

Trust, Once Verified

For the most part, I'm a person who rolls with the punches, although some things *do* bother me more than others. Two of the things that make my blood boil: people who intentionally take advantage of hard-working people, and people who take something intended for good and turn it into a weapon against others. Fraudsters manage to do both.

Fraud is the intentional use of deception to gain something of value for yourself while someone else suffers the loss. Fraud certainly didn't begin with email, the internet, or Artificial Intelligence. People have been deceiving other people for thousands of years. Technology has simply given fraudsters faster, cheaper, and more convincing ways to reach us.

My wife and I approach people very differently. She can spot a scam a mile away. Her natural posture is, "I'll trust you when you've shown me you're trustworthy." I tend to start from, "I trust you until you give me a reason not to."

I wish I were more like her. While neither approach is necessarily wrong, where you fall on that continuum matters. If, like me, you give away trust easily, you have to work twice as hard to protect yourself and your family.

And there are plenty of opportunities to get fooled. In 2025, consumers filed about 3 million fraud reports with the Federal Trade Commission and reported \$15.9 billion in losses according to the AARP. The FBI separately received more than one million internet-crime complaints representing nearly \$21 billion in reported losses. In Kentucky alone, reported internet-crime losses approached \$120 million.

Those are only the reported incidents. Imagine how many suspicious calls, texts, emails, letters, and encounters never get reported at all.

A familiar scenario starts with urgency: "Your bank account has been compromised. Click here immediately." Another might be a call supposedly from a government agency, your boss, or even a family member who desperately needs money. Today, technology can spoof phone numbers, imitate legitimate websites, and even mimic voices. The tooling may be more modern, but the strategy is centuries old: *get you emotional enough that you act before you think*.

So slow down. Think critically before acting. Don't trust until verified.

In other words, if you don't recognize a number, let it go to voicemail. Don't know the sender of an email? Don't respond. Weren't expecting the message? Don't click the link. Research the organization independently, call a number you already know to be legitimate, or ask someone you trust what they think.

For businesses, add another rule: independently verify unusual requests to change payment instructions, transfer money, or provide sensitive information. A second set of eyes can prevent an expensive mistake.

And remember the advice our parents gave us long before anyone had heard of phishing and other email-based scams: “if something seems too good to be true, it probably is.”

Fraud isn’t going away anytime soon. Where there is an opportunity for honest people to prosper, fraud follows close on the heels of it. Technology advances quickly; human nature doesn't. Trust people once you’ve verified their intentions, and give yourself enough time to verify.

Robbie Wilson

President, Regional Technology Council

www.regionaltechcouncil.org