UTILFORGE
FREE SAFETY TOOLS

HOW TO BECOME SAFER ONLINE

The five signs of a scam, and the checks that protect your family

A cybersecurity awareness guide for families, libraries and educators, from UtilForge.org



A registered 2026 Champion of Cybersecurity Awareness Month

Large print edition. The type in this book is set at 16 point, with generous spacing, so that it can be read without strain and photocopied without loss.

Free to copy. This book may be printed, photocopied, handed out and shared by anyone, for any number of people, as long as it is shared whole and unchanged, and nobody is charged more than the cost of printing it. Libraries, care homes, colleges, community groups, banks, employers and families are all welcome to do so without asking. A free copy to download is always at **utilforge.org/book**.

Licence. To make that permission formal, this book is published under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International licence (CC BY-NC-ND 4.0). In plain words: copy it and share it freely, credit UtilForge.org, do not sell it, and do not change it. The full licence is at creativecommons.org/licenses/by-nc-nd/4.0.

The checks. Every check this book describes can be used at UtilForge.org without paying, and runs on your own phone or computer, where what you type stays. UtilForge also offers packs of tools, which help keep the project going; nothing in this book depends on them.

Who wrote it. UtilForge.org makes free cybersecurity tools. It began inside one family. The founder’s mother and father, who were learning to use the internet, found payments they had never agreed to leaving their bank account. The checks in this book are the ones that family wished it had. UtilForge is a registered 2026 Champion of Cybersecurity Awareness Month, the October campaign led in the United States by the Cybersecurity and Infrastructure Security Agency and the National Cybersecurity Alliance.

What this book cannot do. No check can prove that a message is safe. The checks in this book find the common signs of a scam

and tell you what to do next. When money, a code or your details are involved, the last step is always the same: contact the company or the person yourself, using a number or an address you find on your own.

If a word is unfamiliar, such as phishing, deepfake or two-step login, the short glossary near the back of the book explains it in plain English.

Two words used throughout. A **scam** is a trick that gets you to hand over money, a code or your details to someone who is lying about who they are or what they want. A **check** is what you do before you act: a pause to find out whether a message, a call or an offer is what it says it is. The free pages at UtilForge.org that do this are called checks too.

The stories. The eight short stories in this book are fiction. The people, names, messages and events are invented, and any resemblance to a real person is coincidence.

They are built from the way these things really happen, and every one ends the way we would like things to end.

Dates. The facts in this book were checked in October 2026. Scams change. The habit does not.

First edition, October 2026.

Why this book exists

UtilForge.org has one aim: to help make a safer online world for all people.

The way to a safer online world is not fear, and it is not a list of things to avoid. It is awareness: knowing how the tricks work, and having something in your hand to check with. That is why UtilForge is a registered 2026 Champion of Cybersecurity Awareness Month, the October campaign that the Cybersecurity and Infrastructure Security Agency and the National Cybersecurity Alliance run in the

United States for everyone, everywhere. This year’s theme is “Don’t Make It Easy for Them”. This book is UtilForge’s contribution to that campaign.

So the order of this book is deliberate. First, the knowledge: how a scam is built, in five steps, so that you can recognise one you have never seen before. Then the measures: free checks that run on your own phone, so that knowledge turns into a habit. Then the people: how to pass both on, at a kitchen table or in a library, so that nobody is left to work it out alone.

A person who can check a message is a person who can use the internet with confidence, bank online, apply for jobs online, and stay in touch with family online. That is what digital inclusion means in practice, and it is why this book is free, in large print, and free to copy.

How to use this book

If you are reading for yourself, start with Part One. It is short: six chapters, one on the five steps and then one on each step. When you have read them, you will know the shape that most scams follow, and you will know what to check when a message does not fit it.

If you are looking for work, or studying, start with Chapter 9, “The job that asks you to pay first”, and the story “The visa fee”. Then come back to Part One.

If you are an educator, or the person your family asks, the librarian, the class leader, the family member everyone rings, the neighbour who “knows about computers”, Part Three is for you. It has a forty-five minute session you can run at a kitchen table, an afternoon to set up a phone together, the words to use, and the words to avoid.

If you run a library, a care home, a community group, a college or a workplace, the whole book is yours to print. Part Three has a session plan. Part Four is written to be handed out on its own. The five steps card is after Part Five, before the stories and the glossary, and a copy to print is at utilforge.org/book.

If you do not have a smartphone, the five steps (Chapters 1 to 6), the chapter on phone calls (Chapter 11), the family safe word (Chapter 15), the first phone call after a loss (Chapter 18) and the card all work without one. The checks themselves can be run on a library computer, or on the phone of someone you trust.

If something has already happened, go straight to Part Four, “If it has already happened”. It starts with the one phone call that matters most, and it says, because it is true, that this was not your fault.

Between and after the parts you will find short stories. They are made up. Every one ends with a person checking, or being helped to check, or being helped afterwards.

Two things the book will ask you to do

Copy and paste a message. On most phones: press and hold on the message until a small menu appears, then choose *Copy*. Open the check page, press and hold inside the empty box until *Paste* appears, and choose it. On an iPhone, the menu appears above the message; on an Android phone, it may appear at the top of the screen. If it does not work the first time, hold a little longer. If it does not work, hold a little longer.

Turn on aeroplane mode, to see for yourself. The checks keep working after the page has loaded, even with the phone cut off from the internet, because the check happens on the phone itself. To see this, open the page

first, then turn on *aeroplane mode*: on most phones, swipe down from the top of the screen and tap the aeroplane picture. Run the check. Then turn aeroplane mode off again. Do not reload the page while you are offline; it will not load, and that proves nothing either way.

Contents

Part One: The playbook 13

1. Most scams follow five steps 13
2. Step one: Pretend 18
3. Step two: Problem or prize 24
4. Step three: Pressure 28
5. Step four: Privacy 32
6. Step five: Pay 35

Part Two: The scams of 2026, and the check for each 50

7. The text that says you owe something 51

8. The message from “a family member, on a new number” 53

9. The job that asks you to pay first 54

10. The friend who wants to help you invest 58

11. The voice on the phone 61

12. The stranger who offers your money back 64

Part Three: For educators, and anyone a family asks 79

13. How people really get help 79

14. A forty-five minute session at a kitchen table 83

15. The family safe word 89

16. Set up a phone together 94

17. What to say, and what never to say 101

Part Four: If it has already happened 105

18. The first phone call 105

19. By how you paid 108

20. Where to report it, country by country 111

21. The second scam 119

Part Five: Four more habits (not scams) 123

22. The black box that was not really black 123

23. What you paste into an artificial intelligence 126

24. The words you cannot see 128

25. The VPN: what it protects, and when to switch it off 132

The five steps card (to cut out and keep) 137

Glossary of terms used in this book 156

Sources 164

Stories: The parcel · Thandi’s mother · The visa fee · The mentor · The safe word · Mr Okafor’s statement · The library at four o’clock · The kitchen table

PART ONE: THE PLAYBOOK

1. Most scams follow five steps

There are thousands of scams. Most of them follow the same few steps.

The parcel that cannot be delivered until you pay a small fee. The bank that needs you to move your savings to a safe account. The family member on a new number who needs a bill paid today. The recruiter with a job abroad, if you will just pay for the visa. The friend online who has found a way to make money, and wants you to join. The prize you have won in a draw you never entered.

They look different. Underneath, most of them are built from the same five steps, used for the same reasons. Some scams use several of the steps, and many use all five. Once you can see the steps, the disguise is much easier to see through.

Here they are.

1. **Pretend.** The scammer pretends to be someone you trust, or someone with authority over you.
2. **Problem or prize.** They bring you a fright or a reward, so that your feelings move faster than your thinking.
3. **Pressure.** They give you a deadline, so that you do not have time to check.
4. **Privacy.** They ask you to keep it to yourself, so that nobody can point out what is happening.
5. **Pay.** They ask for money in a form that is hard to trace and hard to get back: gift cards, a transfer to a new account, or cryptocurrency, which is digital money such as Bitcoin that can very rarely be called back once it is sent.

This is not a theory invented for this book. The Federal Trade Commission is the United States government's consumer protection agency. It describes four of these signs in its own plain words: scammers pretend to be an

organisation you know, they say there is a problem or a prize, they pressure you to act immediately, and they tell you to pay in a specific way. The fifth, secrecy, is documented by the Federal Bureau of Investigation. In September 2026 it warned that criminals pretending to be police officers and government officials were urging people not to tell their family, their friends, their bank or the police about the call. Between January 2025 and July 2026, the Bureau received nearly 61,000 complaints about that one kind of scam, with more than $1.6 billion reported lost.

Here is why the five steps matter more than any list of individual scams.

A list of scams goes out of date. The parcel text of this year is the toll-road text of last year and will be something else next year. If you learn the list, you are always one scam behind.

The five steps do not go out of date, because they are not about the disguise. They are about what the scammer needs from you. They need you to believe them. They need you to feel something strongly, and to hurry. They would rather you stayed quiet. And they need you to pay in a way that cannot be undone.

Here is the rule, and it is the most important sentence in this book: **if you spot any one of the five steps, stop and check first.** You do not need to find all five. Not every scam uses all five, and a message that is missing one is not safe because of that. One step is enough reason to pause.

That is the whole of this book: how to recognise one step, and what to do in the pause.

The habit that takes it away

The habit is to check first. Not to become suspicious of everyone, not to stop using your phone, not to live in fear. Just to put one pause between a message arriving and anything happening because of it.

UtilForge.org makes checks for exactly that pause. The first one is called *Is this a scam text message?* and its address is **utilforge.org/text**. You paste the message into the box on the page, press the button, and the page tells you which of the common scam signs it can see, and what to do next. It runs on your own phone. Once the page has loaded, it keeps working in aeroplane mode, with the phone cut off from the internet. What you paste stays on your phone.

When the check finds signs, it says so plainly. These are the real words it uses, and on the screen the first line is in capital letters. The results quoted in Part One and in Chapter 7

are shortened: the final line of each result and its “What to do” box are left out, and nothing else is changed:

> **Stop. This looks like a scam.** Do not pay, tap the link, call the number in it, or share any code.

When it finds none, it says that too, and it says something else that matters just as much: no check can prove a message is safe. The last step is always yours, and it is always the same. If money, a code or your details are involved, contact the company or the person yourself, using a number you already have or an address you type in yourself.

That is the habit. If you doubt it, check it.

---

2. Step one: Pretend

Every scam begins with a borrowed face.

The scammer does not arrive as a stranger. They arrive as your bank, your delivery company, the tax office, the police, a well-known shop, a recruiter from a company you have heard of, or a member of your own family. They borrow the name, the logo, the tone of voice, and increasingly the voice itself.

They do this because trust is faster than thought. When a message says it is from your bank, you start by reading what your bank wants, not by asking whether it is your bank. The pretending has already done its work before you reach the second sentence.

What pretending looks like in 2026

A message from a company you use. “Your parcel could not be delivered.” “Your account will be suspended.” “Your streaming payment failed.” The name is right. The colours are right. The web address is nearly right.

A message from an authority. “This is the fraud team.” “This is the court.” “You have an unpaid toll.” The Federal Bureau of Investigation’s September 2026 warning described callers who use artificial intelligence to appear on video calls as police or government officials. In some cases, the same warning says, the callers wear fake police uniforms and sit in mock sets of official buildings. The name or number that your phone shows for a caller can also be faked.

A message from family. “Hi Mum, I dropped my phone, this is my new number.” This one has its own chapter, because it is so common and because it works so well.

A voice. A short recording of someone’s voice, such as a voicemail greeting or a clip from social media, can be enough for some voice-copying software to make a convincing copy. No website can check a live phone call, and this book will say so more than once. There is a defence, and it is in Chapter 15.

What the check sees

Paste this message into *Is this a scam text message?* at utilforge.org/text, as one reader did with a text that arrived on a Tuesday morning:

> Hi Mum, I dropped my phone in the bath, this is my new number. I need to pay a bill today and my banking app is locked. Can you help? Please don’t tell Dad yet.

The check says:

Stop. This looks like a scam.

It is written as if it comes from a family member, and it involves money. Scammers pretend to be a family member. Check by calling them on the number you already have for them.

It sounds like a family member on a new number. The “Hi Mum, I lost my phone” message is a well-known scam, and it usually ends with an urgent bill to pay.

It asks you to keep it secret. Scammers say “don’t tell anyone” so that nobody can stop you and point out the scam. Someone who loves you will understand if you check first.

It rushes you with a deadline. Pressure to act now is how scams stop people from checking.

Four reasons, four steps, in one short message: pretend, problem, privacy and pressure. The fifth, pay, is what the next message would have asked for.

How to take this step away

You do not have to decide whether the message is real. You only have to reach the real person or company by a route the scammer does not control.

- **Family:** call them on the number you already have for them. If the “new number” is real, the old one will not answer, and nothing is lost by trying. If it is not, you have just saved yourself. If the old number really does not answer, reach them another way before any money moves: ring someone who lives with them, start a video call yourself, or ask for the family safe word (Chapter 15).
- **A company:** open its own app, or type its web address yourself, or ring the number printed on your card or your bill. Never use the number or the link in the message.
- **An authority:** no police force, court or tax office asks to be paid in gift cards or cryptocurrency, or through a link in a text

message, and none of them will mind if you hang up and ring the number on their official website.

