BENJAMIN ROSE INSTITUTE ON AGING

EDUCATION CENTER

Resource Companion for the Psychology of Cybercrime

Website Resources

Fight Cyber Crime Website

Scam Survivor Healing

Advocacy Scripts

The following QR codes direct you to scripts to advocate for funding Adult Protective Services, the Long Term Care Ombudsman Program, the Elder Justice Reauthorization and Modernization Act, and the reauthorization of the Older Americans Act

FUND APS IN FY27

bit.ly/APS27

FUND LTCOP IN FY27

bit.ly/LTCOP27

Sponsor EJRMA 2026

https://bit.ly/EJRMA2026

Reauthorize Older Americans Act

https://bit.ly/EJC_OAA

Questions & Answers

Q: How do we refer people to the cybercrime support group?

A: Through our website! https://fightcybercrime.org/

Q: Isn't crypto a poor investment anyway even if legit for the most part?

A: That's a fair thought. Crypto is volatile and risky even in legitimate contexts, and many financial advisors would agree. But in this context what matters most is why fraudsters use it: transfers are irreversible, near-instant, and nearly impossible to trace. Once the money moves, it's gone. That's not incidental, it's the point.

And for the people you all might serve, many are being introduced to crypto for the first time by the fraudster themselves, they're being walked through setting up a wallet, shown which ATM to use, etc. The unfamiliarity is part of the vulnerability.

Q: How do you get to those sites that tell you if a photo is fake?

A: Aura and McAfee have programs that help detect deepfakes. There are other tools available as well, but we recommend doing your research to verify that the tool is legitimate.

Q: Do you have advice for people who refuse to acknowledge they are being scammed? It's definitely a romance scam but they are inclined to not accept it because they have met the mother and children, etc.

A: This can be a very difficult situation, as these scams are sophisticated. Leading with calling something a scam can trigger reactance, where the scammed person will defend themselves. The goal is to keep the door open and not to "win" the argument. Presenting hard evidence up front can often backfire, so it's best to meet the person being scammed where the doubt is already. For example, if there is a thread of canceled visits, you can ask "what do you think of that?" or other questions to spark curiosity. Those often land better than evidence, and encourage the person being scammed to reflect on the scammer's behavior.

It's also important to prepare for what happens if the scammed individual begins to accept they are being scammed. This is when grief hits, and it's important to meet the emotional weight of what they're losing—not just the financial piece.

Q: Are Google and other companies screening their advertisers in search to decrease fraud/scammers from posing as legitimate businesses?

A: They're trying, but it's not enough yet. Google blocked 5.1 billion harmful ads in 2024, suspended 39.2 million advertiser accounts, and permanently banned over 700,000 specifically for AI-driven impersonation scams. By 2025, identity verification became nearly mandatory where advertisers now have to provide company documents and a

responsible person's ID. But malvertising still surged 10% year-over-year, and campaigns routinely run for weeks before detection, partly because when Google suspends a compromised account, attackers simply activate another from their inventory. The practical takeaway for this audience: a sponsored result at the top of a Google search is not a guarantee of legitimacy. Many people still assume it is, and that assumption is being exploited.