

SAFETY TIPS FROM IOWA SENIOR MEDICARE PATROL (SMP):

BE AWARE OF SPOOFING SCAMS



Spam calls are no longer just about trying to sell you something. Sophisticated scammers can pretend to be from banks, tax offices, courier companies and more by “spoofing” phone numbers.

What is a spoofed call??

When a caller deliberately fakes a local or familiar number on caller ID to hide their true identity.

HOW TO SPOT A SPOOF...

Caller claims to be from a government agency demanding immediate action.

Caller requests personal details like passwords or banking information.

Caller threatens account suspension or legal action.

...TIPS TO STAY SAFE.

If anything sounds suspicious, hang up & call the official number directly.

Never call back a suspicious number or click on any links sent by text afterward.

If you have been impacted by Medicare fraud, errors or abuse:
Call Iowa Senior Medicare Patrol (SMP) at: 1-800-351-4664
or visit: <https://shiip.iowa.gov/fraud>



PROTECT



DETECT



REPORT

How Can I Stop Spam Calls?!

Setting up “Call Screening” on your cell phone

What is call screening?

Call screening is a built-in tool for your phone to **automatically**: Identify callers, screen or silence unknown numbers, block spam & fraud calls, answer calls on your behalf using AI, provide a realtime transcript so you can decide whether to pick up.

HOW TO SCREEN CALLS...

IPHONE

1. Open settings
2. Select “apps”
3. Select “Phone”
4. Scroll down to “Screen Unknown Callers”
5. Toggle on your choice: “Never, Ask Reason for Calling, or Silence

Android

1. Open the Phone app
2. Tap the three-dot menu in the top right corner
3. Select “Settings”
4. Tap “Call Screening” (or Bixby text call)
5. Toggle the switch to “ON”

GOOGLE

1. Open the Phone app
2. Tap the three-dot menu in the top right corner
3. Select “Settings”
4. Tap Call Screen
5. Turn on “Automatically Screen Calls”
6. Choose your protection: Max, Medium or Basic

Make sure to also...

- **Avoid sharing your number publicly.** Many spam lists originate from websites, contest forms, or online accounts that expose your phone number. Avoid posting your number on social media, forums or classifieds
- **Be cautious with “free” wi-fi networks** or apps requesting unnecessary phone permissions
- **Use alternate numbers** (like Google voice) for online signups
- **Remove data sharing** from apps that don’t need phone access.