The scammer’s borrowed face only works on the channel they chose. Step off it, and the face falls away.

---

3. Step two: Problem or prize

Once the scammer has a face you trust, they need you to feel something. Fear or hope will do. Either one moves faster than thinking.

The problem

A parcel is held. An account is about to be closed. A payment has failed. There is a warrant. There is a virus. A family member is in trouble. Someone is taking money from your account right now.

The problem is always just plausible enough. Most of us are expecting a parcel. Most of us have a subscription somewhere. Most of us have, at some point, worried about our bank account. The scammer is not guessing about you. They are guessing about everyone, and sending the same message to a million phones, knowing that for some of them it will land on exactly the right day.

The prize

You have won. You have been selected. You have been chosen for a job without applying. A refund is waiting. A tax rebate is yours to claim. A famous investor’s method is available to you, today only.

The prize works on the same principle as the problem. It makes you want the message to be true, and wanting something to be true is the surest way to stop checking whether it is.

The small fee

The most effective problem of all is a small one. A redelivery fee of $1.99. A customs charge of a few pounds. A toll of $4.15.

Here is a typical message, and what the check at utilforge.org/text says about it. (The web addresses in this book’s example messages end in “.example”, an ending that can never be registered, so that nobody can ever set up the pages they point to.)

> Your parcel could not be delivered. A redelivery fee of $1.99 is due. Pay within 12 hours: https://parcel-redeliver.example

> **Stop. This looks like a scam.**
>
> It says a parcel is held until you pay a small fee or confirm your address. Scam messages often ask for a small fee so that paying feels harmless. Some delivery companies do send genuine texts about customs fees, so never pay through the link in the message. Open the company's own website or app yourself and check the tracking number there.
>
> It contains a link. Do not tap it. Go to the company's website or app yourself instead.

The $1.99 was never the point. The point was the page where you typed your card number to pay it.

How to take this step away

Notice the feeling. That is all. When a message makes your stomach drop or your heart lift, that feeling is information. It tells you

that step two has just been played, and that this is the moment to pause rather than the moment to act.

Then go to the source yourself. If the parcel is real, it is in the delivery company's own app under your tracking number. If the account problem is real, it is in your bank's own app. If the prize is real, it will still be real tomorrow, after you have checked. An unexpected prize is always worth checking first.

---

4. Step three: Pressure

If you had a day to think, you would check. The scammer knows this. So they take the day away.

Pay today. Within twelve hours. Claim within twenty-four hours or it goes to the next winner. Your account closes at midnight. The officer is waiting on the line. The visa window shuts on Friday.

Pressure is the step that connects the feeling to the payment. Step two made you anxious or hopeful. Step three stops that feeling from cooling down.

What pressure looks like

- A countdown: “within 12 hours”, “before 5pm today”, “only three places left”.
- A consequence: suspension, arrest, a late fee, a missed opportunity, a family member left stranded.
- A person who will not let you off the phone. The Federal Bureau of Investigation’s September 2026 warning described callers who keep the person on the phone for the whole of the scam, so that there is never a quiet moment to check.
- A friendly kind of pressure: “I’m only here for the next ten minutes, let’s get this sorted for you now.”

What the check sees

> Congratulations! Your number has won a 1,000 dollar prize. Claim within 24 hours or it goes to the next winner: https://claim-reward.example/win

> **Stop. This looks like a scam.**
>
> It says you have won something. You cannot win a draw you did not enter, and a real prize never needs a fee before you receive it.
>
> It rushes you with a deadline. Pressure to act now is how scams stop people from checking.
>
> It contains a link. Do not tap it. Go to the company’s website or app yourself instead.

How to take this step away

Here is the one sentence to remember: **a real deadline will still be there after you check**, and the real organisation, reached on a

number you found yourself, can tell you what it is.

A real parcel is still at the depot tomorrow. A real bank does not close your account for failing to tap a link. A real employer can wait a day for your answer. A real court does not demand payment there and then, over the phone, in gift cards or cryptocurrency. The only deadlines that vanish when you pause are the ones that were invented to stop you pausing.

So pause. Put the phone down. Make a cup of tea. Ring the person you trust. Paste the message into the check. The scammer’s whole plan depended on you not having that ten minutes. Take it.

---

5. Step four: Privacy

This is the step that gives the scam away. It is also the step that scammers rely on most, because it removes the one thing that beats them every time: another person.

“Don’t tell anyone at your branch, as staff may be involved.” “Please don’t tell Dad yet.” “Keep this between us.” “This is a confidential investigation.” “Your family won’t understand.” “Don’t mention this to the shop assistant when you buy the cards, or they’ll cancel your account.”

Every one of these is the same request. Do not let a second pair of eyes see this.

Why it works

Shame does the scammer’s work for them. People who have been drawn halfway into a scam often feel foolish before anything has even gone wrong, and that feeling makes them less likely to ask for help, not more. The

scammer feeds it. “You’re clever to have spotted this; most people don’t.” “Let’s not worry your family with it.”

The Federal Bureau of Investigation’s September 2026 warning about fake police and government callers put it plainly: the callers urge people not to tell their family, their friends, their bank or the police. The Federal Trade Commission’s advice is the opposite instruction: stop, and talk to someone you trust. In our experience, a request for secrecy about money is one of the strongest warning signs there is.

What the check sees

> This is your bank’s fraud team. Someone is trying to take money from your account. To protect it, move your savings to a safe account today. Do not tell anyone at your branch, as staff may be involved.

> **Stop. This looks like a scam.**
>
> It claims there is a problem with your bank or account and asks you to act. A real bank will never ask you to move money to a “safe account” or to confirm details through a link.
>
> It asks you to keep it secret. Scammers say “don’t tell anyone” so that nobody can stop you and point out the scam. Someone who loves you will understand if you check first.

That last sentence is worth reading twice. *Someone who loves you will understand if you check first.* It is the answer to every version of “don’t tell anyone” that you will ever receive.

How to take this step away

Tell someone. That is the whole instruction.

It does not matter who. A family member, your neighbour, the librarian, the person at the next desk, the shop assistant selling you the gift cards. Scammers usually lose the moment a second person hears the story, because the

second person has not been through steps one, two and three. They are not frightened, not hopeful and not hurried. They can see the shape.

And if the message was from your bank, your bank will not mind that you told someone. Only a scammer minds.

---

6. Step five: Pay

Everything before this was preparation. This is the step the scammer was working towards, and it is the step where the money leaves.

Notice what they ask for. Not a cheque. Not a card payment to a company with a name and an address and a refund policy. They ask for the forms of money that move instantly, are hard to trace to a person, and are hard to call back.

The forms of payment scammers ask for

- **Gift cards.** You buy them at a shop, scratch off the code, and read the code to the caller or photograph it. The value is gone the moment the code is read. No real bank, government agency or court asks to be paid in gift cards.
- **Cryptocurrency**, digital money such as Bitcoin, including cash fed into a cryptocurrency cash machine, which is a kiosk in a shop that turns notes into cryptocurrency. Once sent, it is rarely recovered.
- **Bank transfers to a “safe account”.** Your own bank’s fraud team will never ask you to move money to a new account to protect it. Only a scammer does.
- **Money transfer services** and **payment apps**, where the money reaches a person, not a company, and reaches them at once.
- **Your card details, typed into a page the scammer built**, which is what the $1.99

parcel fee was always for.

What the check sees

> Your account will be closed today. To keep it open, pay the 500 dollar fee in gift cards and send photos of the codes to this number. Do not tell the shop what they are for.

Pasted into *Before You Pay* at utilforge.org/pay, after choosing “I got a message asking me to pay, tap a link or send a code”:

> **Stop. This looks like a scam.**
>
> It claims there is a problem with your bank or account and asks you to act.
>
> It mentions paying with gift cards, vouchers, cryptocurrency or a money transfer service. Scammers ask for these because the money cannot be traced or returned.

How to take this step away

Before any payment that you did not plan to make this morning, check first. Not because every unexpected payment is a scam, but because this is the last moment at which checking costs nothing.

Ask yourself three questions:

1. **Did I start this?** Did I go looking for this payment, or did it come looking for me?
2. **How am I being asked to pay?** If the answer is gift cards, cryptocurrency, a transfer to a new account or a money transfer service, stop.
3. **Have I told anyone?** If the answer is no, that is step four, and the answer to step four is always the same.

If the payment is real, you will be able to make it tomorrow, through the company’s own app or website, after you have checked. If it is not, you have just kept your money.

The five steps together

Pretend. Problem or prize. Pressure. Privacy. Pay.

You do not need to spot all five, and you should not wait until you have. Most scams use several of these steps, and the ones in Part Two show which. Some leave one out: the toll text asks for no secrecy, and the slow investment scam has no deadline for months. A missing step never makes a message safe.

Spot any one step, and that is your signal: stop, and check first. If the message is real, checking costs you ten minutes. If it is not, checking is the whole defence.

THE PARCEL

A story

Margaret Oyelaran had been waiting for the cardigan since Thursday.

It was not an important cardigan. It was lavender, and it was for her sister's birthday, and her sister would say it was too bright for her and then wear it every day until spring. That was the whole plan. The plan depended on the cardigan arriving.

So when the text came on Monday morning, between the kettle boiling and the radio news, she felt the small drop in her stomach that the sender had been counting on.

Your parcel could not be delivered. A redelivery fee of £1.45 is due. Pay within 12 hours to avoid return to sender: https://parcel-redeliver.example

There was the link. Her thumb was already moving towards it.

What stopped her was not suspicion. It was the kettle. It clicked off, and she put the phone down to pour the water, and in the twelve seconds that took, the feeling cooled by one degree. Just one. Enough to notice it had been there.

Her friend Joy had shown her the check in August, on the day she had moved into the new flat. “Margaret, anything that asks you for money, you put it in here first. It all happens on your phone. Look, I’ll put the phone in aeroplane mode and it still works.” Margaret had nodded, and had not expected to need it.

She found the page. It was called *Is this a scam text message?*, which struck her as a sensible name for a thing. She pressed on the message until it copied, pasted it into the box, and pressed the black button.

Stop. This looks like a scam.

Below that, in plain words, it told her what it had seen. A parcel held for a small fee. A link. It told her that some delivery companies did send real messages about customs charges, so she should not assume, but that she should never pay through a link in a message. It told her to open the delivery company’s own app or website herself and look up the tracking number there.

She did. The cardigan was in a van. It would arrive between two and four.

Margaret sat down with her tea and felt, to her own surprise, rather pleased with herself. She now knew something she had not known at eight o’clock: the shape of the thing. A small fee, a deadline, a link. She would know it next time without the kettle.

At ten past two the doorbell went. The driver was a man with a scanner and an apologetic smile, and he had no idea that he was the end of a story.

“Sign here, love. No charge.”

“No,” said Margaret. “I didn’t think there would be.”

She told her sister about it on the birthday itself, over the lavender cardigan, which was indeed too bright for her and which she did not take off all afternoon.

“Send it to me,” her sister said. “The page. Send me the page.”

So she did. That is how it spreads. Not through adverts. Through sisters.

THANDI'S MOTHER

A story

The message came at 11.40 on a Wednesday night, which was the first thing Nomvula noticed, because Thandi never texted after ten.

Hi Ma, it's me. I dropped my phone in the bath, this is my new number for now. I'm so stressed, I need to pay the rent deposit by tomorrow morning and my banking app is locked on the new phone. Can you send it from your side and I'll pay you back on Friday? Please don't tell Dad yet, he'll just worry.

Nomvula read it twice. It sounded like Thandi. The "I'm so stressed" sounded like Thandi. The "he'll just worry" sounded exactly like Thandi, who had spent twenty-six years protecting her father from things he would have been perfectly fine about.

She had the banking app open before she had finished thinking.

What she did next, she could not fully explain afterwards. She said it was the time. She said it was the “new number”. She said it was the fact that Thandi, who was a nurse, did not use the word “deposit”, she said “the money for the flat”. Whatever it was, Nomvula put the phone face down on the kitchen table and looked at it for a while as if it might do something.

Then she picked it up and rang Thandi. Not the new number. The old one. The one that had been in her phone, under *Thandi* and a small red heart, since 2019.

It rang four times.

“Ma? It’s nearly midnight. Is Dad okay?”

Nomvula found that she had to sit down.

“Where is your phone?”

“It’s… in my hand, Ma. I’m talking to you on it. What’s going on?”

So she told her. And Thandi, who was a nurse and had seen a great many frightened people, did not say *Ma, how could you nearly fall for that.* She said, “Oh, Ma. Oh, I’m so glad you rang. Send it to me. The message. Let me see what they wrote.”

They sat up together, three hundred kilometres apart, and looked at it. Thandi pasted it into a check on her own phone and read the result out loud. It said the message was written as if it came from a family member and involved money. It said the “Hi Mum, I lost my phone” message was a well-known scam that usually ended with an urgent bill. It said the message asked her to keep it secret, and that someone who loved her would understand if she checked first. It said: check by calling them on the number you already have.

“That’s what you did,” Thandi said. “You did the thing it says to do. You did it before you even looked.”

