

Avoiding Scams in an AI World

with John Beaumont



Spot scams, recognize red flags, and protect yourself.



URGENT:
Verify your account now
bit.ly/secure123



You've won!
Claim your prize
click-here.win



Account Update
Confirm your information
update-account.com



Suspicious Activity

Unknown sender
Unusual link
Requesting personal info

DO NOT CLICK

Scams Are Now a \$20 Billion Problem

Reported cyber-enabled fraud and scam losses continue to climb.

\$20.877B

reported losses to IC3* in 2025

Only reported losses are counted. The real impact is almost certainly higher.

*** Internet Crime Complaint Center. This is where the FBI collects reports of online scams, fraud, and cybercrime - the annual IC3 report is one of the best sources for scam statistics.**

Source: FBI IC3 2025 Annual Report, pp. 3-6.

FBI IC3 data reflects complaints submitted to IC3; not every scam is reported.

1,008,597

complaints reported

26%

increase in losses from 2024

~3,000

complaints per day

\$20,699

average reported loss

Florida Is a Major Target

This is not just a national issue - Florida ranks near the top.

FLORIDA

#3 nationally for both complaint count and total reported losses

Florida residents are heavily represented in scam reporting and losses.

California is #1 and Texas is #2 in the IC3 data

Axios reported, based on FTC data, that Florida led the U.S. in fraud reports in 2024, with residents reporting \$866 million in fraud losses, and that Tampa Bay ranked 9th nationally among metro areas by fraud cases per 100,000 residents.

71,843

complaints from Florida

\$1.596B

reported Florida losses

306.2

complaints per 100,000 residents

\$6.8M

losses per 100,000 residents

Source: FBI IC3 2025 Annual Report, pp. 27, 28, 29, 30, 31.

Florida data includes reported IC3 complaints where state information was provided.

Slam the Scam: Identifying and Avoiding Scams in an AI World

Older Adults Report the Largest Losses

The 60+ group is hit especially hard in reported losses.

60+

reported **\$7.748 billion** in losses

12,444 complainants age 60+ lost more than \$100,000.

Seniors are deliberately targeted

201,266

complaints from people age 60+

\$38,500

average loss

+37%

complaint increase from 2024

+59%

loss increase from 2024

Source: FBI IC3 2025 Annual Report, p. 44.

60+ data is based on complaints filed by individuals age 60 and older.

Slam the Scam: Identifying and Avoiding Scams in an AI World

Today's Roadmap

What we will cover in this class

The Scam Landscape

- 1 How Scams are changing in the AI era

How Scams Work

- 2 The emotional triggers that scammers use

Common Scam Types

- 3 The scams that you are most likely to encounter

Identity Theft

- 4 Scammers use personalized public info

AI makes scams convincing

- 5 Fake voices, images, polished emails.

