



You've spent a lifetime building your nest egg with diversification, tax efficiency, and careful planning. But in 2026, your financial fortress faces a new threat that doesn't need a battering ram because it can use your own voice.

It is time to build a moat to help protect you from generative AI, which has turned cybercrime from a technical challenge into a psychological one.

Generative AI is a form of artificial intelligence that creates new content, like text, images, audio, voices, or even computer code, from scratch. Unlike traditional AI, which analyzes or classifies data, generative AI can imagine and produce something entirely new. It doesn't just look at a photo and tell you it's a cat; it can draw a completely new cat that has never existed before.

This is a threat because generative AI has become so good that it can predict:

1. How your voice sounds.
2. How your bank writes its security emails.
3. How your face moves during a video call.

It has evolved from a tool that helps us work faster to one that can mimic reality with incredible precision.

This means that the days of spotting a scam by poor grammar or "Nigerian prince" tropes are over. Today's threats are sophisticated, polished, and very personal. Some strategies used are:

Deepfakes
*The Impersonation
Threat*

Using as little as 30 seconds of audio from a public video or voicemail, AI can now clone a person's voice with near-perfect accuracy. We are seeing a surge in emergency scams, where a loved one or trusted professional calls to request an urgent wire transfer to resolve a crisis.

**Hyper-
Personalized
Phishing**
The Custom Scam

AI bots now scrape social media and public records to craft emails that reference recent travel, a specific charity you support, or even the exact tone of your company's internal memos.

Vibe Hacking

The Slow-Play Con

This is the use of "emotionally intelligent" AI bots that build rapport over weeks, often through professional networking sites, only to eventually "recommend" a fraudulent investment platform.

How to Strengthen Your Digital Defenses

In the past, multi-factor authentication was the gold standard. While still essential, it is no longer invincible. AI-powered man-in-the-middle attacks can now create fake login portals that mirror your bank, intercepting security codes in real-time.

Furthermore, authorized push payment fraud is on the rise. Because AI is so good at social engineering, it convinces *you* to authorize the transfer. Once you hit "send" on a wire transfer, the money is often gone before the bank's fraud department even gets an alert.

The best defense against high-tech fraud is often surprisingly low-tech. Here is how to stay ahead:

01. The Family "Safe Word"

Establish a unique code word with your family and your inner circle. If you receive an urgent, out-of-character request for money, even if it sounds exactly like your child or spouse, ask for the code word.

02. The 2-Minute Rule

AI thrives on urgency. If someone calls demanding immediate action, hang up. Wait two minutes. Then, call the official number on the back of your credit card or our direct office line. Never use a callback number provided during the initial call.

03. Lean into Biometrics

Move away from SMS-based codes. Use hardware security keys or facial/fingerprint biometrics where available. These are significantly harder for AI models to spoof than a six-digit text code.

As your partner, we are here to be your last line of defense. While we embrace technology, we maintain a "human-in-the-loop" policy, verifying any unusual requests directly with you.

Technology is evolving quickly, but the value of a trusted relationship remains the ultimate encryption. If you have any questions, please don't hesitate to reply to this email so that we can help provide some safeguards for your financial fortress.



Dustin Metcalf, CRPC®
President & Founder

CA Office: (760) 491-1499
WA Office: (360) 865-7365
Dustin@fourcfinancial.com

Learn More >
ABOUT MY PRACTICE

Contact Me >
FOR A CONSULTATION

Four C Financial | www.FourCfinancial.com | 73000 Highway 111, Suite 202, Palm Desert, CA 92260

Investment advice offered through Integrated Partners, doing business as FourC Financial, a registered investment advisor.

The opinions voiced in this material are for general information only and are not intended to provide specific advice or recommendations for any individual.

The information contained in this e-mail message is being transmitted to and is intended for the use of only the individual(s) to whom it is addressed. If the reader of this message is not the intended recipient, you are hereby advised that any dissemination, distribution or copying of this message is strictly prohibited. If you have received this message in error, please immediately delete.

[Unsubscribe](#) [Manage preferences](#)