

Adaptive Security Launches Free Training to Protect Older Adults From AI Scams

LOS ANGELES, March 19, 2026 /PRNewswire/ -- Adaptive Security, the leading provider of AI-powered social engineering prevention solutions, today launched free public training resources designed to help families protect older adults from AI-enabled scams, including voice cloning, deepfake videos and impersonation fraud.



The training teaches people how modern scams work and how to stop them before money or personal information is lost. It is available at no cost in 14 languages, including the official United Nations languages.

Americans age 60 and older lost an estimated \$81 billion to fraud last year, according to federal data. Security experts say artificial intelligence is rapidly increasing the scale and realism of scams targeting older adults.

The new course expands Adaptive's public safety initiatives. Earlier this year, the company partnered with Elliston Berry, a 2025 TIME100 honoree, on educational resources designed to help schools and families respond to deepfake abuse targeting children.

"AI has made scams faster, cheaper and far more convincing," said Brian Long, co-founder and CEO of Adaptive Security. "A scammer can now clone a voice from a few seconds of audio and impersonate a family member in distress. Education is one of the most effective tools we have to stop this."



The training includes real-world examples and guidance from cybersecurity and law enforcement experts, including Brady Finta, a former FBI agent and founder and CEO of the National Elder Fraud Coordination Center (NEFCC).

The course also features first hand stories from victims of AI-enabled fraud, including Gary Schildhorn, who narrowly avoided sending money after receiving a call that used his son's cloned voice. Additional cases in the training show how scammers use government impersonation, romance manipulation and other tactics to steal money and exploit trust.

"These scams are becoming more sophisticated and emotionally manipulative," Finta said. "They are designed to create urgency and fear so people act before verifying the situation. Teaching people how to pause and confirm what's happening can prevent significant financial loss."

Adaptive developed the training to help families recognize the warning signs of AI-driven social engineering and adopt simple verification practices. The course teaches participants how to identify common scam patterns, including manufactured emergencies, impersonation of trusted authorities and requests for untraceable payments such as gift cards, cryptocurrency or wire transfers. It also shows families how easy it is to create and share their own deepfakes, giving older adults a safe way to see how convincing these tools have become before criminals use them for fraud.

Practical prevention strategies include calling family members back on trusted phone numbers, creating family verification code words and avoiding financial decisions made under pressure.

Serving 800 global enterprise customers, Adaptive Security said the new training reflects growing public concern about AI scams affecting older adults and their families.

"Most people assume they would never fall for a scam," Long said. "The reality is these attacks are designed to exploit trust and emotion. The best defense is knowing what to look for and having a plan before it happens."

The free course is available at:
<https://www.adaptivesecurity.com/protecting-older-adults>

About Adaptive Security

Adaptive Security is the leading provider of AI-powered social engineering prevention solutions, specializing in protection against deepfake personas, AI-driven phishing and multi-channel social engineering threats. By combining advanced AI simulations, real-time risk assessment and security awareness training, Adaptive empowers organizations to proactively defend against emerging cyber threats.

For more information, visit www.adaptivesecurity.com

Media Contact:
Joshua Thompson
josh@adaptivesecurity.com