Using ChatGPT

- 6 Use AI safely to analyze suspicious messages

Using ChatGPT Demo

- 7 Real examples and spotting red flags

What to do if you are Targeted

- 8 Practical steps if something feels wrong

Simple Takeaway Message

- 9 Stop – Check – Verify - Report

The Scam Landscape

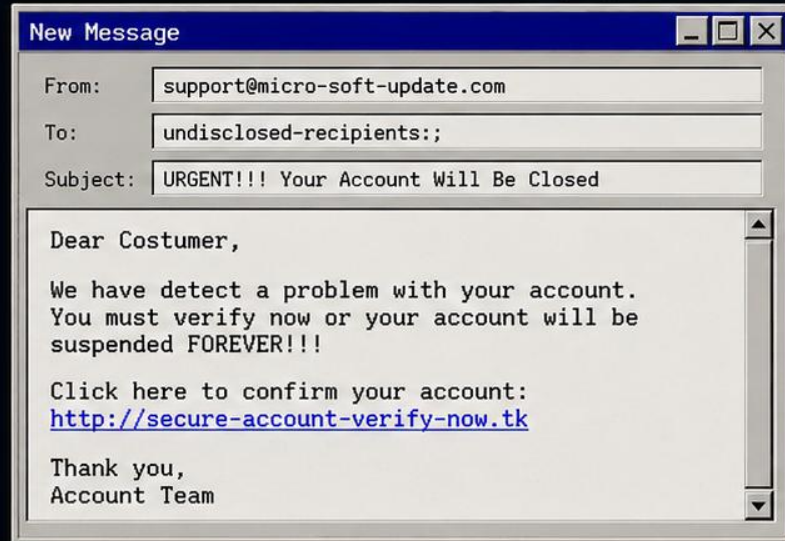
How Scams are changing in the AI era



Scams Are Not New — But They Are Getting Better

They Are Using AI too

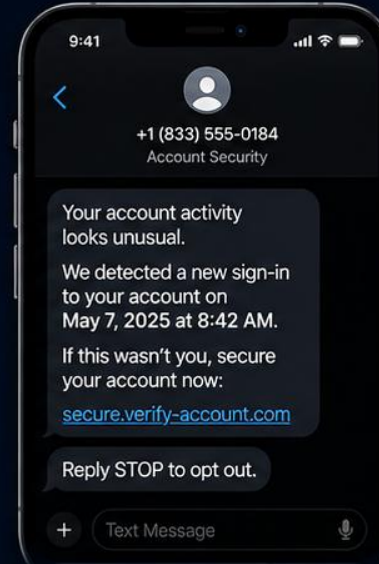
Then



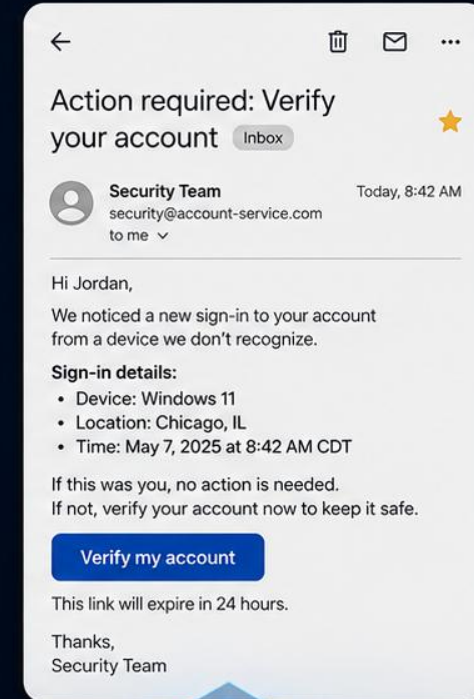
- ✗ Bad spelling
- ✗ Obvious fake sender
- ✗ Strange story
- ✗ Suspicious link
- ✗ Easy to dismiss



Now



- ✓ Better writing
- ✓ Familiar branding
- ✓ Personal details
- ✓ Realistic urgency
- ✓ Harder to dismiss



Same tricks. Better packaging.

Scammers Target Moments — Not Foolish People

The danger moment is when we are rushed, worried, distracted, helpful, lonely, or hopeful.



Scammers target moments of emotion and distraction.

That's why slowing down is one of your best defenses.

The Most Important Skill: Pause

Scammers want speed. Your defense is the pause.