“I nearly didn’t.”

“But you did.”

There was a pause on the line, the kind of pause that only happens between people who have known each other a long time.

“Ma. The ‘don’t tell Dad’ part.”

“I know.”

“That’s the bit that should have told you. A scam wants you kept away from the people who could help. That’s what that line is for.”

Nomvula looked across the dark kitchen towards the bedroom, where the person she shared a bed with was snoring in the particular rhythm he had used since 1991.

“I’m going to tell him in the morning,” she said.

“Tell him tonight,” said Thandi. “Wake him up. It’s a good story. He’ll like it.”

He did.

They agreed a word that weekend, the three of them, around the same kitchen table. A plain word, nothing anyone could guess from a photograph. They said it once each, there in the kitchen, and that was the only place it was ever said. Thandi printed the card from the website, the one with the three rules and a line for each name, and stuck it to the fridge with the magnet from the hospital. The word itself she did not write on it.

“If I ever ring you and ask for money,” she said, “you ask me for the word. Even if it sounds like me. Especially if it sounds like me. And if I can’t give it, you hang up and ring me back on this number.”

Her father read the card and nodded.

“And if you tell it to anyone who rings you,” said Thandi, “we need a new one.”

“Who’s going to ring me and ask? The fridge?”

The card is still on the fridge. The word is not on it. It is in three heads, and that is where it stays.

PART TWO: THE SCAMS OF 2026, AND THE CHECK FOR EACH

The five steps are the shape. This part is the detail: the six scams that official bodies were warning about most often as this book went to print. For each one: what it looks like on your screen, which steps it uses, which free check catches it, and what the check actually says.

Every message quoted here was pasted into the real check on 18 October 2026, and every result is in the check's own words. On the screen, the first line of a result is in capital letters. The results in Part One and in Chapter 7 are shortened, as Chapter 1 says; the rest are complete. Notice, as you go, that not every scam uses all five steps. Any one of them is reason enough to check.

---

7. The text that says you owe something

What it looks like. A text message says you owe a small amount to someone official. An unpaid road toll. A parking fine. A customs charge. A missed delivery. It gives a deadline and a link.

These texts are sent by the million. In November 2025, Google took one text-message scam operation to court. Google said the operation, which sent parcel and toll messages, had harmed more than a million people in more than 120 countries.

Which steps it uses. Pretend (a road agency, a delivery company). Problem (you owe something). Pressure (pay today). Pay (your card details, typed into their page). No request for secrecy: four steps, not five, and still a scam.

The check. *Is this a scam text message?*, at utilforge.org/text.

> Road toll notice: You have an unpaid toll of $4.15. Pay today to avoid a $50 late fee and suspension of your licence: https://tollpay-notice.example/pay

> **Stop. This looks like a scam.**
>
> It says you owe a toll, a fine or a parking charge. Fake fine messages are common. Check with the road agency or council using their own website.
>
> It rushes you with a deadline. Pressure to act now is how scams stop people from checking.
>
> It contains a link. Do not tap it. Go to the company’s website or app yourself instead.

What to do. Do not tap the link. If you think you might owe something, go to the agency’s own website, by typing its address yourself, and look it up there. If you already tapped and

typed your card details, ring the number on the back of your card now and tell the bank what happened. Part Four has the rest.

---

8. The message from “a family member, on a new number”

What it looks like. “Hi Mum” or “Hi Dad”, from a number you do not know. A dropped phone, a broken phone, a stolen phone. A reason the banking app will not work. A bill that must be paid today. Often, a request to keep it quiet.

It is sent to thousands of people at once. Most of them do not have a family member who has just lost a phone. The scammer only needs the few who do.

Which steps it uses. All five, in one short message. Pretend (a family member). Problem (locked out, bill due). Pressure (today). Privacy (“don’t tell Dad”). Pay (a transfer to a new account).

The check. *Is this a scam text message?*, at utilforge.org/text. Chapter 2 shows the full result for a message like this. The key line:

> Check by calling them on the number you already have for them.

What to do. Ring the old number. If the story is true, the old phone will not answer and you have lost nothing. Then reach them another way before any money moves: someone who lives with them, a video call you start yourself, or the family safe word. If the story is false, you have just saved yourself and, by telling your family, you have warned the next person. Then agree a family safe word (Chapter 15), so that next time the question answers itself.

---

9. The job that asks you to pay first

What it looks like. A message, often on a messaging app, often from someone calling themselves a recruiter. You have been

selected. There is a job, sometimes abroad, sometimes “online, from home, a few hours a day”. The salary is good. There is housing, or flexibility, or a famous company’s name. Then there is a fee: for the visa, for training, for equipment, for a background check, for “activating” your account. And a request for your passport or your bank details.

Australia’s National Anti-Scam Centre reported that job scam losses reported to Scamwatch rose by 81.5 per cent in 2025, and that reports from people aged 25 to 34 more than doubled.

Two patterns stand out:

- **The task job.** You are paid small amounts for “liking” products or completing simple tasks, then asked to deposit money to “unlock” larger earnings. The deposit is the scam.
- **The job abroad.** A good job in another country, with the visa arranged for you, if you pay the fee. In 2026 the United

Nations Human Rights Office and the United Nations Office on Drugs and Crime both reported on fake job offers of exactly this kind. People from dozens of countries have answered them, travelled, and been held in guarded compounds in South-East Asia, forced to run scams on others. The fee is the least of what those offers cost.

Which steps it uses. Pretend (a recruiter, a known company). Prize (the job). Pressure (places are limited). Pay (the fee, and your documents). Four steps.

The check. *Before You Reply to a Recruiter*, at utilforge.org/jobs.

> Dear candidate, congratulations! You have been selected for a hotel job abroad, salary 2,800 dollars a month with free housing. To process your work visa, pay the visa fee of 350 dollars today. Send a copy of your passport on WhatsApp. Places are limited.

Stop. Do not pay or send documents yet.

This message matches patterns that United Kingdom, United States and South African agencies warn about. Find the company yourself, contact it using details from its own website, and talk to someone you trust before you reply.

It names a fee or deposit you must pay. A real employer does not charge a candidate to register, train, start or be checked. Report Fraud lists fees for training, equipment, visas and security checks as warning signs.

It offers the job without an interview, or says you were selected. Check that you applied to this company, and that a person from it has spoken to you.

It mentions visas, travel or accommodation arranged through an agency. Report Fraud describes job offers abroad that ask for fees for visas, training or equipment, and pressure to use particular agencies.

(Shortened. The check found six warning signs in that one message; three are shown here. Report Fraud is the United Kingdom's police reporting service.)

What to do. You should never have to pay to apply for a job, to start one, or to be checked for one. Find the company yourself, through its own website, and ask whether the job exists. If you have already paid or sent your passport, press the button on the same page that says "I already paid or sent documents", and read Part Four of this book.

---

10. The friend who wants to help you invest

What it looks like. This one is slow. It begins as a wrong-number text, a message on a dating app, a friendly comment on social media, or a new contact who seems to share your interests. For weeks, nothing is asked of you. Then your new friend mentions how well

they have done with an investment, usually in cryptocurrency, and offers to show you. You start small. The app shows your money growing. You put in more. When you try to take it out, there are fees, taxes, problems. Then your friend is gone.

Of all the scams where people are talked into paying, investment scams take the most money, in every country whose figures this book's authors checked: the United States, the United Kingdom, Australia and Canada. The Federal Bureau of Investigation runs Operation Level Up, which contacts people while they are still being scammed. In its report on 2025, published in April 2026, the Bureau said that 78 per cent of the 3,780 people it reached that year did not yet know they were being scammed. The relationship is the disguise.

Which steps it uses. Pretend (a friend, a mentor, a trading platform). Prize (the returns). Pressure (a window that is closing, a price that

is rising). Privacy (your family “wouldn’t understand”). Pay (cryptocurrency, transfers).

The check. *Before You Invest*, at utilforge.org/tools/before-you-invest, takes an offer through eight questions. It shows how to find the firm on your country’s financial register, which is the official list of firms allowed to handle people’s money. And it puts one question above all the others: *what happens if I wait a week? A real opportunity is still there after you have checked it. A scam depends on you not waiting.* For this scam in particular, add three human questions of your own:

- Did you choose how you met this person, rather than them arriving in a message you did not ask for?
- Have you met them in person, or through people you already know? A video call is no longer proof on its own: the Federal Bureau of Investigation warned in 2026

that scammers use artificial intelligence to appear on live video.

- Can you take your money out today, without a fee or a tax that nobody mentioned when you put it in?

If any answer is no, stop, and tell someone before any more money moves.

What to do. Talk to someone who is not inside the relationship. Your bank's fraud team will take the question seriously. If you have already invested, ring your bank now, and read Chapter 21, because people who have lost money this way are then targeted by the scam in that chapter.

---

11. The voice on the phone

What it looks like. A call. The voice is your bank's fraud team, or the police, or a court officer, or a government department. Sometimes it is a voice you know: a family

member, a friend, a boss. They are calm and authoritative, or frightened and in trouble. Either way, something must happen now.

The Federal Bureau of Investigation's September 2026 warning described the current version. The caller accuses you of missing a court date or owing a fine. They keep you on the phone for the whole of the scam. They urge you to tell nobody: not family, friends, your bank or the police. They ask for payment by prepaid card, by courier, by wire, or by cash fed into a cryptocurrency machine. Some use artificial intelligence to appear on video calls as police or government officials, and in some cases they wear fake uniforms and sit in mock sets of official buildings. The name or number your phone shows for the caller can be faked too.

And a voice can now be copied from a short recording. A family member's voice, in distress, asking for help.

Which steps it uses. All five, live, with a human being applying them in real time.

The check. There is no website check for a live phone call. This book will not pretend otherwise. UtilForge's checks read messages; they cannot listen to your phone. What there is instead is older, and it works:

1. **Hang up.** You are allowed to. A real bank, a real police force and a real court will not be offended.
2. **Ring back on a number you find yourself:** the number on your card, on your bill, or on the organisation's own website, typed by you.
3. **For family, ask for the safe word** (Chapter 15). A voice can be copied. A word your family agreed in private and never typed is much harder to get hold of. It is one more check, not a guarantee, and if the word does not come, the answer is the same as step two: hang up and ring back on the number you already have.

If you use a landline, wait a few minutes before you ring back, or use a different phone. Some scam calls can keep an old-style line open after you have put the receiver down.

What to do. No police force, court, tax office or bank asks to be paid in gift cards, cryptocurrency or cash handed to a courier. If a caller asks for any of these, the call is a scam, whatever name or number your phone shows.

---

12. The stranger who offers your money back

What it looks like. You have already lost money to a scam. Then someone gets in touch. A law firm, a recovery agency, a government unit, a “fraud investigator”. They know about your loss. They can get the money back. There is a fee first: a retainer, which is a lawyer’s advance fee, or a processing charge, or a tax.

The Federal Trade Commission describes this as a scam aimed at people who have already been scammed. In July 2026, the Federal Bureau of Investigation warned about a deepfake video, a fake video made by a computer, of one of its own senior officials, promoting a fake version of its complaint website. It was aimed at exactly these people. The Canadian Anti-Fraud Centre recorded tens of millions of dollars lost in 2025 to fake recovery services and fake fraud investigators.

Which steps it uses. Pretend (a law firm, an agency). Prize (your money back). Pressure (the case closes soon). Pay (the fee first).

The check. This one has a guide rather than a tool: “Someone offers to get your money back”, at utilforge.org/learn/someone-offers-your-money-back. Its warning signs:

- They contacted you, not the other way round.

- They say they are from a government agency, a charity or a law firm.
- They ask for a payment first, and call it a retainer or a processing fee.
- They want it in gift cards, cryptocurrency, a wire transfer or a payment app.
- They ask for personal details, such as an identity number or your bank details.
- They offer to deposit a refund for more than you lost, then ask you to send the difference back.

What to do. Never pay up front for help recovering money. Real recovery, where it is possible at all, comes through your own bank and through official reporting, and neither charges a fee to begin. If you have lost money, Chapter 18 is where to start.

THE VISA FEE

A story

Daniel was twenty-three, had a hospitality diploma, and had sent out forty-one applications since March. He kept them in a spreadsheet. Column F was “Outcome”, and column F was mostly blank.

So when the WhatsApp message came, he read it standing up.

Dear candidate, congratulations! Your profile has been reviewed and you have been selected for a Front Office position at a five-star hotel abroad. Salary 2,800 USD per month, free staff housing, flights provided. To process your work visa, a visa fee of 350 USD is payable today. Please send a copy of your passport data page to this number. Places are limited.

He had not applied for a job abroad. But he had put his profile on three job sites, and “your profile has been reviewed” explained that. The message used a real hotel’s name; he looked it up. The salary was more than twice what he would earn at home. The message was polite and properly spelled, and it had a logo. (USD is United States dollars.)

He had 350 dollars. Just. It was the money for the next three months of applications, the bus fares and the printing and the one good shirt.

He did not send it. He wants that to be clear, when he tells this story now. He did not send it. But he had the banking app open, and he had typed the amount, and his thumb was over the button, and he was already imagining telling his mother.

