Article #93 - Ten Commandments to avoid AI scams
By Bro. Hal Bookbinder (hal.bookbinder@ucla.edu)

Thou shalt not

ו Succumb to pressure to act now.
ז Share personal data when contacted.
ח Pursue unsolicited opportunities.
ט Download unverified AI utilities.
י Try to outsmart AI.

Thou shalt

א Keep up with the news.
ב Limit sharing in social media.
ג Remain aware, remain vigilant.
ד Independently verify before acting.
ה Trust your gut.

While I believe that Artificial Intelligence (AI) will provide amazing advances in science, medicine, analytics, and productivity, and prove a boon for humankind, it will also be disruptive. Significant effort will be required to limit its potential for harm. While the Government is now scrambling to catch up, reviewing the Federal Register shows numerous studies on the benefits and challenges of AI.

My May article, Artificial Intelligence, discussed the use of AI to make the existing grandparent scam more believable and more dangerous. I also noted that with AI, some of the easy clues in scam emails and texts, will become a thing of the past. While we do not yet fully know how AI may be used to perpetuate scams, some of the ways can be readily imagined.

There is a vast amount of personal information that is available on the Internet, including entries in public and semi-private databases. Using this data, AI will be able to better guess the passwords we use (few of us use truly random ones) and to personalize scams. It will be able to fashion communication that is so knowledgeable about each of us that we are more likely to believe in its legitimacy.

By scanning the Internet, including our postings on Facebook, LinkedIn, and Twitter, AI may learn that we are avid genealogists, are in job search mode, have suffered a loss, are ready to invest, are preparing to retire, or are on vacation in Europe. While scams today find and use this information, it can be costly and time consuming. AI can gather, analyze, organize, and use such information on an industrial scale.

AI might reach out to us as a distant relative trying to connect or a genealogical database offering new finds. It might offer an opportunity that is exactly what interests us right now. It could seemingly come from our specific bank, brokerage, grocery, utility, or doctor. It might even include specific knowledge about our accounts or medical history, and even ask about our spouse or children by name.

AI may be able to contact us in a way that shows knowledge that could only be coming from a relative or friend. Contact may be by email, text, or phone. Similarly, it might assume your identity and attempt to scam family and friends. You might first learn of this when someone reaches out to you asking how you could recommend this worthless stock to them, or otherwise set them up.

Folks have been fooled into downloading free, or low-cost, AI tools, only to be infected with a virus or sustain a ransom attack. Be sure to regularly scan your system for viruses. Trust that cyber criminals will keep pushing the envelope and coming up with new AI-driven scams. While there will likely be controls put in place, in the end, you need to primarily rely on yourself to avoid being scammed.

Bro. Hal Bookbinder is a retired Information Technology Director and College Instructor. Prior article in this series can be accessed at https://tinyurl.com/SafeComputingArticles.