How Scams Work

The emotional triggers that scammers use



The Four Buttons Scammers Push

Most scams are built around one or more emotional triggers



Fear

You're in trouble



Urgency

Act now



Authority

I'm official

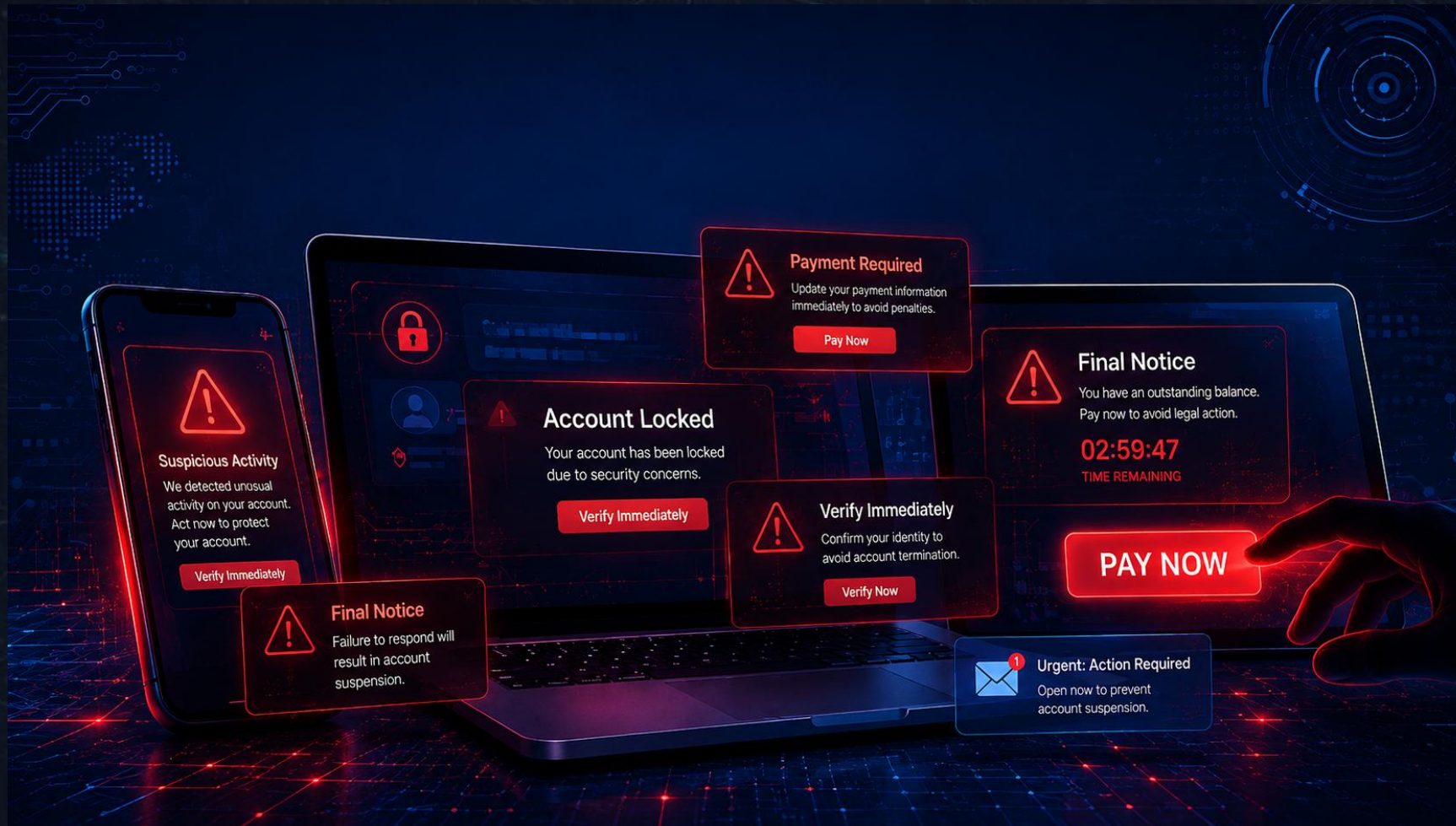


Opportunity

You've been selected

Fear: “Something Bad Is Happening”

Scammers want panic to outrun judgment



Common fear messages

There's fraud on your account
You owe money
Your identity has been stolen
You could be arrested
Your computer has been hacked
A family member is in trouble

Urgency: “Act Now!”

Scammers don't want you to think — they want you to react

Watch for phrases like:

Act now
Verify immediately
Final notice
Your account will be closed
You have 24 hours
Don't hang up
Files will be deleted



Authority: “Trust Me, I’m Official”

Scammers borrow trust from names we recognize

**SPOOFED
CALLER ID**



This is the Social Security Fraud Department.
Do not hang up.



We need to **verify** your account **immediately.**



REMEMBER

- Government agencies won't call to demand payment.
- Don't share personal or financial information.

They may pretend to be from:

Your bank

The IRS

Social Security

A police department

A tech support company

A lawyer or government agency

A well-known store or entity

Opportunity: “This Could Be Your Lucky Day”

Not every scam threatens you — some flatter you

Opportunity scams:

You’ve been selected
You may be entitled to money.
This investment is low-risk
A relative left unclaimed assets
This offer expires soon
You have special expertise
Download this special app
Use this coupon



Common Scam Types

The scams that you are most likely to encounter



Classic Scams – Old But Still Working

The classics still work because they target familiar worries and hopes:

Government imposter scams

“This is Social Security / IRS / Medicare...”

Bank and credit card scams

“There is suspicious activity on your account...”

Tech support scams

“Your computer is infected...”

Prize, sweepstakes, and inheritance scams

“You have won/inherited money...”

Romance and friendship scams

“I care about you... but I need help...”

Charity scams

“Please donate now...”

Check and wire scams

“Send payment quickly...”



What's Happening Today in Florida

Active Scams that you might see

1



#1 Imposter Scams

Fake IRS, Social Security, Medicare, tech support, or even family calls.

2



Jury Duty Scams

'You missed jury duty.' Arrest threats and demands for payment by gift card, Zelle, Venmo, or crypto.

3



AI Voice / Grandparent Scams

A loved one sounds panicked and asks for money immediately.



Florida is a major fraud target.

4



Property Deed Fraud

Criminals file false documents against homes. Property fraud alerts can help.

5



Investment & Crypto Scams

High return, low risk, limited time — often ending in real losses.

6



Romance Scams

Online relationships build trust, then turn into requests for money.

ALSO ACTIVE:



Toll / SunPass-style texts

Smishing texts claim unpaid tolls. Clicking can steal your info or install malware.



Fake online shopping deals

Too-good-to-be-true prices and fake stores steal your money and personal information.



Current Example

The Walmart Robocall Scam



The scam is not the purchase — the scam is your reaction.

The fake fraud alert

HOW THE SCAM WORKS

1 Trusted brand



Scammers spoof Walmart's phone number so the call looks real.

2 Big unexpected charge



You're told there's a suspicious purchase you didn't make.



3 Urgent action: "Press 1"



You're pressured to press 1 immediately to "stop" the fraudulent charge.

4 Fake representative



You're connected to a scammer posing as a Walmart fraud specialist.

5 Personal information requested



They ask for your card number, account login, SSN, or one-time codes.



Once you engage, they can **steal** your money and your **identity**.



STAY SAFE: 3 SIMPLE STEPS



Do not press 1
Never respond to robocall prompts.



Hang up
End the call immediately.



Check the official app or website
Sign in yourself or call the official number on the back of your card.