It was his mother he thought of. Not because she would have stopped him; she would have been as excited as he was. He thought of her

because the last time he had been this excited about something, she had said, “Check it, Danny. Ask someone who isn’t you.”

The someone who was not him was Mr Adebayo, who ran the career desk at the library on Thursdays and had a sign on his table that said *NO QUESTION IS STUPID*.

Mr Adebayo read the message without expression. Then he turned his own screen round.

“Paste it in here.”

The page was called Before You Reply to a Recruiter. Daniel pasted the message and pressed the button, and the screen went pale red.

Stop. Do not pay or send documents yet.

Below that, five reasons, each one a sentence or two. It named the fee. It said a real employer does not charge a candidate to register, train, start or be checked. It noted that

he had been “selected” without an interview, and told him to check whether he had actually applied to this company and whether a person from it had spoken to him. It said that job offers abroad that arrange the visa through an agency and ask for a fee are a pattern that fraud agencies warn about. It said the passport request was a warning sign before any written offer.

“Five,” said Mr Adebayo. “I’ve seen eight. Five is a solid result.”

Daniel laughed, which surprised him.

“Now,” said Mr Adebayo, “the part people skip. Find the hotel yourself.”

They did. The hotel’s own careers page had no Front Office vacancy. It had a line, in red, near the top: *We never ask candidates to pay any fee at any stage. Report any such request to us.* There was an email address. Daniel wrote to it, with the WhatsApp number, from the library computer.

“Will they do anything?”

“Maybe. Maybe they warn the next person. That’s something.” Mr Adebayo closed the tab. “You know what the worst part of that message was? Not the money.”

“The passport.”

“The passport. Money you can earn again. Your passport in a stranger’s hands is months of trouble. Part Four says what to do if it has already gone.” He looked at Daniel over his glasses. “You came here before you sent it. Remember that about yourself.”

Daniel did not get a job abroad. He got a job in October, at a conference hotel forty minutes from his mother’s house. He works on the front desk, where part of his job is checking that people are who they say they are.

Column F says *Started 6 October*.

He still has the message. He uses it, sometimes, with the new starters who come through on placements and who have forty-one applications out and a thumb hovering over a button.

“Paste it in,” he says. “Ask someone who isn’t you.”

THE MENTOR

A story

The first message was a wrong number.

Hi Linda, it's Anna from the pottery class, are we still on for Saturday?

Robert wrote back to say she had the wrong number, because he was the kind of man who wrote back. Anna apologised. She was charming about it. She asked, since they were already talking, where he was writing from, and he told her, and it turned out she had a cousin there.

That was in February. By April they messaged most days. Not about anything. The weather. Her dog. His garden. His wife, who had died two winters before, and whom he found he could talk about to Anna in a way he could not to his sister Helen, who got that look.

In May, Anna mentioned, in passing, that she had done rather well with something. She did not push it. She said a friend had shown her a trading platform. She sent a screenshot. Robert said that was nice for her, and meant it.

In June she asked if he wanted to see how it worked. Just to see.

He put in two hundred. The app showed it become two hundred and forty in a week. He put in two thousand. He could see it, every morning, a number going up. It was the first thing he looked at after the garden. Anna was delighted for him. She said he had a feel for it.

By August it was eleven thousand, on the screen, and he had put in nine. He mentioned to Helen, carefully, that he had been doing a bit of investing. Helen got the look.

“Rob. Who’s Anna?”

“A friend.”

“Have you met her?”

“We talk every day.”

“Have you *met* her, Rob. In person. Or does anyone you know, know her?”

He had not, and nobody did. There had always been a reason. Her camera. Her signal. Her cousin visiting.

Helen did not shout. She said, “Can I show you something? It’ll take two minutes, and then if I’m wrong, I’ll shut up about it.”

She opened a page on her phone called Before You Invest, and she did not type anything into it. She read one line from it aloud: *What happens if I wait a week? A real opportunity is still there after you have checked it. A scam depends on you not waiting.* Then she put the phone down and asked three questions of her own, and after each one she waited.

“Did you choose how you met Anna, or did she arrive in a message you weren’t expecting?”

“Have you ever met her in person, or through anyone you already knew? Because a video call isn’t proof any more, Rob. They can fake those now.”

“Can you take your money out today, without paying a fee nobody told you about?”

Robert did not answer the third one. He opened the app and pressed Withdraw, and a message appeared that he had never seen before, because he had never tried before. A tax of 20 per cent was payable before funds could be released. There was a button to pay it.

He put the phone down.

What Helen said next is the reason this story is in this book.

She did not say *I told you so.* She did not say *how could you.* She said, “Rob, this is designed by professionals to do exactly what it did. It got you because you’re kind and you

were lonely and you answer wrong numbers. Those aren’t flaws. Can I ring the bank with you?”

They rang the bank. Some of the money came back. Most of it did not; it had gone into cryptocurrency and out the other side within hours of each payment, the fraud team said, in a voice that had said it many times. They reported it. The bank told him, kindly, that someone might now contact him offering to recover the rest for a fee, and that this person would also be a scammer.

Two weeks later, someone did.

Robert did not reply. He sent the message to Helen, with one line: *Chapter twelve.*

He still gardens. He still answers the phone. He has not stopped being kind, and he has not stopped talking to strangers, because Helen was right that these were not flaws. He has

added one thing. Before any money moves, anywhere, to anyone, he says the sentence Helen taught him, out loud, to the kitchen:

“Ask someone who isn’t me.”

Then he does.

PART THREE: FOR EDUCATORS, AND ANYONE A FAMILY ASKS

13. How people really get help

If you are reading this part, you are probably the person your family rings. Or you run the Thursday afternoon session at the library, or a class, or a staff briefing. Or you are the carer, the neighbour, the family member who “knows about phones”. This book calls all of these people educators, because that is what they do, whether or not it is their job. This part is written for you, and it begins with the belief this book is built on.

People rarely get safety help from adverts. They get it from people.

Two pieces of evidence point that way. In the United States, the Public Library Association’s 2025 survey, published in June 2026, found

that 83 per cent of public libraries offer at least one programme for people aged 65 and over, and that 73 per cent work in partnership with senior centres and similar organisations. And in a 2015 survey published by the Pew Research Center in 2017, nearly three in four Americans over 65 said that when they got a new device, they usually needed someone else to set it up or show them how to use it.

The same is true at every stage of life. Job seekers go to their careers service, or ask the person who got the last job. Families ask the one relative who reads the terms and conditions.

So the way to protect someone is rarely to send them a video. It is to sit beside them, once, for forty-five minutes, and do the check together on their own phone. After that, the habit belongs to them.

What an educator is, and is not

An educator shows a check on their own device, then watches the other person run it on theirs. An educator does not take control of anyone’s phone or computer. An educator does not keep copies of anyone’s bank statements, identity documents or passwords. And an educator follows the safeguarding rules of any organisation they work with, which are the rules that protect the people being helped, including any background check that organisation requires.

An educator is not a replacement for a bank’s fraud team, the police or security software. When money has already gone, the educator’s job is to make the phone call to the bank easier, not to make it themselves, and then to point to the official reporting service in Chapter 20.

What makes the habit stick

Research on fraud prevention points to the same conclusion from several directions.

A single warning works, for a while. In 2021 the Investor Education Foundation of the Financial Industry Regulatory Authority, in the United States, published a fair test with groups chosen at random. A three-minute warning cut people’s willingness to invest in fraudulent pitches by about 40 per cent, straight afterwards. Six months later, people who had only had the warning were no better than people who had never seen it. People who had been given a reminder at three months were still about 10 per cent less willing.

Habits that are practised last longer than facts that are heard. Google’s 2025 trial of a short scam-spotting game with 3,000 people in India found that the gains were still there at the three-week follow-up, and that playing the game worked better than watching videos and reading tips.

And frightening people works better when it comes with something to do. A large review of fear-based health campaigns, published in 2015, found that frightening messages work better when they come with a clear action the person can take, and better for one-off actions than for habits that must be repeated.

That is why this book keeps saying the same five words, and why the session below has everyone run a check with their own hands rather than watch one. The aim is not to frighten anyone. The aim is to make “check first” as ordinary as locking the door.

---

14. A forty-five minute session at a kitchen table

This session plan is based on UtilForge’s free session plan at utilforge.org/clinics, adapted for this book so that it follows the five steps. It works at a kitchen table, in a library, in a care home or in a staff room. Nothing in it is for

sale. You will need: one phone or tablet per person, or one between two; this book or the printed cards; and tea.

Minute 0 to 5: One true story

Begin with a story, not a statistic. Any of the stories between the parts of this book will do, or one from your own community. If you are comfortable, tell one of your own. The point of the story is to make the first thing in the room a person, not a threat.

If you want one sentence of context, use this: UtilForge began inside one family, when the founder’s mother and father, who were learning to use the internet, found payments they had never agreed to leaving their bank account. The checks exist because that family wished it had them.

Do not open with how much money is lost each year. People know it is a lot. Numbers at the start of a session make people feel small. Numbers at the end, if at all.

Minute 5 to 15: The five steps

Read the five steps aloud, one at a time, and after each one ask the room: “Has anyone had a message like that?” Someone always has. Let them tell it. The room learns more from their neighbour’s parcel text than from any slide.

1. Pretend: they pretend to be someone you trust.
2. Problem or prize: a fright, or a reward.
3. Pressure: a deadline.
4. Privacy: “don’t tell anyone”.
5. Pay: gift cards, cryptocurrency, a transfer to a new account.

Then the one sentence to take away: **spot any one of the five, stop, and check. A missing step never makes a message safe.**

Minute 15 to 35: Everyone runs one check

This is the heart of the session, and the part most sessions skip. Do not skip it.

Show the check once on your own device. Open utilforge.org/text. Show the box. Paste in a message, press the button, read the result aloud. Then, with the page still open, put your phone in aeroplane mode and do it again, so that everyone can see that it still works, because the check happens on the phone in their hand. (Do not reload the page while offline; see “Two things the book will ask you to do” at the front.) That demonstration does more for trust than any promise.

Then have every person do it on their own phone. Give them a message to paste if they do not have one of their own. The parcel message from Chapter 3 is a good first one, because almost everyone has had one like it. Use it with the link, because the link is one of the signs the check looks for:

> Your parcel could not be delivered. A redelivery fee of $1.99 is due. Pay within 12 hours: https://parcel-redeliver.example

Walk round. Help with the copying and pasting, which takes most of the time. Do not touch anyone’s phone unless they hand it to you and ask, and never keep a copy of anything on it. When their screen says *Stop. This looks like a scam*, let them read the reasons themselves. If someone pastes a message of their own and the screen says *Be careful* instead, that is the check finding one sign rather than several; the advice is the same.

If there is time, do a second check. Family Safe Word (utilforge.org/safeword) is a good choice, because it ends with something they can take home.

Minute 35 to 45: The card, and the person to ask

Hand out the five steps card from this book (it follows Part Five), or print it from utilforge.org/book. Then ask each person to write one name on it: the person they will ring,

or show the message to, before any money moves. A family member. A neighbour. The librarian. You.

That name is the most important thing anyone leaves with. The check finds the signs. The person breaks the silence. Both matter, and step four, privacy, is beaten by the second one.

End with the sentence from Chapter 5, because it is the one people repeat afterwards: *Someone who loves you will understand if you check first.*

Afterwards

If you ran the session for an organisation, UtilForge asks three things, and only if you want to. Permission to say that you hosted a session. One sentence about it in your own words. And a short conversation after thirty days about what confused people, so that the checks can be changed. Write to support@utilforge.org.

Keep a note of what confused people anyway, for yourself. The next session will be better for it.

---

15. The family safe word

Everything else in this book is about messages, because messages can be checked. This chapter is about the one thing that cannot be: a voice on the phone, live, asking for help.

A voice can now be copied from a short recording: a voicemail greeting, a video on social media, a clip from a family group chat. The copy can be made to say anything, in distress, in a hurry. In 2025 the Federal Bureau of Investigation warned twice about cloned voices in voice messages and texts pretending to come from senior officials, and its advice to families is the same as this chapter’s: create a secret word or phrase with your family.

How it works

A family safe word is one plain word, or two, that only your family knows. The rule for it is short. **Never type it, never write it where others can see it, and never say it to someone who has rung you.** You give it to each other once, in person, or on a call that you yourself started to a number you already had. After that it lives in your heads.

Then, if a call or a message asks for money, a code or urgent help, even if it sounds exactly like your mother, your father or any other family member, you ask for the word.

No word, or the wrong word? Stop. Hang up. Ring the person back on the number you already have. They may well be genuine and flustered, and the ring-back will show that in a minute. The word is one check. The ring-back on a number you already have is the one that settles it.

A safe word can be overheard, and a phone can be lost, so if you ever think the word has got out, agree a new one.

Choosing the word

- Avoid pet names, birthdays, street names, and anything that appears in a photograph or a post. Those are the first things a scammer who has looked you up will try.
- A random word is harder to guess than a meaningful one. The Family Safe Word page at utilforge.org/safeword makes one on your own device from a list of plain words. It saves nothing, and the word stays on that device.
- Two words are harder to guess than one.
- If anyone ever types the word into a message, choose a new one. The word only works while it has never been written down anywhere a stranger could read it.

