



INSIDER



URGENT:

Verify Your Account
Immediately



Suspicious
Activity
Detected

The Complete Guide to Spotting & Stopping Scams



Don't take the bait.
Protect yourself,
and the people you love.



MEMBER GUIDE

The Complete Guide to Spotting & Stopping Scams

Don't take the bait. Protect yourself, and the people you love.

WRITTEN FOR YOU BY

Sandy Goldman

Founder, 65Nation

YOURS TO KEEP · YOURS TO SHARE

“

Pause. Reflect. Protect.

That pause is where scams go to die.

Contents

START HERE

A note from Sandy	5
The one rule that beats almost everything	6

PART ONE • THE ELEVEN SCAMS

1	The “Unpaid Toll” Text	8
2	The Frantic Call from “Family”	10
3	The Fake Warning on Your Screen	12
4	The Slow-Build Romance	13
5	The Medicare “Update”	15
6	The “Your Account Is Locked” Message	16
7	The Prize You Never Won	17
8	The “Get Rich” Investment	18
9	The Store That Isn’t There	20
10	The Threat from “the Government”	21
11	The Charity That Isn’t One	22

PART TWO • YOUR DEFENSE KIT

The five fingerprints of every scam	24
If it already happened	25
Your six-question gut check	26
Keep these numbers close	27
One last thing, from me to you	28

A NOTE FROM SANDY

Before we begin

Every day, someone your age loses their savings to a scam. Not because they are careless. Not because they are slipping. Because today's scams are built, very deliberately, to fool smart, capable people.

I am Sandy Goldman. Most mornings, I write to more than a hundred thousand of us at 65Nation. I put this little book together for one reason. I am tired of watching good people get robbed by cowards with a script.

So let me hand you what I have learned. Not fear. A plan. By the last page, you will spot these tricks before they spot you.

Why they come for us

Criminals target our generation on purpose. We tend to have savings. We answer the phone. We were raised to be polite and to hear a person out. Every one of those good qualities is something they try to turn against us.

But here is the good news. You do not need to memorize a hundred different scams. Underneath, they are all the same handful of tricks. Learn the pattern once, and you are protected against nearly all of them.

THE WHOLE SECRET

The one rule that beats almost everything

If you remember nothing else from this book, remember this.

Real people don't rush you. Real agencies don't ask for strange payments.

Every scam carries two fingerprints.

First, the urgency

They need you scared and moving fast, because a calm person asks questions, and a rushed person does not.

Second, the payment

Gift cards. Wire transfers. Crypto. “Move your money to keep it safe.” No honest agency, bank, or business ever asks for any of these.

THE WHOLE SECRET

Feel either one? **Stop.** Your pause is their biggest enemy.

PART ONE

The Eleven Scams

*Eleven stories, one pattern. Once you feel the trick underneath,
you are protected against nearly all of them.*



The “Unpaid Toll” Text

PICTURE THIS

It is a Tuesday morning. You are having your coffee when the phone buzzes. “E-ZPass: unpaid toll of \$6.75. Pay today to avoid a \$50 late fee.” There is a neat little link.

Six dollars. You do use that road now and then. Why risk a fifty-dollar penalty over pocket change? Your thumb drifts toward the link.

Stop right there. That flicker of hesitation you feel? That is the whole game, and you are about to win it.

Urgency is a weapon.

What's really going on

The tiny amount is the trick. Nobody argues over six dollars, so you tap before you think. The link opens a page that looks exactly like a real toll site. You type in your card to “settle up,” and just like that, they have it.

They never wanted the toll. They wanted your card.

DID YOU KNOW

In 2024, the FBI received more than 60,000 complaints about fake toll texts. You are not being singled out. You are one of millions.

Red flags

- ◆ A text about a toll you don't remember
- ◆ A tiny dollar amount, just small enough to pay without thinking
- ◆ A link to pay right now
- ◆ A deadline of “today”

What to do

Real toll agencies do not text you for money. Do not tap the link, not even to peek. If you truly wonder, look the agency up yourself and check.

BOTTOM LINE

Do not tap. Forward the text to **7726** (it spells SPAM), then delete it. That is the whole job.

Source: FTC alert, 2025; FBI Internet Crime Complaint Center.



The Frantic Call from “Family”

PICTURE THIS

It is late. The phone rings. “Grandma?” The voice is crying. “I’ve been in an accident. I’m in jail. Please don’t tell Mom and Dad.”

Your heart is in your throat before your mind can catch up. A calm man takes the phone and explains where to send the bail money.

Everything in you wants to help this instant. That feeling is exactly what they are counting on.

Fear is their business model.

