP. Never share it.

17. **Fake Application**: A seller requires an unfamiliar payment app. Refuse the download.

18. **Account Transfer**: A recruiter wants to use your bank account. Decline.

19. **Recovery Agent**: Someone guarantees recovery of lost money for a fee. Verify independently.

20. **Changed Payment Details**: A supplier suddenly provides another bank account. Confirm through an established contact.

Remember: Stop, verify independently, and proceed only when you are satisfied the request is genuine.