Remember: Legitimate companies will **never** call and ask for your personal or financial information.

Be informed. Be cautious. Be secure.

Where Are We Heading?

More Personal. More Convincing. More Automated.



PUBLIC RECRDS



GENEALOGY DATABASES



CLONED VOICE



FAKE IMAGES / DEEPFAKES



ROBOCALLS



CHATBOTS



MASS TEXTS



EMAIL



PHONE

More Personal

Scammers know more before they contact you

Public Records
Social Sites
Genealogy Databases
Cookies
Information for Sale
Data breaches



COOKIES



INFORMATION FOR SALE



DATA BREACHES



SOCIAL SITES



PROPERTY RECORDS

More Convincing

AI makes scams sound and look legitimate

AI-written emails with fewer mistakes
Cloned voices that sound like family
Fake images, documents, or videos
Professional-looking fake websites
Personal Information



AI-WRITTEN FAKE EMAILS



FAKE DOCUMENTS



FAKE WEBSITES

More Automated

Scammers can target more people, faster

Mass texts and robocalls
AI-generated messages
Chatbots posing as support agents
Rapid follow-up across phone, email, and text
Cloned phones and emails



Identity Theft

Scammers use personalized public info



The Impact of Identity Theft

Why this deserves serious attention

IDENTITY THEFT: THE IMPACT IN 2024

1.1M

identity theft reports
filed with the FTC

Up 9.5% from 2023

\$47B

lost to identity fraud
& scams combined

Up \$4B from 2023 — AARP/Javelin

18M

Americans affected by
traditional ID fraud

Up from 15M in 2023



Slow Recovery

Nearly half of victims said issues were STILL unresolved 12 months later



Emotional Toll

43% experienced anxiety or depression; 42% developed lasting trust issues



Older Adults Hit Hardest

Adults in their 70s lost a median of \$1,000 — vs. \$417 for those in their 20s



Florida #1 Nationwide

Highest ID theft rate in U.S.: 138 reports per 100K residents in 2024

Identity Theft: The Scam That Keeps Going

Identity Theft: One Theft, Many Ways to Exploit You



Identity theft can affect **nearly every part of your life.**

Identity Theft Is Often Harder to Spot Than a Scam

It can begin quietly — with small pieces of information collected over time.

Identity theft can start with:

- **A fake verification request**
Confirm your SSN, Medicare number, or date of birth
- **A one-time passcode**
Read me the code we just sent you
- **A phishing link**
Update your account information here
- **A stolen check or document**
Personal information taken from mail or paperwork
- **A compromised email account**
Password resets, bank alerts, and impersonation
- **A data breach**
Your information exposed before the scam ever begins



If You Think Your Identity Has Been Compromised

Act quickly — but don't panic.



1



Pause and breathe

Do not let panic make the decision.

2



Talk to someone you trust

A friend, family member, bank, or advisor can help you think clearly.

3



Stop contact

Do not reply, click, send money, or provide more information.

4



Lock down cards and accounts

Use your bank or credit card app/website to freeze, lock, or report a card.

5



Contact the real organization

Use the official app, website, statement, or phone number — not the one in the suspicious message.

6



Change passwords and check activity

Focus on email, banking, credit cards, retirement, and benefit accounts.

7



Freeze credit and report it

Consider a credit freeze and report identity theft at [IdentityTheft.gov](https://www.identitytheft.gov).



Speed matters. Shame does not. Ask for help quickly.



AI makes scams convincing

Fake voices, images, polished emails.



AI Lowers the Bar for Scammers

You no longer need much skill to create something convincing



In the past, scammers needed some skills.

- Write believable messages
- Research official jargon
- Create convincing stories
- Technical skills to engage
- Skills to avoid detection

But still most scams were easy to spot

Now, AI will help them

- Write a polished email
- Sound believable and official
- Personalize the story
- Do the technical work
- Mask the scammer

AI can turn a clumsy scam into a believable one.

Scammers Can Now Easily Copy the Signs of Trust

Logos, Caller ID, emails, and websites can all be copied or faked



We used to trust:

- Logos
- Caller ID
- Email addresses
- Phone numbers
- Websites
- Official wording

But scammers can now copy or fake them.

The new rule:

Looking real is not the same as being real.

Voice and Video Threats Are Increasing

Specifically targeted



-  Social media videos
-  Voicemail greetings
-  Public recordings
-  Compromised accounts



AI can now make a scam call sound like someone you trust.

Voice samples may come from:

- social media videos
- voicemail greetings
- public recordings
- compromised accounts



FBI warning:

Criminals are already using AI-generated voice messages to impersonate trusted people and officials.



Bottom line:

A familiar voice is no longer proof.

The Cloned Scams Still Work The Same Way

They rely on you trusting your own senses



1



Believable voice

A familiar voice gets attention

2



Emotional emergency

Accident, arrest, or crisis

3



Authority added

A lawyer or official joins in

4



Urgent demand

Money, access, or information now

5



No time to verify

Don't call anyone. Act now



Bottom line: The voice gets your attention. The pressure gets your money.

