DIGITAL NAVIGATION SERVICES

Staying Safe Online in the Age of AI

Take-Home Reference Guide

Scams are not new — but artificial intelligence has given scammers powerful new tools: flawless writing, cloned voices, and convincing fake photos and videos. The good news is that the habits that protect you are simple and don't change. Keep this guide handy as a reminder.

Part One: Everyday Security Basics

1. Use a Password/Passkey Manager

- Reusing the same password everywhere means one leaked site can unlock all your accounts.
- A password manager creates and remembers long, unique passwords for every site — you only remember one master password.
- Apple Passwords (iPhone/Mac) and Google Password Manager (Android/Chrome) are free and already built into your device — no new app to install.
- Bitwarden (free) and 1Password (paid, ~$3-5/month) are independent options that also manage passkeys, the newer, safer login method.

Try This:

- If you mostly use one brand of device, start with the manager already built in.
- If you use a mix of devices, or want more control, try Bitwarden — it's free and works everywhere.
- Whenever a site offers “set up a passkey,” your manager can create and store it for you.
- Never store passwords in a notebook by the computer or reuse one password everywhere.

---

2. Turn On Two-Factor Authentication (or a Passkey)

- 2FA asks for a second proof it's really you — usually a code sent to your phone.
- Even if a scammer steals your password, they're stopped without that second code.
- A text-message code is good; a free authenticator app (like Google Authenticator) is even better.
- Best of all: a passkey. It replaces the password entirely with your device's fingerprint, face, or screen lock — it can't be phished, guessed, or reused on a fake site.

Try This:

- Turn on 2FA for email and banking first — they protect everything else.
- When a site offers “set up a passkey” or “sign in without a password,” take it — it's the safer, easier option going forward.
- Ask a family member or library staff to help you set up the first one together.

3. Spot Phishing Emails & Texts

"Your account has been suspended. Click here within 24 hours to verify your identity or lose access permanently."

- Phishing uses urgency and fear to make you click or reply before you think.
- Watch for mismatched sender addresses, generic greetings, and links that don't match the real company.
- Legitimate companies never ask for your password or one-time code by email or text.

Protect Yourself:

- Don't click links in unexpected messages — go to the company's site yourself.
- When unsure, call the company using the number on your card or statement.

---

4. Caller ID & Email Spoofing: When “You” Isn't You

"A call shows your bank's real phone number on caller ID. An email arrives that appears to come from your own email address. Neither one is actually them."

- “Spoofing” means faking the caller ID name/number or the email “From” field so it displays whatever the scammer chooses — including a real bank's number or your own address.
- Phone and email systems weren't built to verify who's really sending, so that information can be typed in and shown however the scammer wants.
- A common trick: an email claims “I hacked your account, this is proof I'm emailing from it” — it's just a faked sender field, not real access.

Protect Yourself:

- Caller ID and the “From” name aren't proof of identity — treat both like an unknown contact.
- Hang up or don't reply, then contact them using a number you already have on file.
- If “your own” email looks suspicious, it's spoofed, not hacked — change your password just in case.

5. Blackmail (“Sextortion”) Emails

- These emails claim the sender has hacked your device or webcam and collected private photos, videos, or files.
- They demand payment — almost always in Bitcoin — within a tight deadline, threatening to release everything or lock you out of your accounts.
- This is a mass-mailed scam, not a personal threat. These emails almost never involve real access to your device. Sometimes an old, breached password is included as a scare tactic.

Protect Yourself:

- There is no real proof — just a threat and a payment demand. Never pay, reply, or engage.
- Delete the email and, if it worries you, change the password it mentions (on every site where you reused it).
- If you feel distressed by one of these, please know it is a bluff sent to thousands of people, not something to be embarrassed about.

---

6. Scam Pop-Ups (Browser, App & Social Media)

- A pop-up claims your device is “locked” or “disabled” due to illegal activity, sometimes paired with a fake “payment sent” notification, and tells you to call a support number immediately.
- Browsers and phones cannot lock themselves from a webpage — this is a fake screen designed to look like a system alert.
- These show up in web browsers, apps, and social media (including Facebook and Instagram) — anywhere an ad can be shown. They're usually triggered by a shady ad network, not a virus.

Protect Yourself:

- Never call the number or tap anything in the pop-up — not even “Cancel.”
- Fully close the browser or app (on a phone, swipe it away in recent apps, don't just tap back).
- If it won't go away, restart your device — that clears it completely.

---

7. Keep Your Software Updated

- Updates aren't just new features — most contain fixes for security holes scammers actively exploit.
- Set your devices to update automatically so you don't have to remember.

Try This:

- Turn on automatic updates in your phone and computer settings.
- Only download updates from the official App Store, Google Play, or the software itself.

Part Two: New AI-Age Scams

1. More Scams, More Targeted, Less Skill Required

- Cloning a voice or faking a video used to take real technical skill and money. AI apps now do it for anyone, in minutes, often for free.
- That means far more people can run scams — a single scammer can launch thousands of personalized attempts at once, at almost no cost.
- AI can also personalize each attempt using details scraped from social media and public records, so messages feel eerily specific instead of generic.

