

The Forged Record in Your Inbox

Genealogists are trained skeptics. You already know a transcription is not a source, a family legend is not a citation, and a record is only as good as its provenance. The same discipline — applied to your email — is the single best defense against the scams now aimed at older adults.

Every serious family historian has met a forged record: the pedigree that conveniently connects to royalty, the "index entry" three steps removed from any original document. You didn't fall for it, because you asked the genealogist's questions: **Who created this? Where did it really come from? Does the original say what the copy claims?**

Scam emails are forged records. They claim a false origin, they cite documents that don't exist, and they fall apart under source criticism. The difference is the stakes:

\$7.7 billion

reported lost to fraud by
Americans age 60+ in 2025 — up
37% in a single year

\$352 million

of that came from scams using AI
tools such as cloned voices, with
more than 3,100 victims over 60

3 questions

are enough to catch nearly all of
it — the same three you ask of
any record

Sources: FBI Internet Crime Complaint Center (IC3), 2025 Elder Fraud Report.

Reading the forgeries

Below are seven invented example messages — composites of real scams reported this year, rebuilt as training specimens. Every red-dashed box marks a tell. **None of these is a real message, and the companies named do not exist;** the patterns, however, arrive in real inboxes every day.

EXHIBIT A**The subscription that never was****TRAINING EXAMPLE — THIS IS A FAKE EMAIL, ANNOTATED**

From: Heritage Archive Plus <billing-dept8842@secure-notice-center.com¹>

To: you@example.com

FINAL NOTICE: Your annual renewal of \$499.99 processes TODAY²

Dear Valued Customer,³

Your Heritage Archive Plus Premium membership will automatically renew today for \$499.99. Your stored family trees and DNA matches will be permanently deleted if payment fails.

If you did not authorize this charge, you must cancel within 2 hours:

Cancel My Renewal »⁴

Link destination: <http://heritage-archive.account-verify-33.ru/cancel>⁵

Or call our Billing Protection Team immediately: +1 (888) 555-0147⁶

Heritage Archive Plus · Member Services

- 1 The sender's address doesn't match the name.** "Heritage Archive Plus" writes from secure-notice-center.com. A real company mails from its own domain. This is the provenance check — always read the part after the @.
- 2 Alarm plus a deadline in the subject.** "FINAL NOTICE" and "TODAY" exist to make you act before you think. Real billing gives you notice measured in weeks, not hours.
- 3 A generic greeting.** A service you actually pay knows your name. "Dear Valued Customer" means a list of thousands got this same message.
- 4 A button demanding immediate action.** The scam works whether you "cancel" or "confirm" — either click leads to a page asking for your card number to "process the refund."
- 5 The link's real destination is nothing like the company.** On a computer, hover the mouse over any button or link without clicking and the true address appears in the corner of the window; on a phone or tablet, press and hold the link and the address pops up. Random numbers and unfamiliar endings like this are conclusive.
- 6 A phone number in the email itself.** Calling it connects you to the scammer's own "billing team." If you ever want to verify a charge, find the number on your statement or the company's real website — never in the message.

One more tell for genealogists: you'd remember subscribing. Scammers invent a service and bill you for it precisely because "wait, do I have that?" makes people call the number to find out.

EXHIBIT B**The grandchild in trouble****TRAINING EXAMPLE — THIS IS A FAKE EMAIL, ANNOTATED**

From: Michael <mike.helpme.2026@gmail.com¹>

To: you@example.com

Grandma please read this its urgent

Grandma, it's Michael. I'm writing from a friend's account because my phone broke.² I got into a car accident out of state and I'm at the courthouse. Everyone is okay but I need \$900 for the fine today or it goes on my record.

Please don't tell Mom and Dad — I'm so embarrassed and I'll pay you back Friday, I promise.³

The clerk said the fastest way is Apple gift cards from Walgreens or CVS. Just buy three \$300 cards, scratch the back, and email me photos of the codes.⁴

Please hurry, they only gave me until 4pm. I love you.

- 1 A stranger's address wearing a family name.** Anyone can type "Michael" into a free email account. The story about the broken phone exists to explain why the address isn't his.
- 2 A reason you can't reach him the normal way.** Every version of this scam blocks the obvious move — calling him. That is exactly the move to make: call the number you've always had for him, or call his parents.
- 3 Secrecy.** "Don't tell Mom and Dad" is not embarrassment — it's the scammer removing the people who would recognize the fraud in seconds. No legitimate emergency requires keeping family in the dark.
- 4 Gift cards as payment.** No court, hospital, or government agency in the United States accepts gift cards. The moment anyone asks for gift card codes — for any reason — the conversation is a scam, full stop.

The same scam now arrives by phone — in your grandchild's own voice

A few seconds of audio from a social media video is enough for AI tools to imitate a family member's voice on a phone call. The FBI attributes \$352 million in 2025 losses among Americans 60+ to AI-assisted scams like these.

The defense costs nothing: agree on a family code word. Pick a phrase only your real family knows. Any urgent call or message asking for money gets one response — "what's our word?" — followed by hanging up and calling the person back on the number you've always used. A cloned voice can't answer, and a real grandchild won't mind.

