



AARP Fraud Watch Network Monthly State Scam Alerts October 2026

*Please consider publishing these alerts in your local publications, and share them on social media, too. If you have alerts to suggest, please send them to us and we will add them into our scam alert schedule. **If you would like to schedule a virtual/in-person scam prevention speaker for your group**, please complete our [online request form](#). Questions? Suggestions? Contact Jane Margesson jmargesson@aarp.org or 207-229-5628 (cell).*

Week 1 – Lock Down Your Data: Cybersecurity Awareness Month
--

LEARN MORE LINK

October is Cybersecurity Awareness Month, a good reminder that we can make it harder for criminals to steal our personal information or take over our accounts.

Scam messages often include a link or an attachment that perpetrators use to introduce malware onto your device or send you to a site that will seek to collect login or payment information.

Protect all online accounts with strong, unique passwords (strongly consider using a password manager) and turn on multifactor authentication when available. Also, keep your device software updated – the updates often include important security fixes.

Learn how to spot and avoid scams with AARP Fraud Watch Network™. Suspect a scam? Call our free helpline at 877-908-3360 and talk to one of our fraud specialists about what to do next.

Need a [scam prevention speaker](#) for your group? Click the link to fill out our online form or send an email to me@aarp.org.



AARP Fraud Watch Network Monthly State Scam Alerts

October 2026

Week 2 – Medicare Open Enrollment Scams	<u>LEARN MORE LINK</u>
--	--

Medicare's annual open enrollment period runs from October 15 through December 7.

As beneficiaries and new enrollees review their health and prescription drug coverage and options, criminals may pose as Medicare representatives or Medicare Advantage agents and try to steal Medicare numbers, financial or other personal information.

Know two things: unsolicited contact about Medicare is highly suspicious, and Medicare will never contact you out of the blue.

For helpful resources on enrollment and open season, check out [medicare.gov](https://www.medicare.gov), [aarp.org/medicare](https://www.aarp.org/medicare) or your State Health Insurance Assistance Program, a federally funded resource with trained counselors that can answer your questions in person, online or by phone. Search online for help at shiphelp.org/SHIPs or call 877-839-2675.

Learn how to spot and avoid scams with AARP Fraud Watch Network™. Suspect a scam? Call our free helpline at 877-908-3360 and talk to one of our fraud specialists about what to do next.

Need a [scam prevention speaker](#) for your group? Click the link to fill out our online form or send an email to me@aarp.org.



AARP Fraud Watch Network Monthly State Scam Alerts

October 2026

Week 3 – Fake Bank Alert: Don't Hand Over Your Code

[LEARN MORE LINK](#)

The AARP Fraud Watch Network™ Helpline (877-908-3360) is hearing from more people about bank impersonation scams. Consumers are targeted, usually through a call or text, by a criminal pretending to be from your bank.

They claim there's suspicious activity on your account, and you need to act immediately to protect your money. The warning can sound convincing because they are impersonating your actual bank and may have specific information about you and your account.

A major red flag is being told to transfer or withdraw money to keep it "safe." The bank impersonator may instruct you to wire funds, use a payment app, or withdraw cash and feed it into a designated cryptocurrency kiosk for "safekeeping."

The playbooks for this and other financial crimes are focused on a form of manipulation that serves to get past the logic center in our brains and go right to action through emotion. Any unexpected or unsolicited contact these days is a fraud risk. If you receive a concerning message from your bank, contact them using a phone number you know belongs to your bank, or check your account online or in the app if you have that access.

Learn how to spot and avoid scams with AARP Fraud Watch Network™. Suspect a scam? Call our free helpline at 877-908-3360 and talk to one of our fraud specialists about what to do next.

Need a [scam prevention speaker](#) for your group? Click the link to fill out our online form or send an email to me@aarp.org.



AARP Fraud Watch Network Monthly State Scam Alerts

October 2026

Week 4 – Spotting Social Media Scams

[LEARN MORE LINK](#)

Social media helps us stay connected, but criminals use the same platforms to find potential targets. A scam might arrive as a bargain-priced product, an investment opportunity, a new romantic interest, or a message that appears to come from someone you know.

Criminals create fake profiles, impersonate real people and businesses, or take over legitimate accounts. They can also use information people share publicly on social media to make their stories more convincing.

Use the platform privacy settings to limit who can see your posts and personal information. And use strong and unique passwords (strongly consider a password manager) and multifactor authentication where available.

Learn how to spot and avoid scams with AARP Fraud Watch Network™. Suspect a scam? Call our free helpline at 877-908-3360 and talk to one of our fraud specialists about what to do next.

Need a [scam prevention speaker](#) for your group? Click the link to fill out our online form or send an email to me@aarp.org.