A Real Florida Case

"When I picked up the phone, it was my daughter's voice"

\$15,000

lost after an AI voice impersonation
call

Dover, Florida • Hillsborough County

What happened:

- A frantic call sounded like her daughter crying
- The caller claimed there had been a car crash
- A supposed public defender demanded bail money
- Cash was handed to a "legal courier"

Lesson:

**When emotion is high,
verification must be stronger.**



The screenshot shows the top portion of a news article on the FOX 13 Tampa Bay website. The navigation bar includes links for News, Weather, Sports, Good Day, We Live Here, Contests, and More. The main headline reads: "Dover woman loses \$15K after scammers used artificial intelligence to impersonate daughter". Below the headline, it says "By Aaron Mesmer | Published July 17, 2025 10:49pm EDT | Hillsborough County | FOX 13 News |" followed by a right-pointing arrow.

The Best Defense: A Family Code Word

When the voice sounds real, ask for something only family would know



Create a private family code word

- Choose something simple, but not obvious
- Share it only with close family members
- Do not post it, text it widely, or use it as a password
- Practice the rule: No code word = no money, no action



Use it when a call feels urgent:

- “Mom, I’m in trouble.”
- “I was in an accident.”
- “I’ve been arrested.”
- “Please don’t tell anyone.”
- “I need money right now.”



If they can’t give the code word, **stop** and verify another way.

How to Respond to AI-Enabled Scams

New threats require a few new habits

AI-Enabled Threat	What To Do
 Polished scam emails and texts	 Don't trust good grammar. Verify the sender.
 Fake websites, spoofed numbers, copied logos	 Use your own trusted website, card, or statement.
 Voice cloning	 Use a family code word. Call back on a known number.
 Personalized messages	 Pause and ask: How would they know this?
 Urgent emotional pressure	 Slow down. Never let urgency skip verification.
 AI at scale	 Expect more scams, more often, and more believable.



Bottom line: Don't rely on how real it looks or sounds. Rely on how well it is **verified**.



Next: Use ChatGPT — or another Gen-AI tool — to help analyze suspicious messages.

Using ChatGPT

Use AI safely to analyze suspicious messages



AI Can Help You Slow the Scam Down

Use ChatGPT as a 'pause button,' and help gather your thoughts.



Scammers want speed. ChatGPT can help you slow down.

slide text:

- Paste suspicious text into ChatGPT — not links or attachments
- Ask it to look for pressure, fear, urgency, and unusual requests
- Ask: "What would a legitimate company or agency do instead?"
- Use it to create a safe verification plan
- Then verify through official sources — not through the message itself



PAUSE

Take a breath.
Don't rush.



ANALYZE

Look for red flags,
pressure, and
unusual requests.



VERIFY

Check through
official sources
you trust.



What ChatGPT Is Good At

ChatGPT is good at spotting patterns — especially emotional manipulation.



ChatGPT helps you spot patterns, explain red flags, and think more clearly.

slide text:

- Identifying scam language and pressure tactics
- Explaining why something feels suspicious
- Summarizing a confusing message in plain English
- Listing questions to ask before responding
- Drafting a calm message to a trusted person for a second opinion



SPOT

Find pressure and urgency



EXPLAIN

Turn confusion into plain English



PLAN

Suggest safe next steps



What NOT to Put Into ChatGPT

Use AI to analyze the message — not to expose yourself further.



**Analyze the message —
don't expose yourself further.**

- Don't paste SSNs, account numbers, passwords, or one-time codes
- Don't upload suspicious attachments
- Don't click links so ChatGPT can “check them”
- Don't copy full email headers unless you know what you're doing
- Don't ask ChatGPT to call, email, or interact with the scammer



**Ask a smart friend to look —
but cover up your private information first.**



REDACT
Hide personal
information
(SSN, accounts, DOB)



HIDE PASSWORDS
Don't share
passwords



HIDE CODES
Don't share one-time
codes or OTPs



DON'T UPLOAD
Don't upload suspicious
attachments



DON'T CLICK LINKS
Don't ask AI to check
links



NO CONTACT
Don't ask AI to call,
email, or contact
the scammer



ChatGPT Can Be Wrong Too

AI can help you think — but it can also make mistakes.



Helpful, but not always right.

- It may miss a scam
- It may overreact to a legitimate message
- It may suggest a wrong website or phone number
- It may sound confident even when unsure
- Always verify through official sources



**Use AI to think it through —
not as your final authority.**



The Safe AI Rule: Analyze, Don't Act

ChatGPT can help you think through a suspicious message — but you still verify before doing anything.



Analyze the message



Look for red flags



Remove private information



Create a verification plan



Verify independently before acting



Use AI as a thinking partner — not as the final authority.



