

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to spot a Social Security scam

<https://cyberguardlab.com/blog/social-security-scam>

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.



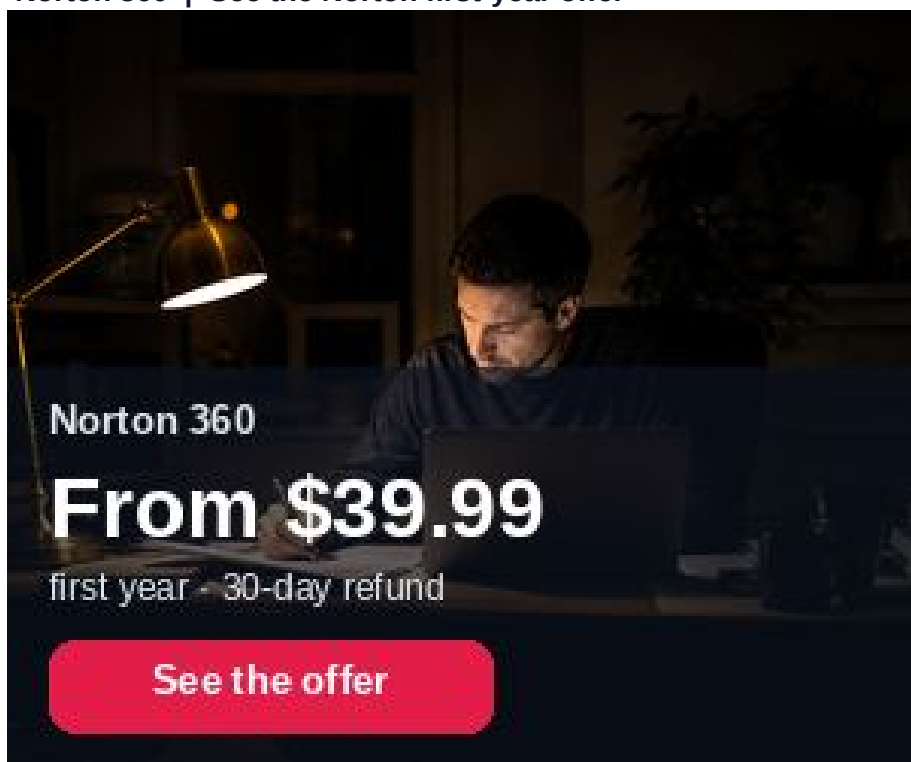
A Social Security scam is when someone pretends to be from the Social Security Administration (SSA), the SSA Office of the Inspector General, or another government office and pressures you about your Social Security number (SSN), benefits, or "crimes" tied to your number. Per FTC government-impersonation guidance and SSA OIG alerts, real SSA will not threaten you, suspend your SSN, or demand gift cards, wire transfers, cryptocurrency, or payment-app sends. This guide is about SSA / government SSN impersonation, not fake IRS tax refund calls, gift card payment traps, or generic phishing email how-tos. You do not need to buy antivirus to hang up and call SSA yourself.

1. How SSA impersonation usually works

From FTC and SSA OIG consumer alerts:

Paid link

Norton 360 | See the Norton first-year offer



Norton 360

From \$39.99

first year - 30-day refund

[See the offer](#)

[See the Norton first-year offer](#)

Offer page: <https://cyberguardlab.com/norton> Hop: <https://trysecurities.com/offer/norton?dtm=gg&cid=>

- * Scary claim - Caller says your SSN was used in a crime, your benefits will stop, or your number will be "suspended" or "seized."
- * Spoofed caller ID - The screen may show a real-looking SSA or government number. Caller ID can be faked.
- * Urgency to pay or "protect" money - They demand gift cards, wire, crypto, payment apps, cash, or even gold-sometimes with a courier coming to pick it up.
- * Fake verification - They ask for your SSN, bank details, or one-time codes "to confirm your identity."
- * Follow-up scripts - Emails, texts, or voicemails repeat the same threat so you act before you can think.

2. What real SSA will not do

FTC and SSA OIG are clear:

- * Real SSA will not threaten you with arrest, lawsuits, or benefit cutoff over the phone to force instant payment.
- * Real SSA will not suspend your Social Security number as a scare tactic.
- * Real SSA will not demand gift cards, wires, crypto, payment apps, cash, or gold for any agency problem.
- * Real SSA will not send someone to your door to collect cash or precious metals.
- * A call that says "someone is using your SSN to commit crimes-pay now" is a scam - FTC has specifically warned about that script.

3. What to do when the call, text, or email hits

- * Hang up / ignore the link - Do not argue, do not share codes, do not buy gift cards.
- * Call SSA yourself - Use a number from ssa.gov or your own paperwork-not the number the caller gave you.
- * Never pay irreversible methods - Gift cards, wire, crypto, and payment-app "protection" sends are scam payment tools.
- * If someone is coming to pick up cash or gold, call the police - That is an active crime script, not an SSA visit.
- * Warn family - Especially older relatives who get emergency money or tech support pressure calls.

4. If you already shared info or paid

- * Contact your bank, card issuer, or payment provider right away.
- * Report the scam at ReportFraud.ftc.gov.
- * Report SSA impersonation to the SSA Office of the Inspector General.
- * If your SSN or other personal info was exposed, start a recovery plan at IdentityTheft.gov.
- * Change passwords on email and financial accounts and turn on stronger sign-in where you can.

FAQ

How do I spot a Social Security scam?

Threats to suspend your SSN, claims that your number was used in a crime, pressure to pay now with gift cards / wire / crypto / payment apps, or a courier for cash/gold are classic red flags. Real SSA does not do those things.

Caller ID showed Social Security-can it still be fake?

Yes. FTC: caller ID can be spoofed. Hang up and call SSA using an official number you look up yourself.

Is this the same as an IRS refund scam?

Related pressure style, different agency script. For tax-refund impersonation, see fake IRS tax refund scam. This page stays on SSA / SSN threats.

Do I need paid antivirus to stop this?

No. This is impersonation and payment pressure. Defender is optional later only if you also clicked a shady attachment on a PC - see Is Microsoft Defender enough?.

Where do I report it?

ReportFraud.ftc.gov and SSA OIG. For identity theft steps: IdentityTheft.gov. Also see how to report a scam to the FTC.

If you still want a paid suite

Stopping an SSA impersonation call does not require paid antivirus. Microsoft Defender is a valid buy-nothing choice for many Windows households. What actually helps is hanging up, calling SSA yourself, and refusing irreversible payments. If the household later wants multi-device paid protection, use only these on-site paid links: TotalAV ([paid link](#)), Norton ([paid link](#)), Bitdefender ([paid link](#)), McAfee ([paid link](#)), Avast ([paid link](#)).

Sources

- * How to Avoid a Government Impersonation Scam (FTC)
- * No One Is Using Your Social Security Number to Commit Crimes - It's a Scam (FTC)
- * Report Fraud to SSA OIG
- * ReportFraud.ftc.gov (FTC)
- * IdentityTheft.gov

Also read

- * How to spot a fake IRS tax refund scam
- * How to spot a gift card scam
- * How to spot a tech support scam phone call
- * How to report a scam to the FTC
- * How to spot a grandparent emergency money scam
- * How to spot a phishing email