

Beyond the Basics: Spotting Next-Gen Scams

Safety Minute Briefing

IOWA | Iowa Utilities Commission

The Evolution of the Threat

Generative AI and automated tools have eliminated classic scam indicators like poor spelling and robotic voices.

AI Voice Cloning (Vishing)

The 3-Second Rule: Modern AI tools require only 3 seconds of recorded audio (from social media, webinars, or voicemail greetings) to clone a voice with 85%+ match accuracy.

Emotional Exploitation: Scammers simulate emergencies (arrests, car accidents, urgent wire transfers – even utility disconnection) to trigger panic and override logical analysis.

The Indistinguishable Threshold: Human listeners can no longer reliably distinguish cloned voices from authentic family members or co-workers.



Quishing & Thread Hijacking

Quishing (QR Code Scams)

- How it works: Attackers send PDF attachments or emails containing QR codes instead of text links.
- Why it works: Security filters inspect readable text links. Images/QR codes bypass traditional scanner filters and force you to use an unmonitored mobile phone.

Thread Hijacking

- How it works: Attackers compromise a legitimate email user's inbox and reply directly inside an existing, trusted email thread.
- Why it works: Because the prior conversation history is genuine, victims lower their guard and readily open malicious attachments.

The Caller ID Fallacy

Caller ID Cannot Be Trusted: 40% STIR/SHAKEN Authentication Rate

VoIP technology allows attackers to display ANY caller ID number they choose — including your local bank branch, IT helpdesk, or even family members.

While authentication frameworks like STIR/SHAKEN attempt to verify caller legitimacy, adoption remains incomplete across telecom networks globally.

Golden Rule: Seeing a familiar contact name or logo on your ringing screen proves nothing.

Unconventional Defenses You Can Use

Family/Team “Safe Word”
Establish a secret, offline verbal word or phrase with family or key coworkers. If anyone calls claiming an emergency or requesting financial action, demand the safe word.

Callback Rule
If an unexpected caller claims to be from your bank, boss, or tech support, immediately hang up. Call back using a known, independently sourced phone number.

The 15-Minute Pause
Enforce a mandatory 15-minute cooling-off period on any urgent request. Time pressure is the attacker's main tool; a deliberate pause restores logical critical thinking.

Safety Minute Action Plan

Today's Personal Action: Establish an emergency safe word with your immediate family or household.