Telling the family

Tell each person the word face to face, or on a call you started. Do not send it. Agree together what it is for: money, codes, and urgent requests for help. Agree that asking for it is never an insult, even when the voice sounds right. *Especially* when the voice sounds right.

Print the card, for the rules and the names, not for the word. The Family Safe Word page prints a card with the three rules and a line for who has the word, and it leaves the word out unless you ask for it. Put the card on the fridge, where people in a hurry will see the rules. A fridge is seen by visitors, carers and tradespeople, and appears in photographs and video calls, so the word itself must never be on it.

At work

The same idea protects a team. If a colleague, a supplier or a boss asks by message or phone to change bank details or to pay

something in a hurry, confirm by ringing them on a number you already hold. Never use a number from the message. Banks in many countries list a request to change payment details that arrives by email, messaging app or phone among their warning signs.

What a safe word is not

A safe word is one extra check, not a guarantee. A word can be overheard, a phone can be lost, and a scammer who has got into a family's messages may know more than you think. It works best with the habit of ringing back on a number you already have, and it only ever protects the people who have it. Which is a reason to set it up this weekend, not next.

---

16. Set up a phone together

The phone is where most of the scams in this book arrive: the text about a parcel, the call from a “bank”, the message from a “family member, on a new number”. In June 2026 the Federal Trade Commission reported that nearly one in three fraud reports it received in 2025 were about someone pretending to be a person or organisation the victim already trusted, reached by text, phone call, email, social media and search results.

The same phone already holds some of the best protections against them. Many of those protections are switched off, or sit in a menu nobody has opened. This chapter is one afternoon, two people, one phone, and the four things to switch on together.

Before you start

The phone belongs to the person who uses it. They hold it, they tap each setting, and they decide. The other person sits beside them,

reads the steps aloud and helps find the right menu. That way the owner knows what changed, why it changed, and how to change it back.

Agree a time, the way you would for any visit. An afternoon, a cup of tea, the phone charged, and the passwords for email and banking to hand, kept by the owner. Nobody else needs to see them.

The free phone safety checklist at utilforge.org/tools/phone-safety-checklist shows where each setting is on an iPhone and on an Android phone, step by step. Menus move when a phone updates, so the checklist is kept current and this chapter describes what each step does rather than which button to press.

Step one: screen calls and messages from strangers

Both iPhone and Android phones can now answer or silence calls from numbers that are not in the contacts, and sort texts from unknown senders into their own list. A real caller can leave a message. A scam call that relies on catching someone off guard gets a recording instead of a person.

Before switching it on, add the numbers that matter to the contacts together: the family, the doctor, the pharmacy, the school, the bank. Then the people who should get through do get through.

Step two: save the bank’s real number

Turn the bank card over. The number printed on the back is the bank’s real number. Save it in the contacts under the bank’s name, with the word “real” after it, so it stands out.

When a call or message says it is from the bank, this is the number to ring back on: not the number in the message, and not the number the caller gives. Chapter 11 explains why the number shown on an incoming call proves nothing. The saved number is the one that does.

Step three: a passkey or two-step sign-in for email and banking

Email matters most, because a password reset for almost every other account is sent there. Whoever controls the email can often take over the rest.

A **passkey** lets the phone itself prove who is signing in, with the face, fingerprint or screen lock the owner already uses. There is no password to steal, and a fake website cannot use it. **Two-step sign-in** adds a second check after the password, usually a code sent to the

phone or shown in an authenticator app. Either way, a stolen password on its own is no longer enough.

Set one up for the email account first, then for the bank’s app. While you are in the bank’s app, switch on payment alerts, so that every payment sends a message straight away and a payment nobody made is noticed the same day.

One rule goes with it: a code is for typing into the app or website you opened yourself. It is never read out to anyone who rings, whoever they say they are.

Step four: one family rule for money and codes

The last step is a conversation, not a setting. Agree one rule, together, out loud:

> **Nobody in this family sends money to a caller, or shares a code, until they have rung back on a number they already have.**

Then agree the family safe word, the way Chapter 15 describes: in person, never typed, never written where others can see it. The rule and the word work together. The word is a first check when a voice sounds like family. The ring-back on a saved number is the check that settles it.

Write the rule, not the word, on a card for the fridge, with the bank’s real number and the name of the first person to ring if something feels wrong.

Six months later

Phones update, banks change their apps, and new scams arrive. Put a date in the diary six months on, and go through the four steps again: are the settings still on, is the bank’s

number still right, does everyone still remember the word without writing it down? It is a shorter afternoon the second time.

If you would like to give it as a gift

An afternoon like this can be a present in its own right, for a birthday, a new phone, a teenager’s first phone or a festival. UtilForge’s printable A Safer Phone gifts, at utilforge.org/for/safer-phone, hold a card to give, family safe word cards, the set-up checklist and a fridge guide. The checklist and the safe word card are also free on their own, at the addresses in this chapter.

What it is not

No setting stops every scam. A screened call can still be a scam that leaves a message, and a passkey protects an account, not a person who is persuaded to send money. What the afternoon adds is the pause:

everyone in the family knows to stop, check and ring back before money moves, and nobody is told off for checking.

---

17. What to say, and what never to say

This chapter is short, and it may be the most useful one in the book for an educator, because the words we use when someone has nearly been scammed, or has been, decide whether they ever tell us again.

Never say

- “How could you fall for that?”
- “I would never have.”
- “Didn’t you think it was obvious?”
- “You should have known.”
- “I told you about this.”

Every one of these does the scammer’s work for them. Shame is step four. It makes people hide the next message instead of showing it. A

2022 survey for AARP, the American organisation for people aged 50 and over, and the FINRA Investor Education Foundation found that about half of adults surveyed saw fraud victims as partly to blame, and nearly half believed reporting was a lost cause. Silence is the scammer's best friend, and these sentences build it.

Say instead

- "This is not your fault. These are designed by professionals to do exactly what they did."
- "I'm really glad you showed me."
- "You stopped before the money went. That's the whole thing."
- "Can we ring the bank together?"
- "Send me the message. Let's look at it."
- "You did the right thing by telling someone. That's the step that beats them."

When they are halfway in

Sometimes the person has not lost anything yet but is still inside the story. The family member is still “in trouble”. The recruiter is still “waiting”. The mentor is still “a friend”. Arguing rarely works, because the scammer has already told them that people will argue.

What works is a question they can answer by checking, not by believing you. “Can we ring her on her old number, just to be sure?” “Can we look up the hotel’s own website together?” “Can you take the money out today, without a fee? Let’s just try.” The check does the arguing. You stay on their side.

When money has already gone

Skip going over what went wrong. Go to Chapter 18 together and make the phone call to the bank first. Everything else, including the conversation about how it happened, can wait

until after the call. Speed is the one thing that improves the odds of getting money back, and shame is the one thing that slows it.

For yourself

If you are the educator, you will sometimes be too late, and you will sometimes be ignored, and you will sometimes be the person who gets the call at 11.40 at night. None of that is a failure. The people in this book who were saved were saved by someone who was simply there, who did not shout, and who knew where the check was. That is the job. It is enough.

PART FOUR: IF IT HAS ALREADY HAPPENED

18. The first phone call

If money, a code or your details have just gone to a scammer, this page is the only one that matters right now. Read it, make the call, and come back to the rest afterwards.

First: this is not your fault. Well-made scams catch careful people. They are designed by professionals, tested on thousands, and improved every week. The fact that one reached you says nothing about you except that you have a phone.

Second: ring quickly. Banks and payment companies can sometimes stop or reverse a payment if they hear quickly, and the chance falls with every hour. So the order is: call first, feel later.

But if a scammer has control of your computer or phone, because you let them "fix" something or installed a program they sent, do one thing before the call: disconnect that device from the internet, or turn it off, and make the call from a different phone. Someone who controls the device may be able to see your banking. Tell the bank that too.

The call. Ring your bank, or the company you paid through, now. Use the number printed on the back of your card, or the number inside the bank's own app, or the number on the bank's own website that you type in yourself. Never use a number from the message or from the caller.

Say: "I have been tricked into making a payment. I want it stopped or reversed, and I want my account protected."

Then do what they tell you. They have done this before. You do not need to have the story straight. You do not need to have worked out

how it happened. You only need to have rung.

If you shared a code or a password, change the password now, on the real website or app, and anywhere else you used the same one. Then turn on two-step login, an extra check when you sign in, such as a code or an approval on your phone. You will find it in the account's settings, usually under "Security" or "Sign-in". If the service offers an authenticator app instead of a text message code, choose the app.

In the United Kingdom, you can also dial 159 from most phones. It connects you to your own bank's fraud team, it is run by Stop Scams UK, in which banks, phone companies and technology firms work together, and the number cannot be faked.

If the device the scammer controlled is still on, keep it off the internet until someone you trust has helped you check it: someone you chose, never someone who contacted you.

Then read on.

---

19. By how you paid

These steps follow the Federal Trade Commission’s guidance on what to do if you have been scammed. The agency is American. The first phone call is much the same everywhere, but your rights, any refund scheme and the time limits depend on your country, so ask your own bank or payment company what applies to you.

Credit or debit card. Ring the number on the back of the card, report the charge as fraud, and ask what protection applies: a dispute, a refund, or a “chargeback”, which is the card company taking the money back from the seller.

Bank transfer. Ring your bank and ask them to try to reverse the payment or recall the funds, which means asking the receiving bank

to send it back. In the United Kingdom, banks must reimburse many “authorised push payment” scams, where you were tricked into making the payment yourself; there are rules and time limits, so ask whether your payment qualifies.

Money transfer company, such as Western Union or MoneyGram. Contact the company, say you were tricked into sending money, and ask for a refund. If the money has not yet been collected, it can sometimes be stopped.

Payment app, such as PayPal, Venmo or Cash App. Report the payment through the app’s own support or fraud process and ask what can be done. Then tell the bank or card that is linked to the app.

Gift card. Ring the company that issued the card, using the number on the card itself. Explain that a scammer has the card number and the PIN, the secret number under the

scratch panel. Ask whether any unspent value can be frozen or refunded. Keep the card and the receipt.

Cryptocurrency, including cash paid into a cryptocurrency cash machine. Contact the exchange or the machine’s operator straight away, using the contact details on your receipt or on the operator’s own website, and report the transaction as fraud. Keep every transaction detail. Be prepared: recovery is rare, because cryptocurrency has few of the protections that cards have. Report it anyway (Chapter 20), because reports are how cases are built and the next person is warned.

You typed your card details into a page. Treat the card as compromised. Ring the bank, ask them to cancel it and send a new one, and check your statement for anything you do not recognise.

You gave an identity number, such as a Social Security number or a national identity number. In the United States, follow the steps

at IdentityTheft.gov. Elsewhere, contact your country's fraud prevention service. In South Africa, the Southern African Fraud Prevention Service offers free "protective registration", which flags your identity so that banks and lenders check more carefully before opening anything in your name; it helps, but it does not stop every misuse. Similar services in other countries may charge a fee.

You sent a copy of your passport or identity document. Tell the issuing authority, and tell your bank, so that both can watch for anyone using it to open accounts in your name.

---

20. Where to report it, country by country

Report it. Reports rarely bring money back on their own, but they are how agencies warn others, take down websites and build cases. Every service below is official or recognised in

its country, and each entry says what kind of service it is: a police report, a reporting portal, an advice line, or a complaints service. Services change, so follow the current instructions on the official page itself. UtilForge does not take reports itself, and nobody at UtilForge will ever contact you about a loss.

The full list is at **utilforge.org/official-help**; the page shows the date each entry was last checked. Where a support line is given below, it is for when you feel overwhelmed or unsafe. These lines are confidential and most are free. They cannot get money back. The countries most often asked about:

United States. Report fraud to the Federal Trade Commission at ReportFraud.ftc.gov. Report online crime to the Federal Bureau of Investigation’s Internet Crime Complaint Center at www.ic3.gov (if one of these sites is unavailable, use the other). Forward scam

texts free to 7726, which spells SPAM on a phone keypad. For identity theft, IdentityTheft.gov. Support line: 988.

United Kingdom. In England, Wales and Northern Ireland, report to the police through Report Fraud, at reportfraud.police.uk or 0300 123 2040; it replaced Action Fraud on 4 December 2025. In Scotland, Police Scotland on 101. To reach your own bank’s fraud team, dial 159. Forward scam texts free to 7726 and suspicious emails to report@phishing.gov.uk. Support line: Samaritans, 116 123.

Ireland. An Garda Síochána, the police, at your local Garda station; garda.ie explains what to bring. Support line: Samaritans, 116 123.

Canada. The Canadian Anti-Fraud Centre, a reporting centre, online at reportcyberandfraud.canada.ca or by phone on 1-888-495-8501, and your local police as well. Support line: 988.

Australia. Scamwatch, a reporting portal, at scamwatch.gov.au; police reports through ReportCyber at www.cyber.gov.au. For help after your identity details are taken, IDCARE on 1800 595 160. Support line: Lifeline, 13 11 14.

New Zealand. The National Cyber Security Centre's reporting page at ncsc.govt.nz/report, and the police for a formal complaint. Support line: 1737.