What's really going on

This scam does not go after your wallet. It goes after your heart. And it has gotten frighteningly good. Criminals now copy a voice from a few seconds of video posted online. It really can sound like your grandchild.

Red flags

- ◆ A panicked call about a loved one in trouble
- ◆ A plea to keep it secret
- ◆ A rush to send money right now

What to do

Hang up. It is not rude, it is wise. Then call your grandchild or their parents on a number you already have. They will almost always be perfectly fine.

65NATION TIP

When someone tells you not to tell your family, that is not a secret. That is the alarm bell. Tell your family right away.

REMEMBER

Set a family **safe word** today. A real loved one in trouble will know it. A scammer never will.

Source: FBI Internet Crime Complaint Center; FTC.



The Fake Warning on Your Screen

PICTURE THIS

You are reading the news when the screen erupts. Red warnings. An alarm sound. “YOUR COMPUTER IS INFECTED. Call Microsoft now.”

A calm technician answers. He just needs to “connect” to fix it. Soon he is moving your cursor and asking you to log into your bank, only to “make sure it is safe.”

No real company hides a phone number inside a warning.

What's really going on

First they scare you. Then they hand you a rescuer. It is a one-two punch, and at first it fools almost everyone. Once they are inside your computer, they can empty accounts or plant a real virus.

Red flags

- ◆ A pop-up telling you to call a number
- ◆ A surprise call from “tech support”
- ◆ Anyone asking for remote access to your computer

What to do

That pop-up is fake, so do not call. Close the browser, or simply turn the computer off and back on. And never let a stranger control your screen.

THE ONE THING TO NEVER FORGET

Microsoft and Apple will never call you, and never put a phone number in an alert. **Not once, not ever.**

Source: FTC, Protecting Older Consumers, 2024 to 2025.



The Slow-Build Romance

PICTURE THIS

He found you on Facebook. Kind, funny, a wonderful listener. For two months you talk every day, and at last, someone truly gets you.

He travels for work, so a video call never quite happens. Then his daughter falls ill overseas, and he cannot reach his own money. He needs three thousand dollars. Just this once.

He has never asked you for a thing. That is what makes this one so hard, and so cruel.

What's really going on

This is the most patient scam of all. They spend weeks, even months, earning your trust before a single dollar is mentioned. By the time they ask, they do not feel like a stranger. They feel like love.

DID YOU KNOW

Romance scams cause some of the largest losses the FTC tracks. Individual victims have lost well into six figures.

Red flags

- ◆ A romance that moves fast online
- ◆ Someone who never video calls or meets in person
- ◆ Eventually, a request for money, gift cards, or crypto

What to do

Before you send anything, tell one person you trust. Search their photos online, since they are often stolen. And hold one line: no money to anyone you have not met in person.

65NATION TIP

A person who is real will get on a video call. A person who always has an excuse is telling you something. Listen to it.

IF IT HAPPENS TO YOU

There is no shame in having a kind heart. The shame belongs to the person who used it. Stop, and talk to someone you trust today.

Source: FTC.



The Medicare “Update”

PICTURE THIS

“We are sending out new Medicare cards with a security chip. I just need to confirm your number so yours reaches you.”

It is enrollment season. You have seen the ads about changes. It sounds like ordinary paperwork, so you reach for your wallet.

What's really going on

Your Medicare number is as precious as your Social Security number. Crooks use it to bill fake claims in your name, and that can foul up your real coverage when you need it. The “helpful update” is simply a way to get the number out of your mouth.

Red flags

- ◆ Anyone calling you first about Medicare
- ◆ “Free” braces or tests in exchange for your number
- ◆ Pressure to confirm today

What to do

Medicare already has your number. They will not call to ask for it. Never give it to someone who contacted you.

BOTTOM LINE

If you have a real question, you make the call. Dial **1-800-MEDICARE** or the number on your card. Never the other way around.

Source: FTC; Medicare.gov.



The “Your Account Is Locked” Message

PICTURE THIS

A text arrives: “Bank alert: did you try to send \$2,300? Reply NO to cancel.” You reply NO.

Seconds later, a calm “fraud agent” calls. Your account is under attack, he says. To keep your savings safe, you must move them into a “secure account” while they investigate.

He sounds like the only person on your side. He is the thief.

No one who truly wants to protect your money will ever ask you to move it.

What's really going on

They borrow a name you trust and add a jolt of fear. The link they send opens a perfect copy of your bank's login, so when you sign in, you hand over the keys. The “move your money” version is the worst of all, because you approve the transfer yourself. Banks may not give it back.

Red flags

- ◆ An urgent account alert with a link or a number
- ◆ A request to log in or “confirm”
- ◆ Anyone telling you to move money to keep it safe

What to do

Do not use the link or the number in the message. Call your bank on the number printed on the back of your card.