EXHIBIT C**The government that emails threats****TRAINING EXAMPLE — THIS IS A FAKE EMAIL, ANNOTATED**

From: Medicare Benefits Division <no-reply@medicare-gov-secure.us.com¹>

To: you@example.com

Suspension of benefits — verification required within 24 hours²

Dear Beneficiary,

Due to irregular activity, your Medicare coverage has been temporarily suspended. Failure to verify your identity within 24 hours will result in termination of benefits and referral to collections².

To restore coverage, review the attached form and reply with your Medicare number, Social Security number, and date of birth³:



Medicare_Verification_Form_2026.pdf.zip⁴

U.S. Medicare Benefits Division · Ref # MC-2026-88431

- 1 A costume version of a .gov address.** Real federal email ends in .gov — nothing after it. "medicare-gov-secure.us.com" is a .com wearing a government costume. Apply the archivist's eye: the jurisdiction is wrong for the record.
- 2 Threats on a timer.** Medicare and Social Security do not suspend benefits by email, and they do not give 24-hour ultimatums. Real agencies send letters — and they never threaten "collections" for verification.
- 3 A request for identifiers no agency asks for by email.** The government already has your Social Security number. Anyone asking you to send it is collecting it.
- 4 A disguised attachment.** The file says "PDF" but actually ends in ".zip" — a container that can hold a program. Never open attachments in unexpected mail; the double file extension is a classic disguise.

EXHIBIT D The package that can't be delivered — the text-message version

TRAINING EXAMPLE — THIS IS A FAKE TEXT MESSAGE, ANNOTATED

Text message from: +63 917 555 0182 ¹

ParcelPoint: Your package could not be delivered due to an incomplete address. A redelivery fee of \$1.25 is required ². Schedule redelivery within 12 hours or the item returns to sender:

<https://parcelpoint-redeliver.info/track8834> ³

Reply STOP to opt out

- 1 A delivery company texting from a foreign personal number.** Real carriers send from short 5- or 6-digit codes, and the U.S. Postal Service will not text you a link about a fee at all unless you signed up for tracking on a specific package. A full-length overseas number is the provenance failure in text form.
- 2 A tiny fee for a package you don't remember.** \$1.25 is deliberately trivial — cheap enough to pay without thinking. The card number you type on that page is the actual target, and "incomplete address" is a story that fits every household, because everyone is vaguely expecting something.
- 3 A made-up tracking domain.** The genuine carrier's site is the one printed on their trucks. When a package matters to you, go to the carrier's real website yourself and type the tracking number from your order confirmation — never the link in an unexpected text.

The same skeleton, different costumes: "your toll is unpaid," "your streaming account is on hold," "your bank card is locked" — all small-dollar texts with a link and a clock. The response to every one of them is identical: delete it, and check the account through the app or website you already use.

EXHIBIT E The prize that costs money to collect

TRAINING EXAMPLE — THIS IS A FAKE EMAIL, ANNOTATED

From: National Sweepstakes Bureau <claims.office.7741@aol.com¹>

To: you@example.com

CONGRATULATIONS — Your entry has WON \$2,500,000.00 (Claim ID: NSB-559-2026)

Dear Winner,

Your email address was selected in the North American Consumer Sweepstakes drawing of August 2026. You have won \$2,500,000.00 and a 2026 Mercedes-Benz.²

To release your winnings, a refundable processing and insurance fee of \$480³ must be received via Zelle or gift card before your claim expires.

This award is strictly confidential until funds are disbursed. Do not discuss your claim with your bank, as third-party interference voids the prize.⁴

Barrister Wm. Okafor, Claims Director · National Sweepstakes Bureau

- 1 A "bureau" with a free personal mailbox.** There is no National Sweepstakes Bureau, and no organization that gives away millions mails from an AOL address. Provenance first, always.
- 2 You won a contest you never entered.** Real sweepstakes require entry, and legitimate lotteries do not notify winners by mass email. If you can't remember buying the ticket, there is no ticket.
- 3 The fee is the entire scam.** This is the "advance-fee" con, older than email: any prize, grant, inheritance, or refund that requires you to send money first is fraud by definition. Real winnings have taxes *withheld*, never prepaid by gift card. Pay the \$480 and there will be a customs fee next, then a tax stamp — it ends only when you stop.
- 4 Sworn to secrecy — from your own bank.** The one institution that would recognize this instantly is the one you're told not to call. Any windfall that demands confidentiality from your family or your bank is protecting itself, not you. (The same letter arrives as an "unclaimed inheritance" from a distant relative — genealogists are targeted with that version by name, because your family tree is publicly posted.)

EXHIBIT F The friendship with an investment attached — a scam with no single tell

TRAINING EXAMPLE — A FAKE CONVERSATION, COMPRESSED FROM WEEKS TO ONE PAGE

Week 1 — A text arrives: "Hi Margaret, are we still on for lunch Thursday?" You reply that they have the wrong number. "Oh I'm so sorry! You seem kind though — I'm Lin, I just moved to Dallas."