South Africa. Your bank first. The police: open a case at your nearest South African Police Service station and ask for the case number, which your bank or insurer will want. Crime Stop, 08600 10111, is an anonymous tip-off line, not the place to open a case. If the bank's answer is not satisfactory, the National Financial Ombud Scheme, a free and independent complaints service (an ombud settles complaints between you and a company), at nfosa.co.za, once you have complained to the bank first. The Southern

African Fraud Prevention Service, a not-for-profit organisation, at www.safps.org.za, for protective registration. Yima, at www.yima.org.za/reportscam, collects reports of scam websites and messages for awareness and statistics; it is not a police report, so report to the police as well. Support line: the South African Depression and Anxiety Group, 0800 567 567.

Kenya. The National Computer and Cybercrimes Coordination Committee, at nc4.go.ke.

Nigeria. The Nigeria Police Force National Cybercrime Centre, at nccc.npf.gov.ng.

Ghana. The Cyber Security Authority's reporting page at csa.gov.gh/report, or call or text 292.

India. The National Cyber Crime Reporting Portal, at cybercrime.gov.in, or the helpline 1930.

Singapore. ScamShield, the government's anti-scam service, at scamshield.gov.sg, with a helpline on 1799, open day and night. ScamShield cannot make a police report; make one at police.gov.sg.

Hong Kong. The police's Anti-Deception Coordination Centre, at adcc.gov.hk, or its Anti-Scam Helpline, 18222.

European Union. Europol lists each country's own reporting route at europol.europa.eu/report-a-crime; the procedures differ from country to country. France: 17Cyber, the online police help service, at 17cyber.gouv.fr. Germany: the Onlinewache, the online police station of your state police. The Netherlands: the police at politie.nl. Spain: the Instituto Nacional de Ciberseguridad advice line on 017; for a formal complaint, the Policía Nacional on 091.

Middle East. Checked against each body's own pages where they could be read and against national news where they could not;

the dates are on utilforge.org/official-help. Saudi Arabia: forward a scam text free to 330330 (the Communications, Space and Technology Commission); for a loss, the Public Security “Kollona Amn” app or the Absher platform; emergency 911; support line 920 033 360. United Arab Emirates: the government portal at u.ae lists the Ministry of Interior eCrime service, Dubai Police eCrime and Abu Dhabi Police Aman on 800 2626; emergency 999; support line 800 4673. Qatar: the Ministry of Interior’s Economic and Cyber Crimes Combating Department on 2347 444 or 6681 5757, or through the Metrash app; emergency 999; support line 16000, option 4. Kuwait: the Ministry of Interior’s Cyber Crime Combating Department on 9728 3939; emergency 112. Bahrain: the Ministry of Interior’s anti-corruption and electronic security hotline, 992, which also takes fraud reports; emergency 999. Oman: the Royal Oman Police on 8007 7444, or the nearest police station; emergency 9999. Jordan: 911,

or the Criminal Investigation Department at the nearest police station, which is the route the Public Security Directorate gives. Egypt: the Ministry of Interior's online crime hotline, 108; general police 122; support line 16328. Israel: an online fraud complaint to the Israel Police at gov.il, emergency 100, the National Cyber Directorate on 119 for a hacked account or a phishing attack, and ERAN on 1201 for support. Iraq: the nearest police station, or 911.

Bangladesh. Bangladesh Police, at your local station or the Criminal Investigation Department's Cyber Police Centre. Women can call Police Cyber Support for Women on 01320 000 888, a service for women only. Emergency 999.

Maldives. The Maldives Police Service Anti-Scam Centre, hotline 125. Support line: 1677.

Brazil. The Polícia Federal for federal crimes; for most fraud, your state's civil police, which has an online police station in most states.

If your country is not listed here, it is likely to be on the page at utilforge.org/official-help, and your bank’s fraud team will know the right place.

---

21. The second scam

This chapter is here because it is the part people are least prepared for.

After you have lost money to a scam, you may be contacted again. By a law firm. By a recovery agency. By a government unit you have not heard of. By an “investigator” who knows the details of what happened to you, very often because the first scammer passed them on. They can get your money back. There is a small fee first.

This is a scam aimed at people who have already been scammed. The Federal Trade Commission documents it. The Federal Bureau of Investigation warned about it in

2025 and again in 2026. The second warning was about a deepfake video, a fake video made by a computer, of one of the Bureau's own officials, promoting a fake version of its complaint website. It works because it arrives when you most want it to be true.

The rule. Never pay anyone, up front, to recover money. Not a retainer, not a processing fee, not a tax, not a release charge. Real recovery, where it is possible, comes through your own bank and through official reporting, and neither charges a fee to begin.

The signs are the five steps again. They contacted you (pretend). They offer your money back (prize). The case is closing (pressure). Sometimes: do not involve your bank, it will slow things down (privacy). Pay by gift card, cryptocurrency, wire or payment app (pay). Any one of them is enough to stop.

If you are contacted, do not reply. Keep the message. Report it in the same place you reported the first scam. And, if you can, tell someone, because the person you tell is the person who will stop the next one.

Afterwards

Being scammed changes how people feel about their phone, their judgement and sometimes themselves. The Office for National Statistics found that in England and Wales, in the year to March 2025, 13 per cent of fraud incidents left people with feelings of shame, embarrassment or self-blame. If you feel this way, you are not alone, and the thing was done to you by a professional.

If you are reading this because it happened to you: you are not foolish, and you are not alone. Reading this is already the thing that protects the next person. If it is weighing on you, the support lines in Chapter 20 are there

to be rung. If you are reading it because it happened to someone you love: Chapter 17 has the words. Use the kind ones.

PART FIVE: FOUR MORE HABITS (NOT SCAMS)

The four chapters in this part are not about scams, and they are not among the five steps. They are here because they are about the same thing: knowing what leaves your hands, and checking before it does. They sit at the end so that nobody mistakes them for Part Two.

---

22. The black box that was not really black

What it looks like. This one is not a message. It is a document you send. A bank statement for a landlord, with the account number blacked out. A medical letter for an employer, with a diagnosis covered. A contract for a client, with a price hidden.

The black box hides the words from sight. It very often leaves them in the file. Anyone who receives the document can select the “hidden” text and copy it out, or open the file in a different program and read it.

Why it is here. This is not a scam. It is the opposite problem: not someone taking something from you, but you giving something away without knowing. It belongs in this book because the people who most need to send blacked-out documents, for housing, for benefits, for work, are the same people everything else in this book is for. Blacking out properly is called redaction.

The check. Two free tools at UtilForge.org:

- **Is It Really Blacked Out?** (utilforge.org/tools/is-it-really-blacked-out) reads a document someone has already blacked out and tells you whether the words underneath can still be read.

- **Redaction Studio** (utilforge.org/redact) blacks out a PDF (Portable Document Format) file properly. It rebuilds each page as a picture, so there is no text left underneath, then opens its own result and checks it. When all is well, the report's heading reads "Redacted file made. Every check passed." and one of its lines reads "No text in the new file that could be copied out".

Both run on your own computer. The file stays there.

What to do. Before you send any document with something hidden in it, run it through the check.

---

23. What you paste into an artificial intelligence

What it looks like. You ask an artificial intelligence assistant to help you write a message, and you paste in the message you are replying to. It has your mother’s name in it. Her address. Her phone number. The name of her carer.

This is not a scam, and this book claims no link between artificial intelligence assistants and the scams in the other chapters. An artificial intelligence assistant is a computer service that answers questions and helps write things. This chapter is here because pasting other people’s names, addresses or health details into one is the same privacy problem whether or not a scam is anywhere near it.

Once you press send, the text goes to the company that runs the assistant. Its rules, your account type and your settings decide how long it is kept and who can see it, so read that

service’s own privacy page. For your own details, that is your choice. For other people’s, it is not entirely yours to make.

The check. *Hide Names from Artificial Intelligence*, at utilforge.org/tools/hide-names-from-ai. You paste the message in, press one button, and the names, addresses, phone numbers and email addresses it finds become labels: [NAME 1], [ADDRESS 1]. You copy that into any assistant, ask your question, paste the answer back, and the real details return. It finds names by their clues and can miss one, so read the result before you copy it. It all happens on your own phone, and what you paste stays there.

What not to paste, ever: passwords and codes, card and bank numbers, identity numbers, health details, and other people’s details. UtilForge has a one-page guide called *What Not to Paste*, at utilforge.org/tools/before-you-paste-into-ai.

What to do if you already have. Change any password that went in. Delete the chat, knowing that a copy may be kept for a while under the service's rules. Look in the service's settings for the switch that lets your chats be used to train the assistant, and turn it off. The guide at utilforge.org/learn/what-happens-to-what-you-paste-into-an-ai shows where that switch is for several of the main services.

---

24. The words you cannot see

What it looks like. You copy a web page, an email or a long report and ask an artificial intelligence assistant to sum it up. On your screen the text looks ordinary. Underneath, it can carry words you never see: white letters on a white background, letters so small they vanish, or characters from the part of the world's shared alphabet, called Unicode, that are made to display nothing at all. Some of those hidden words are short notes written to

the assistant, such as “ignore your previous instructions”. The assistant reads every character, including the ones you cannot see, and it may follow them. The name for this is prompt injection.

Why it is here. This is not one of the five steps, and the person who pastes the text is not the target of a scam. It is here because it is the same habit as the rest of this book, which is to check before something leaves your hands, and because the people who use free assistants to read long letters, contracts and articles are the same people this book is for.

The risk is real and recognised. The Open Worldwide Application Security Project, a non-profit community that publishes open lists of software security risks, puts prompt injection first in its 2025 list of the top ten risks for applications built on large language models, the systems behind today’s assistants. On 8 December 2025 the United Kingdom’s

National Cyber Security Centre described these systems as “inherently confusable”, because they struggle to keep the instructions they are given apart from the text they are asked to read. In June 2025 researchers at Aim Security disclosed a flaw in Microsoft 365 Copilot through which a single email with hidden instructions could make the assistant leak a person’s data, and Microsoft fixed it before the details were published. On 3 September 2026 Microsoft Security Research described an email campaign that hid invisible characters inside ordinary words, so that email filters would miss them.

Each company builds defences into its own assistant. A check on your side works before any assistant reads the text.

The check. Two free tools at UtilForge.org:

- **Prompt injection checker** (utilforge.org/tools/prompt-injection-check) reads pasted text for wording often used to give instructions to an assistant, including

“ignore your previous instructions” in six languages besides English. It finds white, tiny or hidden text in a pasted web page, decodes hidden messages, and offers a cleaned copy.

- **Invisible character remover** (utilforge.org/tools/invisible-character-remover) finds invisible spaces, hidden messages and look-alike letters, takes tracking codes out of links, and keeps the joining characters that emoji and Arabic, Persian and Hindi spelling need.

Both run on your own phone or computer, and what you paste stays there. Add them to your home screen so they are one tap away.

The checker lists its own limits. It looks for known phrases and known hiding tricks, so an instruction written in completely new words can still pass, and a clear result means only that no known warning signs were found.

What to do. Before you paste a page, an email or a document from someone you do not know into an assistant, run it through the check. If the assistant's answer asks you to click a link, send money or share a password that the original text never mentioned, stop, and read the original yourself.

---

25. The VPN: what it protects, and when to switch it off

What it looks like. An advert says your phone is exposed and offers a free VPN, unlimited, for ever. Or a friend tells you never to go online without one. A VPN, short for virtual private network, is an app that wraps your internet traffic in a code, called encryption, and sends it through a computer run by the VPN company before it reaches the website.

Why it is here. This is not one of the five steps. It is here because many people install a VPN believing it will stop scams, and because

a free one can take more than it gives.

What a VPN does. On Wi-Fi you do not control, at a café, a hotel, an airport or a station, it stops the network's owner and other people on it from reading your traffic or seeing which websites you visit. The Australian Cyber Security Centre advises people who use public Wi-Fi often to use a reputable VPN as an extra layer. Most websites already encrypt what you send, which is what the padlock beside the web address means, so the Federal Trade Commission in the United States now says public Wi-Fi is usually safe to use. A padlock means the connection is private. It does not mean the website is honest.

What a VPN does not do. It does not stop a scam text, a fake shop, a job-fee request or a call in a copied voice, because none of those travel through the part a VPN protects. It does not make you anonymous: the VPN company sees your traffic instead of your internet

provider, and every website you sign in to still knows it is you. And it does not change what an artificial intelligence assistant receives.

The trouble with free VPNs. Running a VPN costs money, so a free one is paid for some other way. In 2026 university researchers tested 281 free VPN apps found on Google Play: 246 of them contacted advertising and tracking companies, and 29 let traffic leak outside the encrypted connection. In March 2026 the Federal Bureau of Investigation warned that some free VPN services sign people’s phones up to a “residential proxy” network, which lets strangers send their own traffic through your connection, often under terms hidden in long agreements.

When to switch it off. Banks, payment services and identity checks treat a VPN as a warning sign, because criminals use VPNs to hide where they are. A sign-up, a payment or an identity check can be refused, delayed or marked as suspicious while your VPN is on,

even when you have done nothing wrong. For those steps, switch it off and use your home Wi-Fi or mobile data and your ordinary email address. Switch it back on afterwards if you are on Wi-Fi you do not control.

Seven questions before you install one.