REMEMBER THIS ONE

Your bank will never ask you to move money to protect it. If someone does, they are robbing you. **Hang up.**



The Prize You Never Won

PICTURE THIS

“Congratulations! You have won five hundred thousand dollars!” To release it, you only owe \$499 in taxes and fees, payable today by gift card. And he is glad to stay on the line while you drive to the store.

Half a million dollars for a few hundred. It almost feels rude to say no.

What's really going on

Here is the whole con in one sentence. The prize is not real, and the fee is the scam. Pay one fee, and they will invent another, and another, for as long as you keep paying.

Red flags

- ◆ A prize you never entered
- ◆ A fee to collect it
- ◆ Payment by gift card or wire
- ◆ Pressure to keep it quiet

What to do

A real prize never costs you a penny to claim. Legitimate lotteries and sweepstakes do not charge you up front.

THE RULE THAT NEVER FAILS

If you have to pay to win, you already lost. **Hang up, and go enjoy the rest of your day.**

Source: FTC; AARP.



The “Get Rich” Investment

PICTURE THIS

A friendly new contact online keeps mentioning how well their investments are doing. Eventually they offer to show you.

Your first small deposit grows beautifully on a slick dashboard, so you add more. Then more. When you try to take your money out, there is a “tax” to pay first. Then the platform, and your new friend, both vanish.

What's really going on

This is the costliest scam in the country, and among the cruelest. The slow, friendly version even has a nickname: “pig butchering,” because they fatten you up before the end. The gains are fake. The platform is fake. Often, the friend is fake too.

DID YOU KNOW

In 2024, Americans lost about 9.3 billion dollars to crypto crime. Adults over 60 lost more than any other group, roughly 2.8 billion.

Red flags

- ◆ An investment tip from someone online
- ◆ Promises of big returns with little risk
- ◆ A special app you are steered toward
- ◆ Fees you must pay before you can withdraw

What to do

Go very slowly with any investment tied to someone you met online, or to crypto on a specific platform. Check any adviser for free at investor.gov before you send a cent.

65NATION TIP

Real investments do not come from strangers online, and you can always withdraw from a real one. If you cannot get your money out, it was never really there.

BEFORE YOU INVEST A DOLLAR

Talk to a licensed professional you found yourself, not one who found you. **That single call can save your retirement.**

Source: FBI Internet Crime Complaint Center, 2024 report.



The Store That Isn't There

PICTURE THIS

An ad shows the exact chair you have wanted, seventy percent off, “only 2 left.” The site looks polished and professional. You enter your card.

The chair never comes. The emails bounce. The store is gone, and so is your card number.

What's really going on

The unbeatable deal is the bait. The ticking clock is there to stop you from checking. The real product being sold is your payment information.

Red flags

- ◆ A price too good to be true
- ◆ A store you have never heard of
- ◆ A countdown timer
- ◆ Requests to pay by wire or gift card

What to do

Before you buy from a new site, search its name plus the word “scam.” And always pay by credit card, which has your back if things go wrong.

QUICK GUT CHECK

If the deal feels too good to be true on a store you do not know, it is. **Close the tab.**

Source: FTC.



The Threat from “the Government”

PICTURE THIS

“This is the Social Security Administration. Your number has been suspended, and a warrant is out for your arrest.” The caller ID even reads SSA.

To protect your money, they say, you must move it into a “secure federal locker,” which turns out to be a crypto machine at the corner gas station.

Real agencies mail letters. They don't call to threaten you.

What's really going on

They lean on our two deepest worries: money and the law. But no real agency threatens arrest by phone, and none will ever send you to a crypto machine or ask for gift cards. The badge, the warrant, the urgency. All of it is a prop.

Red flags

- ◆ A threatening call from an “agency”
- ◆ A suspended Social Security number or a warrant
- ◆ Demands for gift cards or crypto
- ◆ An official name on caller ID, which is easily faked

What to do

Hang up. If you want to be sure, call the agency yourself at its real number.

REMEMBER

The government writes to you. It does not call to frighten you. **When in doubt, hang up and look it up.**

Source: FTC; FBI.



The Charity That Isn't One

PICTURE THIS

Days after a hurricane fills the news, a warm voice thanks you for your past generosity and asks you to help the victims today, right now, with your card number.

The name sounds familiar. Almost. Your kindness is the very lever they are pulling.

What's really going on

Scammers read the headlines too. Disasters and holidays open our hearts, and they rush in before we can think. They borrow real charity names, or invent ones that sound right, and press for money on the spot.

