



Before-You-Click Safety Checklist



J. Hutchinson, CISSP, CISSP-ISSMP

Pause before you act.

Scammers rely on panic and urgency. If you receive a call, text, or email claiming there's an emergency, pause before responding. Contact the person or organization using a phone number you know is legitimate.

Set a family code word. Pick a simple phrase only your family knows. If the caller is not able to recite the phrase, it is a bogus call.

Do not pay. Ever. Paying rarely ends the threats and almost always invites more demands. No legitimate agency asks for gift cards or wire transfers. Most threats are bluffs, and even real material rarely surfaces.

Never share personal info on inbound calls. Medicare and insurers won't call asking for your Social Security number, Medicare ID, or banking details. If you're worried, hang up and call the agency directly using the number on their official website. Never provide your Social Security, Medicare, banking passwords, or one-time security codes to someone who contacts you unexpectedly. Only share the number with trusted doctors, pharmacists, and insurers. Government agencies, banks, Medicare, Social Security, and reputable businesses won't threaten arrest, demand immediate payment, or insist that you keep the conversation secret.

Don't Trust a Familiar Voice Alone AI can clone the voice of a child, grandchild, spouse, or friend. Even if the voice sounds exactly like someone you know, verify the situation by calling them directly or another trusted family member.

Never call numbers from pop-ups. Pop-up warnings urging you to call a support number are almost always scams. Close the browser instead. Find support phone numbers and chat links directly on the company's official website, not from search ads.

Tighten up social media. Make accounts private and limit who sees your photos. Even a short video gives scammers enough audio to clone a voice. Check for duplicate profiles. Report the fake account to the platform and warn your friends. It protects everyone in your circle.

Be wary of "free" offers. Free braces, genetic tests, or COVID kits in exchange for your Medicare number are common scam hooks. Check Medicare Summary Notices and insurance Explanations of Benefits for services you never received. If it promises guaranteed returns or rewards, it's likely a scam.

Don't Click Unknown Links or Attachments Emails and text messages can look convincing, especially when created with AI. If you weren't expecting the message, don't click the link. Visit the company's website directly or call them using an official number.

Save the evidence before blocking. Screenshot the messages, usernames, payment requests, and email headers. You'll need them for reports.