1. Who runs it, and in which country is the company registered?
2. How does it pay for itself?
3. What does its privacy policy say it keeps, and for how long?
4. Has an independent firm checked it, with a published report?
5. Does it come from the official app store, with a developer name that matches the company?
6. Does it ask for anything a VPN does not need, such as your text messages, your call log, accessibility access (which lets an app read and tap your screen), device administrator rights (which can stop an

app being removed), or your antivirus switched off?

7. Is it sold with a pop-up that says your phone is infected, a promise of “100 per cent anonymous”, or a request to pay by gift card?

The check. *Do I need a VPN? Is this VPN safe?*, at utilforge.org/tools/vpn-check. It asks a few plain questions, tells you whether a VPN would help with what worries you, and reads a VPN app’s description, permissions list or advert for warning signs. It runs on your own phone or computer, and what you paste stays there. A clear result means only that no known warning signs were found in the words you pasted.

THE FIVE STEPS CARD

Cut along the line, fold in half, and keep it on the fridge or in a wallet. Print as many as you like. A copy to print is at utilforge.org/book.

SCAMS USE FIVE STEPS. SPOT ANY ONE: STOP, AND CHECK FIRST.

1. Pretend. They pretend to be your bank, the police, a company, or your own family. → Reach them yourself, on a number you already have.

2. Problem or prize. A fright, or a reward. → Notice the feeling. That is the moment to pause.

3. Pressure. A deadline. → A real deadline is still there after you check.

4. Privacy. “Don’t tell anyone.” → Tell someone. Someone who loves you will understand.

5. Pay. Gift cards, cryptocurrency, a “safe account”. → No real bank, police force or court asks for these.

A missing step never makes a message safe.

Check any message free: utilforge.org/text
Make a family safe word: utilforge.org/safeword (and never write the word on this card)

The person I will ask before any money moves:

If money has already gone: ring your bank now, on the number on the back of your card. Then utilforge.org/official-help.

If you doubt it, check it.

THE SAFE WORD

A story

It was Priya’s idea. She was thirty-four and a pharmacist, and she chose her grandmother’s eightieth birthday to raise it, because the whole family would be in one room and because her grandmother could not easily say no to anything on her birthday.

“Before the cake,” Priya said, “I want us to agree a word.”

Her uncle, who was already holding the cake knife, asked what kind of word.

“A family word. One that only we know. So that if anyone ever rings one of us sounding like one of us, and asks for money, we can ask for it.”

“Sounding like one of us,” her grandmother repeated.

“Nani, they can copy a voice now. From a video. From a voicemail. A short clip can be enough.” Priya had read this in the library’s leaflet. Then, because she was Priya, she had checked it against the Federal Bureau of Investigation’s own warning, which said the same thing and told families to create a secret word. “It’s not that it’s likely. It’s that it’s cheap to stop.”

Her uncle wanted to use the dog’s name. Priya explained, gently, that the dog had its own account on a photo-sharing site, with four hundred followers, and that a stranger who had looked the family up would try the dog first.

Her grandmother wanted to use her late husband’s village. Priya explained, more gently, that the village was in the caption of the photograph on the wall behind them.

In the end they used the page. Priya opened it on her phone, put it in aeroplane mode so that everyone could see the page working on the

phone in her hand, and pressed the button that made two plain words from a list. The words were ordinary. That was the point. Nobody would ever guess them from a photograph, because they had nothing to do with anyone.

Everyone said the words out loud, once, round the table, so that each person had heard them from a face they could see. Then Priya printed the card from the same page, cut the words off the bottom with the cake knife, and gave her grandmother the rest: the three rules, and a line for each name. Her grandmother, with ceremony, put it on the fridge under the magnet shaped like a mango.

“Why cut them off?”

“Because the fridge is in every photo we take in this kitchen, Nani. The rules can be on the fridge. The words stay in our heads.”

“And if someone rings and doesn’t know the words?”

“Then you stop, and you hang up, and you ring the real person back on the number you’ve always had. Even if it sounded exactly like them. Especially if it did. And you never say the words to anyone who rang you.”

“And if it was really you, and you’d forgotten the words?”

“Then you ring me back, and I’ll answer on my own phone, and you can tell me off. Which you’ll enjoy.”

Her grandmother considered this and found it acceptable.

The call never came. That is the ending of most of these stories, and it is the right ending. The card is still on the fridge, and the words are not on it. The dog still has four hundred followers. And at the eighty-first birthday, before the cake, with the kitchen door shut, her grandmother looked round the table and said the two words herself, unprompted, to make sure everyone still had them.

They did.

MR OKAFOR'S STATEMENT

A story

Mr Okafor needed a flat, and the flat needed a bank statement.

The letting agent was perfectly reasonable about it. Three months of statements, to show the rent would be covered. He could black out anything he liked, she said. They only needed to see the income line.

So he did what seemed obvious. He opened the statement and drew a thick black rectangle over his account number. He drew another over his sort code, the number that identifies the bank branch. He drew a third over the name of the clinic that took a payment on the fourth of every month. He saved it. On the screen, it was gone. Black. Nothing to see.

His sister Ruth, who was visiting, watched him attach it to the email.

“Joseph. Can I see that before you send it?”

She opened the file on her own laptop, clicked on the black rectangle, dragged across it, and pasted what she had selected into a blank document.

His account number appeared. Then his sort code. Then the name of the clinic.

Mr Okafor looked at it for a long moment.

“It was black.”

“It was black on top. The words are still underneath. Anybody who gets this file can do what I just did. The agent, anyone she forwards it to, anyone who ever gets into her email.”

He had been a civil servant for thirty-one years. He had, he realised, probably sent documents like this before, to people he could no longer remember, with black rectangles over things he had believed were gone.

“Show me the right way.”

She opened a page called Redaction Studio and dropped the statement in. She typed his account number into a box and pressed Find, and every place it appeared was marked, including one in small print at the bottom of page three that he had missed. She drew a box over the clinic’s name. Then she pressed a button that said *Black out and check*.

“What’s it doing?”

“Rebuilding each page as a picture. So there’s no text underneath at all, because there’s no text. Then it opens the new file itself and tries to copy anything out of it.”

The report came up in green. *Redacted file made. Every check passed.* Below it, a list: the new file opened properly, the page count matched, no text in the new file that could be copied out, no earlier version hidden inside, no

notes or comments. She tried the drag-and-paste trick again on the new file. Nothing came.

“And it didn’t send my statement anywhere?”

“Pull the internet cable out and do it again if you like. It all happens on this laptop.”

He did, because he had been a civil servant for thirty-one years. It worked with the cable out.

He got the flat. He also went back, that week, through his sent emails, as far as he could stand to, and found two more statements with black rectangles on them. He could not unsend them. He rang his bank and told them, and they changed the account number, and were kind about it, and said it happened more than he would think.

He keeps the page bookmarked now, next to his bank. The order is deliberate.

THE LIBRARY AT FOUR O’CLOCK

A story

Grace had run the Thursday session at the branch library for six years. Scam awareness, it was called on the poster, though she had stopped using the word *awareness* out loud because it made people’s eyes go flat.

For most of those six years the session had been a talk. She stood at the front with slides. The slides had numbers on them, billions of dollars, millions of people, and the faces in the room looked the way faces look when they are being told about a flood on another continent. Afterwards people said thank you and went home, and the next month the same people came back and told her about the text they had nearly tapped.

What changed was a leaflet a library in another county had sent round, with a forty-five minute plan on it and one line that annoyed her at first: *Everyone runs one check. Do not skip this.*

She had always skipped it. There were twenty people and one of her and the phones were all different.

She tried it anyway, on a Thursday in October, with eleven people and a plate of biscuits.

She told a story first, instead of showing a number. It was her own, which she had never told the group. Years ago, her mother had rung her from a shop, halfway through buying four hundred pounds of gift cards for a man who said he was from the tax office. Her mother had stopped because the shop assistant had asked, quite casually, what they were for. Grace had been a little in love with that shop assistant ever since.

Then she read the five steps and asked, after each one, whether anyone had had a message like that. Everyone had. A man who had not spoken in six years of Thursdays produced his phone and read out a parcel text, word for word, with the deadline and the link, and the room nodded like a congregation.

Then came the part she had always skipped.

She opened the check on the library's tablet and held it up. She pasted in the man's parcel text. She pressed the button. *Stop. This looks like a scam.* She read the reasons aloud. Then she put the tablet in aeroplane mode, in front of them, and did it again, and it still worked, and something changed in the room that she could not have put on a slide. Eleven people had just watched the check run on a tablet with no connection at all.

"Now you," she said.

It took twenty-five minutes, not twenty. Copying and pasting took most of it. She walked round and did not touch anyone's phone. A woman who had come every month for two years and never once asked a question got her own screen to say *Stop*. She looked up with an expression Grace would have described, if pushed, as triumph.

At the end she handed out the cards, and asked everyone to write one name on the back. The person they would show a message to, before any money moved.

The man who had not spoken in six years wrote *Grace*.

The woman who had never asked a question wrote her brother's name, and then, after a moment, asked for a second card. He was looking for work, she said, and he had been sent a job with a fee attached the week before, and she had not known what to tell him. Now she did. She sent him the page from the library car park, and the next Thursday she

reported, to the room, that he had pasted the recruiter’s message in, got five reasons, and not paid. The room nodded like a congregation.

She has run it that way ever since. The slides are in a drawer. The numbers are on the last card, in small print, for anyone who wants them. The biscuits are the same.

What changed in the room, she says, when people ask, is who was holding the phone.

THE KITCHEN TABLE

A story

This last one is short, because it is the ordinary ending, and ordinary endings are short.

A woman in her seventies sits at her kitchen table with a cup of tea going cold and a phone face-down beside it. A message has just arrived. It does not matter what it said. It said one of the things they say.

She picks up the phone. She reads the message. She feels the thing it was built to make her feel.

Then she does the thing she has done thirty or forty times since the afternoon her sister sat where the teacup is now and showed her. She presses on the message until it copies. She opens the page. She pastes it in. She presses the black button.

Sometimes the page says *Stop*, and tells her why, and she reads the reasons and puts the phone back down and finishes her tea, and the message goes nowhere.

Sometimes the page says it found no common signs, and reminds her that this does not prove anything, and she does what it says to do then: she opens the real app herself, or rings the real number, and finds out.

Either way, the message never gets what it came for, which was her acting before she had checked.

Nobody sees this. There is no counter on the page, by design. Nobody at the company that makes it will ever know that on a Tuesday in a kitchen a message failed. Her sister will not know. The scammer, somewhere, will not know, except as a number that did not reply.

That is the whole of it. Not a victory. A habit, repeated, in a kitchen, by one person, online or offline, it makes no difference.

Multiply it by every kitchen table with a card on the fridge, and that is what a safer online world is made of. Not fear. Not vigilance. A pause, a check, a cup of tea finished.

If you doubt it, check it.

GLOSSARY OF TERMS USED IN THIS BOOK

This glossary explains the terms this book uses, and nothing more. They are listed in alphabetical order. Where a term has its own chapter, the chapter is given.

Advance fee. A payment asked for before you can receive something, such as a prize, a loan, a job or your own money back. The thing never arrives. Chapters 3, 9 and 12.

Aeroplane mode. A phone setting that turns off mobile signal and, on most phones, wifi. Once a UtilForge check has loaded, it keeps working in aeroplane mode, which shows that what you paste stays on your phone.

App. A program on a phone or computer, such as a banking app or a messaging app.

Artificial intelligence (AI). Computer programs that write text, answer questions or make pictures and voices. Scammers use it to

write convincing messages and to make fake voices and videos. Separately, Part Five is about using it carefully yourself: Chapter 23 on keeping private details out of what you paste into it, and Chapter 24 on hidden words in what you ask it to read.

Authenticator app. An app that gives you a short security code, or asks you to approve a sign-in, so that a password alone is not enough to get into your account. Never read the code out to anyone.

Authorised push payment fraud. When you are tricked into sending a payment yourself, for example by a caller pretending to be your bank. In the United Kingdom, banks must refund most of these, up to £85,000, for payments made since 7 October 2024 and reported within 13 months, under rules from the Payment Systems Regulator. Elsewhere, ask your bank what it will cover. Chapter 19.

Caller display. The name or number your phone shows for an incoming call. It can be faked, so it does not prove who is calling. Chapter 11.

Chargeback. A request to your card company to reverse a card payment. Ask your bank or card company as soon as you can. Chapter 19.

Cloned voice. A computer-made copy of a real person’s voice, made from a short recording. It can be used to pretend to be a family member who needs money. Chapters 11 and 15.

Code (security code, one-time passcode). A short number sent to your phone or shown in an app to confirm it is you. Never share a code with someone who contacts you unexpectedly.

Cryptocurrency. Digital money, such as Bitcoin, sent between online wallets. Payments usually cannot be reversed. A

demand to move your money into cryptocurrency to protect it is a scam. Chapters 10, 11 and 12.

Crypto wallet. Where cryptocurrency is kept. It is opened with recovery words: the 12 or 24 words shown when the wallet is set up. Anyone who has those words has the money, so never share them.

Deepfake. A video, picture or voice made by a computer to look or sound like a real person saying or doing something they never did.