Red flags

- ◆ Pressure to give this minute
- ◆ A name that is close, but not quite right
- ◆ Requests for gift cards or crypto
- ◆ Vague answers about where the money goes

What to do

Never give on a call. Say you will donate through the charity's own website, and check the name at give.org first.

65NATION TIP

Give on your terms, never theirs. A good cause today will still be a good cause tomorrow, after you have checked.

BOTTOM LINE

Your generosity is a gift. **Do not let anyone rush it out of your hands.**

PART TWO

Your Defense Kit

A handful of pages to keep near the phone. The patterns, the first moves, and the numbers that matter, all in one place.

The five fingerprints

Every scam in this book, and every one I did not have room for, shares the same five signs. Spot even one, and your guard should go up.

1 It comes to you

You did not ask for the call, the text, or the email. It arrived out of the blue.

2 It stirs up feeling

Fear, urgency, excitement, or love. Strong emotion is the tool that quiets careful thinking.

3 It rushes you

“Act now, or else.” Honest people and real institutions give you time.

4 It wants a strange payment

Gift cards, wire, crypto, or “moving money to safety.” No legitimate group ever asks for these.

5 It wants secrecy

“Don't tell anyone.” They fear a second opinion, because a trusted friend often sees what you cannot.

THREE WORDS WORTH TAPING TO YOUR PHONE

Pause. Reflect. Protect. When something trips one of these wires, take a real pause. That pause is where scams go to die.

FIRST AID

If it already happened

First, breathe. And hear me clearly: **this is not your fault**. You were targeted by a professional, and being fooled says nothing about how smart you are. Now, let us move fast.

- 1 Stop, and send nothing more.** There is no fee that fixes it, and no next step that is real.
- 2 Call your bank or card company now.** If you paid by gift card, call that company too, since some can still freeze the funds. Speed matters.
- 3 Report it.** File with the FTC at reportfraud.ftc.gov and the FBI at [IC3.gov](https://ic3.gov). It helps them catch the pattern and protect the next person.
- 4 Protect your identity.** If you shared personal details, place a free credit freeze with all three bureaus, and visit IdentityTheft.gov for a simple recovery plan.
- 5 Tell someone.** A trusted family member, and the AARP Fraud Watch Helpline, which is free and never judges. You are not alone in this.

THE WHOLE BOOK ON ONE PAGE

Your six-question gut check

Print it, cut it out, and keep it by the phone. Before you ever pay, click, or share a personal detail, run through these six questions. If even one answer troubles you, stop.

BEFORE YOU PAY, CLICK, OR SHARE

Six Questions

- ☐ Did this come to me out of the blue?
- ☐ Am I being rushed, frightened, or pressured to act right now?
- ☐ Am I being told to keep this a secret from my family?
- ☐ Is the payment strange? Gift cards, wire, crypto, or “move your money to keep it safe.”
- ☐ Have I truly checked who this is, using a number I looked up myself?
- ☐ Would I feel fine telling my family about this right now?

If any answer gives you pause: Pause. Reflect. Protect. Set the phone down, and call someone you trust before you do anything else. A real, honest request will still be there in an hour.

QUICK REFERENCE

Keep these numbers close

Print this page too, and keep it near the phone. When something feels off, one of these is the right call.

WHAT YOU NEED	WHERE TO GO
Report fraud (FTC)	reportfraud.ftc.gov · 1-877-382-4357
Report internet crime (FBI)	IC3.gov
AARP Fraud Watch Helpline	877-908-3360 · Mon to Fri, 8am to 8pm ET, free
Report a scam text	Forward the message to 7726 (SPAM)
Medicare questions	1-800-MEDICARE (1-800-633-4227)
Social Security	1-800-772-1213
Check an investment or adviser	investor.gov · BrokerCheck.finra.org
Check a charity	give.org · charitynavigator.org
Identity theft recovery	IdentityTheft.gov
Credit freeze (all free)	Equifax · Experian · TransUnion

ONE LAST THING

From me to you

If you have read this far, you are already harder to fool than you were an hour ago. Not because you memorized every scam, but because you can feel the tricks underneath them now: the rush, the fear, the strange payment, the whisper to keep it quiet.

But here is the truth about everything you just learned. Its real value is not that it protects you. It is that you will pass it on.

Knowledge like this isn't valuable because it helps you. It's valuable because you'll share it.

So send this to your husband, or your wife. Your brother, your sister. The neighbor who still answers every call. One conversation today could save someone you love thousands of dollars, and a great deal of heartache, tomorrow.

That is what 65Nation has always been about. Looking out for each other.

Sandy Goldman

FOUNDER, 65NATION



Stay sharp.
Stay safe.
Stay a step ahead.

65NATION INSIDER