ChatGPT

Here are some things to consider:

- ✓ The sender is unknown.
- ✓ Urgent requests for action.
- ✓ Links may be suspicious.
- ✓ Verify with the official organization.



Verify with official sources



Visit the official website



Call the official phone number



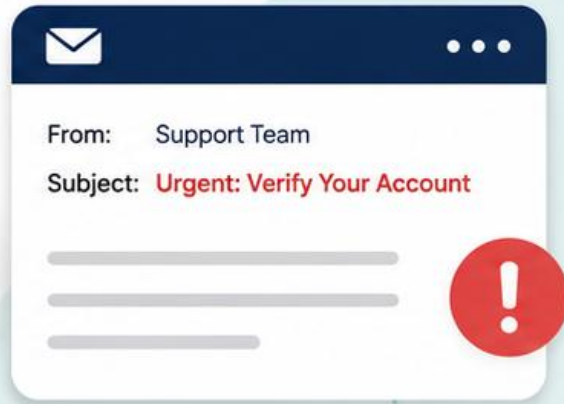
Contact through known channels



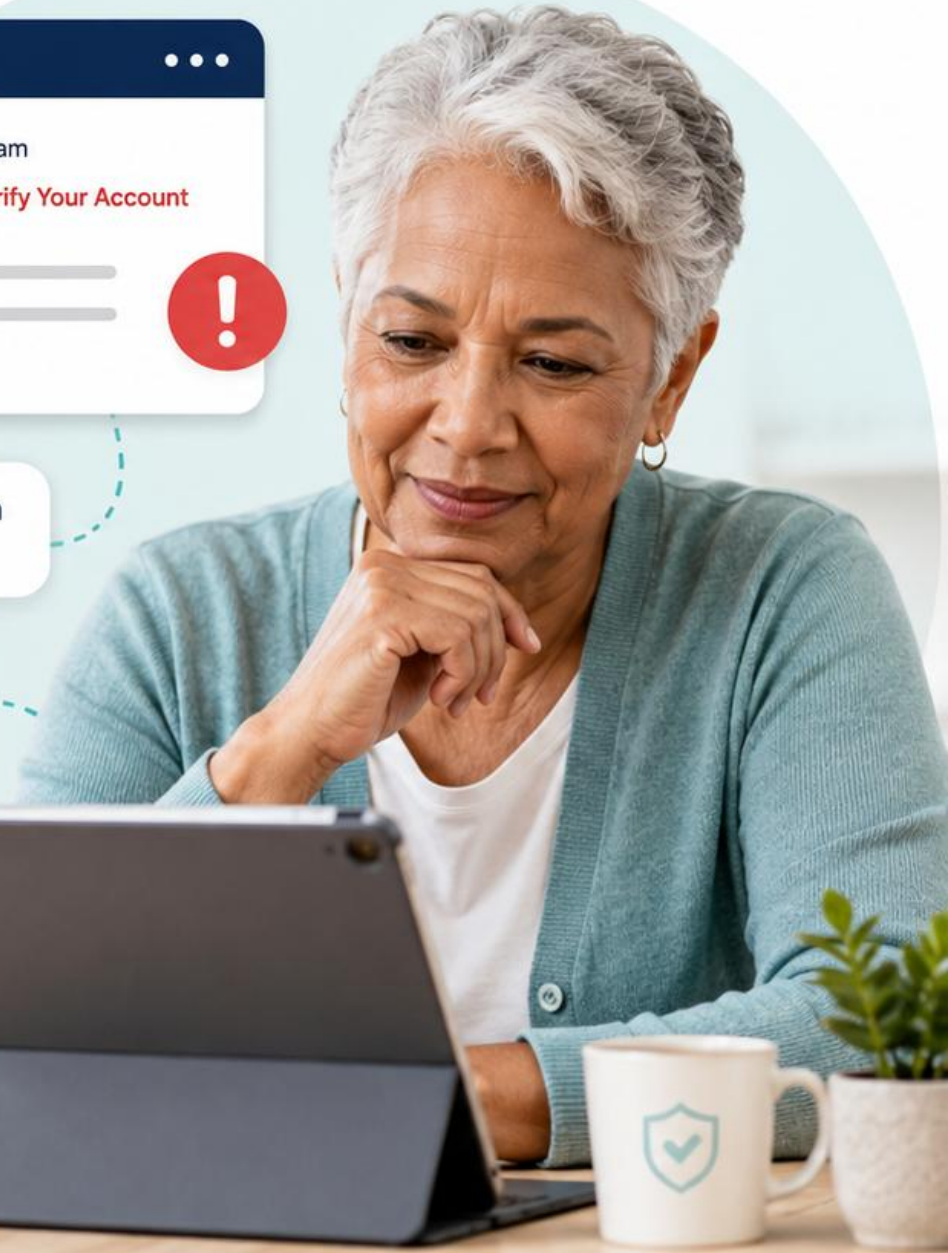


Real examples and spotting red flags

 Live Demo



 Can you confirm your details?