What This Means for You:

- Expect more scam attempts overall, and expect them to feel more convincing and personal than a few years ago.
- The good news: the core habits in this guide — pause, verify, don't trust caller ID or a familiar voice alone — work no matter how good the fake gets.

---

2. Voice Cloning: "It Sounded Just Like Them"

> *"A call from your "grandchild," upset and asking you to wire money right now — using their real voice, cloned from a video online."*

- AI can clone a voice convincingly from just a few seconds of audio, often taken from social media.
- Scammers pair the voice with urgency and secrecy: "Don't tell anyone, I'm embarrassed."
- The voice sounding right is no longer proof of who's calling.

Protect Yourself:

- Set up a family "safe word" only real family members would know.
- Hang up and call that person back on their known number. Any request for money or gift cards is a major red flag.

---

3. Deepfake Photos & Videos

> *"A video of a celebrity or public official "endorsing" an investment — that they never actually made."*

- AI-generated images and videos are now realistic enough to fool a casual glance.
- Deepfakes are used in fake investment ads, romance scams, and impersonation of officials.

Protect Yourself:

- Be skeptical of surprising videos, especially involving money or urgency.
- Verify big claims through a second, trusted source before acting.

4. Deepfakes, Politics & Social Media

"A viral video shows a political figure saying something shocking — but it was never actually said. It was AI-generated and shared thousands of times before anyone fact-checked it."

- Political deepfakes aren't hypothetical — fabricated videos, robocalls, and doctored clips have already appeared in real elections here and abroad.
- These are used by many different groups, across the political spectrum, to mislead, provoke outrage, or influence opinion — not just for financial scams.
- The most emotional, most-shared posts are exactly the ones worth double-checking, since virality often outpaces fact-checking.

Before You Share, Verify:

- Check whether mainstream news outlets are reporting the same story, not just the original post.
- Look at the account posting it: brand new, few followers, only outrage content? Red flag.
- A reverse image or video search can often reveal where a clip really came from.
- Ask an AI assistant to help fact-check a claim — great practice using AI, but treat its answer as a first check, not the final word (AI can be fooled too).

5. AI-Written Scam Messages

"A perfectly written email from "Medicare," with no typos and correct logos, asking you to confirm your Social Security number."

- The old advice — "look for bad grammar" — no longer works. AI writes fluent, error-free messages.
- Judge messages by what they're asking for, not how well they're written.

Protect Yourself:

- Ask: would this organization really request this by email or text?
- Real agencies like Medicare and the IRS won't ask for personal info this way. Contact them using a number you look up yourself.

6. Fake AI Chatbots & Websites

"A "customer support" chat window pops up on a site claiming to be your bank, asking you to type in your login and card details."

- AI chatbots can be built quickly to impersonate real banks, Medicare, Social Security, or tech support.
- Fake sites can look nearly identical to the real ones, down to logos and layout.
- When available, the company's official app is often safer than a website — it can't be typo-squatted or spoofed by a fake link the way a web address can.

Protect Yourself:

- Type the company's website address yourself instead of clicking a link.
- Prefer the official app when you have it — download it only from the Apple App Store or Google Play, and check the publisher name.
- Never enter passwords or account numbers into a pop-up chat window.

Part Three: Habits That Protect You

1. Verify Before You Trust

- Scammers create urgency on purpose — it stops you from thinking clearly.
- A short pause to verify costs you nothing. Acting on a fake request can cost everything.

The Golden Rule:

- Hang up. Look up the real number yourself. Call back.
- It's always okay to say, "Let me call you back," and take your time.

---

2. Think Before You Share

- Details you post — pet names, birthdays, vacations, family names — help scammers sound convincing.
- AI can quickly scan public posts to build a personalized, believable scam script.

Try This:

- Set social media profiles to "friends only" where possible.
- Avoid posting answers to common security questions (pet's name, school, etc.).

If You Think You've Been Scammed

Acting fast can limit the damage. Don't be embarrassed — call these people right away.

1	**Call Your Bank or Card Company**	Report it immediately and ask about freezing accounts or reversing charges.
2	**Change Passwords**	Start with email and banking. Use a device you know is safe.
3	**Freeze Your Credit**	Equifax: 1-888-298-0045 • Experian: 1-888-397-3742 • TransUnion: 1-888-909-8872 — it's free and reversible.
4	**Report It**	File a report at reportfraud.ftc.gov and consider a local police report.

Your Pause-and-Verify Checklist

Keep this page by your phone or computer.

- ☐ Slow down. Real emergencies rarely require an instant decision.
- ☐ Hang up and call back on a number you already have — never one given to you.
- ☐ Verify through a second channel before you trust a voice, text, or video.
- ☐ Never share passwords, one-time codes, or gift card numbers with anyone who contacts you.
- ☐ When in doubt, ask a trusted friend, family member, or the library before you act.

Helpful Resources

- Report fraud: reportfraud.ftc.gov
- AARP Fraud Watch Network Helpline: 1-877-908-3360
- FBI Internet Crime Complaint Center: ic3.gov
- Credit freezes: Equifax, Experian, and TransUnion (search each company's official site)