Stay Safer Online:

A quick guide for writers and speakers: use AI to investigate scams, protect your digital identity, and recognize today's most common traps.

by Edie Melson

AI can be a useful second set of eyes, but it is not a lie detector. The goal is simple: slow down, investigate, and independently verify before you click, pay, share, or panic.

5 Red Flags to Stop and Investigate

1. Urgency - pressure to act immediately.
2. Fear - threats involving your account, money, reputation, or someone you love.
3. Secrecy - instructions not to tell anyone else.
4. Odd requests - unusual payments, verification codes, remote access, or moving the conversation elsewhere.
5. Suspicious links - links that may not lead where they appear to lead.

5 Simple AI Prompts

1. Analyze this message for signs of a scam.
2. What red flags do you see in this email or direct message?
3. What is this sender actually asking me to do?
4. What questions should I ask before responding?
5. How can I independently verify whether this is legitimate?

Never paste passwords, Social Security numbers, banking or credit-card information, one-time authentication codes, medical records, or sensitive business information into an AI tool.

Edie's 3-Question Rule

1. Does this make emotional sense - or is it trying to make me panic?
2. Can AI identify warning signs?
3. Can I independently verify it through a trusted source?

If a message claims there is a problem with an account, don't use the link in the message. Open the official app or type the legitimate website into a new browser window yourself.

Stay Safer Online:

A quick guide for writers and speakers: use AI to investigate scams, protect your digital identity, and recognize today's most common traps.

by Edie Melson

Online Security Habits

Small routines can protect the reputation, platform, contacts, and opportunities you've spent years building.

Make These Part of Your Routine

- Check your email spam folder every day.
- Search for yourself on each social platform at least once a month.
- Look for misspellings of your name, copied photos and bios, extra characters, and duplicate accounts.
- Enable two-factor authentication on every important account.
- Use a unique password for every account and consider a password manager.
- Search your name, website, and book titles periodically.
- Close old accounts you no longer use.
- Verify unexpected links or attachments with the sender another way before opening them.

Common Scams Targeting Writers & Speakers

- Fake literary agents or editors who contact you unexpectedly, then refer you to a paid service.
- Fake publishers or Big Five acquisition offers, often promising unusually large advances.
- Book marketing, publicity, visibility, review, or bestseller-package scams.
- Fake book clubs that invite you to participate and later demand a fee.
- Fake podcast, radio, or interview invitations that eventually require payment.
- Fake book festival, conference, or featured-speaker invitations.
- Impersonation of well-known authors, agents, editors, publishers, producers, or organizations.
- Film/TV adaptation or production-company scams claiming interest in your book.
- Fake copyright-violation or social-media suspension notices.
- Cloned social-media accounts pretending to be you or someone you know.
- Phishing emails disguised as account verification, password resets, invoices, or security warnings.
- Fake Amazon, bookstore, customer-support, or publishing-service contacts.
- Unexpected requests for gift cards, wire transfers, payment apps, or other hard-to-reverse payments.

A polished, personalized message is NOT proof that an offer is legitimate. AI now allows scammers to mention your book, summarize its themes, imitate professional language, and make the message feel personally researched.

Stay Safer Online:

A quick guide for writers and speakers: use AI to investigate scams, protect your digital identity, and recognize today's most common traps.

by Edie Melson

Before You Say YES to an Opportunity

- Search the person's name and organization independently.
- Check the sender's full email address - not just the display name.
- Visit the organization's official website yourself.
- Contact the real organization using contact information you found independently.
- Ask why money is required and whether that fee is normal for this type of opportunity.• Do not let praise, urgency, fear, or excitement rush your decision.
- When in doubt, ask a trusted colleague - and investigate before responding.

Before You Click, Pay, Share, OR Panic:
STOP. ASK. VERIFY.

EEdie Melson is an author, speaker, and photographer. Her blog, The Write Conversation, reaches thousands and has been on the Writer's Digest Top 101 Sites for Writers since 2017. Her passion is to help others define their God-sized calling follow that path. She's the executive director of the Blue Ridge Mountains Christian Writers Conference and board member of the Advanced Writers and Speakers Association. Find her at EdieMelson.com