Family safe word. A word agreed in person by a family, never written down or posted, and asked for whenever a call or message asks for money or urgent help. Chapter 15.

Fraud team. The department of a bank that deals with scams. Reach it on the number on the back of your card or in your bank’s own app, never on a number given to you by a caller. Chapter 18.

Gift card. A prepaid card for a shop. A demand to pay a fine, bill or fee with gift cards and to read out the numbers is a strong sign of a scam. Chapter 6.

Identity theft. When someone uses your personal details, such as your name, date of birth or passport, to borrow money or open accounts as you.

159. In the United Kingdom, a telephone number that connects you safely to your own bank if you think a call or message about your money is a scam. Chapter 18.

Investment scam. A fake investment, often shown on an app or website where your balance appears to grow, that will not let you take your money out. Chapter 10.

Invisible characters. Characters that take up no space on the screen, such as zero-width spaces. They can hide messages inside ordinary-looking text, or break up a word so that a filter misses it. Chapter 24.

Job scam. A fake job offer that asks you to pay a fee, send personal documents or pass money through your account. A real employer does not charge you to get a job. Chapter 9.

Link. Words or a button in a message that open a website when tapped. In an unexpected message, do not tap it: go to the website yourself instead.

PDF (Portable Document Format). A common type of document file, often used for bank statements and forms. Chapter 22.

Phishing. A message, by email, text or social media, that pretends to come from a trusted company in order to take your money, your details or your passwords.

Prompt injection. Hidden words in a web page, email or document that try to give instructions to an artificial intelligence assistant reading it, such as “ignore your previous instructions”. Chapter 24.

Recovery scam. An offer to get back money you have already lost to a scam, for a fee. It is a second scam. Chapters 12 and 21.

Redaction. Removing private details from a document before you share it. A black box drawn on top does not remove the words underneath. Chapter 22.

Safe account. A bank account a caller says will protect your money. No real bank or police force will ever ask you to move money to a safe account. Chapter 6.

Scam. A deliberate deception to take someone's money, details or trust. Anyone can be targeted, and being caught out says nothing about a person's intelligence.

Screenshot. A picture of what is on your screen. Keep screenshots of scam messages; they help when you report.

Two-step login (two-factor authentication). A second check when you sign in, such as a code or an approval on your phone, so that a

stolen password is not enough.

VPN (virtual private network). An app that encrypts your internet traffic and sends it through a computer run by the VPN company. It helps on Wi-Fi you do not control; it does not stop scams. Chapter 25.

Web address. The address of a page, such as utilforge.org/text. Type it in yourself rather than tapping a link you were sent.

Wifi. A wireless internet connection at home or in a public place.

Wrong-number text. A friendly message that seems to have reached you by mistake, often the start of an investment scam. You do not need to reply. Chapter 10.

SOURCES

Every figure in this book comes from one of the sources below. Dates are the dates of publication. Web addresses are given so that a reader can check them; type them in yourself.

The five steps

- Federal Trade Commission, “How To Avoid a Scam”. The four signs: pretend, problem or prize, pressure, pay a specific way; and the advice to stop and talk to someone you trust. consumer.ftc.gov/articles/how-avoid-scam
- Federal Bureau of Investigation, Internet Crime Complaint Center, public service announcement I-091726-PSA of 17 September 2026 on law-enforcement and government impersonation: nearly 61,000 complaints and more than $1.6 billion reported lost between January 2025 and July 2026; callers urging people not to tell

family, friends, financial institutions or law enforcement; keeping people on the phone for the duration; payment by prepaid card, courier, wire, cryptocurrency and cash into cryptocurrency kiosks; artificial intelligence used to appear as law-enforcement and government officials on video calls; in some situations, fake police uniforms and mock sets of official facilities. www.ic3.gov/PSA/2026/PSA260917

- Stajano and Wilson, “Understanding Scam Victims: Seven Principles for Systems Security”, Communications of the Association for Computing Machinery, 2011. Related academic work on why scams succeed; its seven principles are not the five steps.

Scams of 2026

- Federal Bureau of Investigation, public service announcements of 15 May 2025 and 19 December 2025 (officials impersonated with cloned voices; advice to

create a secret word or phrase with your family), 13 August 2025 (fictitious law firms offering recovery), 20 July 2026 (deepfake video promoting a fake complaint website). www.ic3.gov/PSA/2025/PSA250515, PSA251219, PSA250813 and www.ic3.gov/PSA/2026/PSA260720

- Federal Trade Commission, press release of 15 June 2026, “FTC data show people reported losing $3.5 billion to imposter scams in 2025”: nearly one in three fraud reports in 2025 were imposter scams, reached by text, phone call, email, social media and search results. ftc.gov
- Federal Trade Commission, testimony to the Joint Economic Committee of Congress, 25 March 2026: $15.9 billion reported lost to fraud in 2025; imposter scams the most reported; investment scams the costliest. ftc.gov
- Federal Trade Commission, “Refund and recovery scams” and “What To Do if You

Were Scammed". consumer.ftc.gov

- Google, blog post of 12 November 2025 on its legal action against the "Lighthouse" text-message scam operation: "harmed over 1 million victims across more than 120 countries". blog.google
- Australian Competition and Consumer Commission, media release of 30 March 2026, and National Anti-Scam Centre, Targeting Scams Report 2025: A$2.18 billion in reported losses; investment scams largest at A$837.7 million; job scam losses reported to Scamwatch up 81.5 per cent, from A$13.7 million to A$24.8 million; job scam reports from people aged 25 to 34 up 102.5 per cent. accc.gov.au and nasc.gov.au
- UK Finance, Annual Fraud Report 2026, press release of 15 June 2026: £1.28 billion lost to payment fraud in 2025; authorised push payment fraud £576.4 million; investment fraud £221.5 million;

remote purchase card fraud £423.5 million. ukfinance.org.uk

- Canadian Anti-Fraud Centre, “Top 10 frauds in 2025”, 25 February 2026: C$704 million in reported losses; investment fraud C$351 million; fraud investigator scams C$28.3 million and recovery pitches C$25.9 million. antifraudcentre-centreantifraude.ca
- United Nations Office on Drugs and Crime and the European Union, statement of 30 July 2026 (World Day Against Trafficking in Persons), and United Nations Human Rights Office, report of 20 February 2026, on people lured by fake job offers into scam compounds in South-East Asia. unodc.org and news.un.org
- Federal Bureau of Investigation, 2025 Internet Crime Report, 16 April 2026: Operation Level Up contacted 3,780 victims in 2025, 78 per cent of whom were unaware they were being scammed.

www.ic3.gov/AnnualReport/Reports/2025_ic3report.pdf

Educators and prevention

- Public Library Association, Public Library Services for Strong Communities, 2025 survey, published June 2026: 83.3 per cent of United States public libraries offer at least one programme for adults aged 65 and over; 73 per cent partner with senior residences, centres or other organisations for older adults. ala.org
- Pew Research Center, “Barriers to adoption and attitudes towards technology”, 17 May 2017, reporting a survey of October to November 2015: 73 per cent of Americans aged 65 and over (48 per cent “very well” and 25 per cent “somewhat well”) said that when they get a new electronic device they usually need someone else to set it up or show them how to use it. pewresearch.org

- Financial Industry Regulatory Authority Investor Education Foundation, “Can Educational Interventions Reduce Susceptibility to Financial Fraud?”, March 2021: a three-minute video cut willingness to invest in fraudulent pitches by 42 per cent (text version 44 per cent) immediately; at six months, people with a single intervention were no better than those with none; those reminded at three months were 10 per cent less willing. finrafoundation.org
- Google Research, ShieldUp! trial (Roy and Mukherjee, arXiv 2503.12341, 16 March 2025): 3,000 participants in India; improved scam detection kept at the 21-day follow-up; the game outperformed videos and tips. arxiv.org
- Tannenbaum and colleagues, “Appealing to Fear: A Meta-Analysis of Fear Appeal Effectiveness and Theories”, Psychological Bulletin, 2015: fear appeals are effective, more so with a statement of

what to do, and more for one-time than for repeated behaviours.

- AARP and the Financial Industry Regulatory Authority Investor Education Foundation, “Blame and Shame in the Context of Financial Fraud”, 2022: 53 per cent of respondents saw fraud victims as culpable; 47 per cent said reporting is a lost cause. aarp.org
- Office for National Statistics, “Nature of fraud and computer misuse in England and Wales: year ending March 2025”, released 26 March 2026: feelings of shame, embarrassment or self-blame in 13 per cent of fraud incidents. ons.gov.uk
- Stop Scams UK, the 159 service: connects customers of more than 99 per cent of United Kingdom retail bank current accounts to their bank. stopscamsuk.org.uk/159

Reporting services

- UtilForge.org, “Where to report a scam, country by country”, the Middle East, Bangladesh and Maldives entries checked 18 October 2026 and the rest 1 October 2026, with each address opened on those dates; corrections from a line-by-line review on 19 October 2026. utilforge.org/official-help
- City of London Police, news of 4 December 2025: Report Fraud replaced Action Fraud in England, Wales and Northern Ireland; 0300 123 2040. reportfraud.police.uk
- Australian Competition and Consumer Commission, media release of 30 March 2026, recommending IDCARE (1800 595 160) and ReportCyber at www.cyber.gov.au.

The tools quoted

The short addresses used in the chapters go to the same pages as the full ones.

- Is this a scam text message? utilforge.org/text (utilforge.org/tools/is-this-a-scam-text)
- Before You Pay. utilforge.org/pay (utilforge.org/tools/before-you-pay)
- Before You Reply to a Recruiter. utilforge.org/jobs (utilforge.org/tools/before-you-reply-to-a-recruiter)
- Before You Invest. utilforge.org/tools/before-you-invest
- Family Safe Word. utilforge.org/safeword (utilforge.org/tools/family-safe-word)
- Someone offers to get your money back (a guide). utilforge.org/learn/someone-offers-your-money-back
- Redaction Studio. utilforge.org/redact (utilforge.org/tools/redaction-studio). Is It Really Blacked Out? utilforge.org/tools/is-it-really-blacked-out

- Hide Names from Artificial Intelligence. utilforge.org/tools/hide-names-from-ai. What Not to Paste. utilforge.org/tools/before-you-paste-into-ai. What happens to what you paste into an artificial intelligence (a guide). utilforge.org/learn/what-happens-to-what-you-paste-into-an-ai
- Digital Safety Clinics session plan. utilforge.org/clinics
- This book, and the five steps card to print. utilforge.org/book

Hidden instructions and invisible characters (chapter 24)

- Open Worldwide Application Security Project, “LLM01:2025 Prompt Injection”, in its 2025 Top 10 for Large Language Model Applications: prompt injection ranked first. genai.owasp.org
- National Cyber Security Centre (United Kingdom), “Prompt injection is not SQL

injection (it may be worse)”, 8 December 2025: large language models described as “inherently confusable”. ncsc.gov.uk

- United States National Vulnerability Database, CVE-2025-32711, published June 2025 (EchoLeak, disclosed by Aim Security): a flaw in Microsoft 365 Copilot, fixed by Microsoft before the details were published. nvd.nist.gov
- Microsoft Security Blog, 3 September 2026: an email campaign that hid invisible characters inside ordinary words to slip past email filters. microsoft.com/security/blog
- Prompt injection checker. utilforge.org/tools/prompt-injection-check. Invisible character remover. utilforge.org/tools/invisible-character-remover. Hidden instructions in web pages and emails (a guide). utilforge.org/learn/hidden-instructions-in-web-pages-and-emails

Every tool result quoted in this book was produced by pasting the quoted message into the tool on 18 October 2026, and is reproduced in the tool's own words. The results in Part One and Chapter 7 leave out the final line and the "What to do" box, as Chapter 1 says; the others are complete.

The VPN (chapter 25)

- Australian Signals Directorate's Australian Cyber Security Centre, "Wi-Fi, private and public", updated 11 April 2023. cyber.gov.au
- Federal Trade Commission, "Are public Wi-Fi networks safe? What you need to know", consumer advice, checked 24 October 2026. consumer.ftc.gov
- Wang, Ortwein, Stanley, Sobrados, Anwar, Sharma and Ensafi, "MVPNalyzer: An Investigative Framework for Auditing the Security and Privacy of Mobile VPNs",

Network and Distributed System Security Symposium, February 2026 (281 free VPN apps; 246 contacted advertising and tracking addresses; 29 leaked traffic). ndss-symposium.org

- Federal Bureau of Investigation, Internet Crime Complaint Center, “Evading Residential Proxy Networks”, public service announcement, 12 March 2026. ic3.gov
- Shufti Pro developer documentation, “Device risk signals” (VPN detected alert), and Spur knowledge base, “Should transactions be blocked simply because a VPN is detected?”, both checked 24 October 2026.

About UtilForge.org

UtilForge.org exists to help make a safer online world for all people. It makes free cybersecurity tools that run on your own phone or computer, where what you type stays; there are more than forty-five of them,

and the checks in this book are among them. They began inside one family. UtilForge is a registered 2026 Champion of Cybersecurity Awareness Month. If a check in this book has been useful to you, the most useful thing you can do is show it to one other person.

utilforge.org · support@utilforge.org

If you doubt it, UtilForge it.