Takeaway Prompt: Ask AI to Help Spot Scams

Copy, paste, and then add the suspicious email, text, letter, or screenshot underneath.

COPY & USE

You are a friendly, encouraging fraud and scam detection guide helping adults recognize scams before they become victims. You communicate in plain, accessible language and never make anyone feel bad for asking.

Analyze the content I have provided, identify potential scam indicators, explain why each element is suspicious (noting red flags, risk levels, bogus information, etc.), and provide clear recommended actions.

Reminder: AI is a helper, not the final authority — verify through official websites, statements, or phone numbers you already trust.

Reminder! Your payment is overdue.



Xfinity BillPay <kq@mobiletorque.net>

To: support.no-reply@mail.xfinity.com

Reply

Reply all

Forward



Sun 5/17/2026 9:41 AM

The attachments on this message have been blocked for your safety. If you are certain that this message is safe, you can mark it as not Junk in order to access attachments.

Inbox Roles
300 bytes

Mail#5651301875
316 bytes

Document#5651301875
332 bytes

3 attachments (948 bytes)



We haven't received your payment

Xfinity offers options to help you pay your bill.

Please make a payment to avoid service suspension on the account

[Make a payment](#)

[Need help paying your bill?](#)

Xfinity offers payment options designed to work for you. any options you're eligible for will appear automatically when you go to make a payment online.

THIS IS A SERVICE-RELATED EMAIL



Gordon Carter

To: You

Reply Reply all Forward

Thu 1/8/2026 8:47 PM

Attention: John Beaumont,

I hope this message finds you well. I'm Gordon Carter, an attorney accredited by the Private Investigation Bureau (PIB) in collaboration with National Association of Unclaimed Property Administrators (NAUPA). I am currently engaged in a confidential research project on behalf of Fidelity Private Investments, a financial division of Fidelity Management Groups. I got your email from family search site while I was tracing family records, you ought to be notified through an official posted mail. However, accept my apology receiving this without prior notice. This project has been a significant focus of my recent work, I'm excited to share my findings with you:

This research pertains to a deceased client of the bank, Chris Beaumont, who shares your surname and has similar family details. My investigation has uncovered significant financial assets held by the bank in connection with this individual. Chris Beaumont passed away in January 2020** aged 82 has no other heirs listed to claim financial assets. Consequently, the bank has tasked me with identifying a relative for the purpose of facilitating a deposit claim. I would like to discuss the following points in detail:

1. Are you aware of any relative or extended family of yours passed away in January 2020** whose last known address/location was within Marietta, GA.
2. Are you aware of any reasonable financial investment made by this individual with Fidelity Private Investment a financial investment arm of Fidelity Group?
3. Could you establish beyond reasonable doubt your eligibility to assume the status of successor in title to the deceased if you are found suitable for recommendation.
4. Would you accept being presented to the deceased Bank as Next of Kin with detailed genealogical record proving your relationship while we work out the Legal formality?

In this proposal, I have outlined the objectives, methodology, and expected outcomes of this research. This project has the potential to contribute valuable insights to our field, and I am eager to hear your thoughts on it. Your expertise and perspective would be incredibly beneficial as I refine my approach and consider any additional angles that may enhance this research. Your positive answers would help conclude my investigation and submit an inquiry report for review, this would also guide the financial institution towards legally appointing an eligible relative to inherit this investment fund. I would provide you additional information at the receipt of your response.

Thank you for considering my proposal. I look forward to your valuable feedback and hope to engage in a fruitful discussion soon.

Best regards,

Gordon Carter
Admitted Attorney
BA (Law); LLB



Karl borgmann Talent acquisition

To: You

Reply Reply all Forward

Sat 4/4/2026 7:30 PM

Hi John,

You have been specifically identified through a targeted global talent mapping initiative focused on leaders shaping the intersection of enterprise technology transformation, AI adoption, and large-scale operational innovation.

Your career spanning senior leadership roles at organizations such as SAP and Software AG, combined with more than three decades of experience delivering enterprise technology initiatives and guiding organizations through complex digital transformations, places you among a select group of executives capable of bridging business strategy with emerging AI capabilities.

Your recent work as a Generative AI instructor and advocate, along with your extensive background in SAP program delivery, enterprise systems, and global technology leadership, reflects a rare ability to translate advanced technologies into practical, real-world applications that organizations can operationalize.

We are currently leading a confidential search for a Chief AI Officer / Global Head of AI Governance for a category-defining organization undergoing large-scale AI transformation.

This mandate requires a leader capable of embedding governance directly into AI-enabled enterprise systems while scaling global data and AI operating models across complex technology environments.

This is not an open market opportunity. You were identified as part of a highly curated shortlist based on your experience across enterprise IT leadership, large-scale transformation programs, AI enablement, and governance of complex technology ecosystems.