1 A friendly correspondence begins. No money is mentioned.

Weeks 2–4 — Daily messages. Lin remembers your dog's name, asks about your grandchildren, sends photos of meals. Mentions in passing that an uncle helps her invest in "digital currency" and it paid for her condo. **2** Still no ask.

Week 5 — You mention it's interesting. Lin offers to show you, walks you through installing a trading app, and suggests starting with just \$500 "to learn." **3**

Week 7 — Your app shows the \$500 has grown to \$1,940. You're even allowed to withdraw \$200, which arrives in your bank the next day. **4** Lin suggests you're ready for a real position.

Week 9 — You've moved \$40,000 in. The app shows \$71,000. When you try to withdraw, a "tax clearance fee" of \$7,100 is required first. **5** Lin encourages you to pay it. The app, the balance, the uncle, and Lin do not exist.

- 1 The "wrong number" that stays friendly is the opening move.** Thousands of these texts go out daily; whoever answers kindly becomes the mark. There is no Lin — often it's a scripted team working many victims at once.
- 2 The investment enters as a background detail, never a pitch.** This scam — investigators call it "pig butchering" — is built on patience. Weeks of genuine-feeling friendship exist to disable exactly the skepticism you'd apply to a stranger.
- 3 The app came from them.** A trading platform recommended by someone you have never met in person, installed from a link they sent, is their stage set. Every number it shows is typed in by the scammers.
- 4 The small withdrawal that works is bait, not proof.** Letting you take out \$200 is the cheapest \$200 the scammers ever spend — it converts doubters into people who move their retirement savings.
- 5 The exit fee reveals the con.** Real brokerages deduct fees from your balance; only scams demand new money to release old money. This is the advance-fee skeleton from Exhibit E, at catastrophic scale — it is now the single largest source of reported elder-fraud losses.

The one-line defense: never invest through an app, platform, or "opportunity" introduced by someone you have only ever met through a screen — however long you've talked, and however real the friendship feels. Romance versions of this scam run the identical script with affection in place of friendship.

EXHIBIT G**The rescue that robs you twice****TRAINING EXAMPLE — THIS IS A FAKE EMAIL, ANNOTATED**

From: Fraud Recovery Division <agent.k.morrison@recovery-taskforce.org¹>

To: you@example.com

RE: Your fraud case — funds located and frozen

Dear Ms. Hartley,

Our task force has been investigating the scam operation that took your funds earlier this year.

² We are pleased to inform you that \$38,200 of your money has been located and frozen in an offshore account.

To release the funds to your bank, we require a court filing fee of \$1,900³ refundable upon disbursement. We also need your bank's routing number, your account number, and a copy of your driver's license to verify ownership.

For your protection, do not discuss this recovery with your bank or family until funds are released, as the suspects may have informants.⁴

Agent K. Morrison · International Fraud Recovery Task Force

- ¹ **An agency you never contacted, on a domain you've never heard of.** Real investigators — the FBI, your state attorney general — do not email out of the blue from invented "task forces," and no government body charges victims to return their own money.
- ² **They know you were scammed because they scammed you.** Victim lists are resold among criminals, and the original crew often returns wearing a rescuer's costume. Being contacted about "your case" unprompted is the tell, not a comfort.
- ³ **The fee, again.** Same skeleton as Exhibits E and F: money now to release money later. Add the bank details and license, and this one harvests your identity too.
- ⁴ **Secrecy from the very people who could stop it.** By now you know this move. It appears in the grandchild scam, the sweepstakes, and here — because family and banks are where scams die.

If you have been scammed once, expect this email. It is not a possibility, it is the standard second act. The only real recovery channels are your own bank's fraud department and reports filed at ic3.gov — both free.

The genealogical proof standard, applied to email

Three questions before you click anything

- 1 **Provenance — who really sent this?** Read the full address after the @, not the display name. If they don't match, the record is forged.
- 2 **Independent verification — can I confirm this from an original source?** Never use a link or phone number inside the message. Go to the website you already know, the number on the back of your card, or the person's real phone.
- 3 **The pressure test — is someone rushing me or swearing me to secrecy?** Deadlines measured in hours, threats, and "don't tell anyone" are the signature of fraud. Legitimate organizations survive you sleeping on it.

If you already clicked or replied

Act quickly and without embarrassment — this happens to sharp, careful people every day, which is precisely why it's a \$7.7 billion problem. Call your bank or card company first if money or card numbers are involved; change the affected password (and anywhere it's reused); and report it at **ic3.gov**, the FBI's fraud-reporting site. Telling family the same day is the single strongest protective step — these scams die in daylight.

Genealogists spend years learning that the comfortable story and the true story are often different documents. Bring that skepticism to your inbox, and you are already better defended than most.

About this article: prepared by Family Sentinel — a Texas-based service that monitors your email for indications of compromise and malicious or destructive messages, and provides comprehensive safety checks and live support for internet and email security concerns. Learn more at **FamilySentinel.org**. The example messages shown are fictional training composites; the companies, senders, and domains do not exist.

Reprint permission: clubs, churches, libraries, and community groups are welcome to photocopy and distribute this guide unmodified, free of charge.