The role centers on architecting and executing enterprise AI governance frameworks that move beyond documentation into enforceable system-level design, while overseeing global AI and data initiatives with direct strategic impact on the organization's long-term transformation agenda.

The compensation structure reflects the strategic importance of the mandate, with a total target range between \$1.8M and \$2.6M, inclusive of long-term equity and performance incentives.

This process is highly confidential and moving with urgency, and I am currently finalizing the shortlist for presentation to the hiring board.

Due to the nature of this process, I do not conduct preliminary calls.

Please reply directly to confirm whether you would be interested in reviewing the full mandate, or if you prefer to continue in your current capacity.

If I do not hear back, I will proceed with advancing other candidates.

--

Karl Borgmann Talent Acquisition [Rangam Consultants Inc.](#)



kariborgmann.talent.acquisition@gmail.com

Providence, Rhode Island, United States

Experienced Talent Acquisition professional and trusted advisor with a demonstrated history of delivering compliant and effective hiring solutions for business partners and clients. Skilled in talent acquisition, talent management, team development, compliance management, and program data analytics.

Reply Forward

What to do if you are Targeted

Practical steps if something feels wrong



IF SOMETHING FEELS WRONG:

Stop First — The First Win Is Not Responding Immediately



Hang up or stop the conversation — you don't owe anyone an explanation



Don't send money, gift cards, crypto, or wire transfers — ever



Don't reply to emails, texts, or DMs from the sender



Don't share passwords, Social Security numbers, or one-time codes



Screenshot the message before closing it if you can



It's OK to say 'I need to think about it' — real organizations allow this



Don't click any links or call numbers they gave you



Talk to someone you trust before doing anything

IF YOU SHARED INFORMATION OR SENT MONEY

Act quickly — but don't panic. Every step helps.



Contact your bank or card issuer

Call the number on your card — or lock the card in online banking



Change passwords

Start with email and banking; use unique passwords



Document everything

Save messages, screenshots, dates, numbers, and what was said



Contact the payment service

Wire service, Zelle, Venmo, PayPal, gift card issuer — act fast



If personal info was shared: freeze your credit

Free at Equifax, Experian, and TransUnion



Set up account alerts

Turn on transaction and login notifications



If you gave computer access

Disconnect from the internet; get trusted technical help before reuse



Call a fraud support line

AARP Fraud Watch Network: 877-908-3360

If your SSN was shared: contact SSA, request an IRS Identity Protection PIN, and place fraud alerts or credit freezes.

Simple Takeaway Messages

Be proactive – Be a harder target





BE PROACTIVE: SET UP YOUR DEFENSES

Small steps now can make scams easier to spot — and harder to succeed.



Turn on two-factor authentication

On email, banking, shopping, and social media accounts



Set up bank and card alerts

Transaction alerts, login alerts, and low-balance alerts



Freeze your credit files

Equifax: [equifax.com](https://www.equifax.com)
Experian: [experian.com/freeze/center.html](https://www.experian.com/freeze/center.html)
TransUnion: [transunion.com/credit-freeze](https://www.transunion.com/credit-freeze)



Sign up for Florida Property Fraud Alert

hillsclerk.com/property-fraud-alert



Sign up for USPS Informed Delivery

usps.com/manage/informed-delivery.htm



Join the National Do Not Call Registry

donotcall.gov



Report Social Security scams

ssa.gov/scam



Use card locks / spending limits

Many banks let you lock cards or set transfer/spending limits in online banking

You do not have to do everything today — start with one or two protections.

BE PROACTIVE: MAKE YOURSELF A HARDER TARGET

Reduce pressure, reduce access, and reduce what scammers can use.



Let unknown calls go to voicemail

Real organizations will leave a message



Create a family code word

A strong defense against AI voice-cloning and emergency scams



Change passwords regularly

Use strong, unique passwords; a password manager can help



Manage your digital footprint

Share less publicly and review privacy settings often



Verify urgent requests offline

Call a known number or speak to someone directly



Be cautious with quizzes, forms, and "free" offers

They may collect personal details for scams



Keep recovery info current

Update your backup email, phone, and security questions



Ask for a second opinion

Talk to someone you trust before sending money or information

Small habits can make you much harder to fool.

My Upcoming OLLI Classes

Genealogy Made Easy: A Practical Guide to Your Family History

May 27th – 10 am

Easy AI: Making The Most of ChatGPT Everyday

June 16th - 10 am

Living in an AI- Driven World: What Everyone Should Know

June 30th - 10 am

Easy AI: The Secrets to a Great Gen-AI Prompt

July 7th - 10 am

All my AI classes will be at USF NEC 107. Genealogy Class at the North Tampa Branch Library

Thank You For Attending: Any Questions?



**Don't forget to
complete the class
survey**

My YouTube Channel: <https://www.youtube.com/@Beaumont-Genealogy/videos>

My Genealogy Website: (for this Presentation) <https://www.beaumont-genealogy.com/classes>

My Email: John.Beaumont@Outlook.com