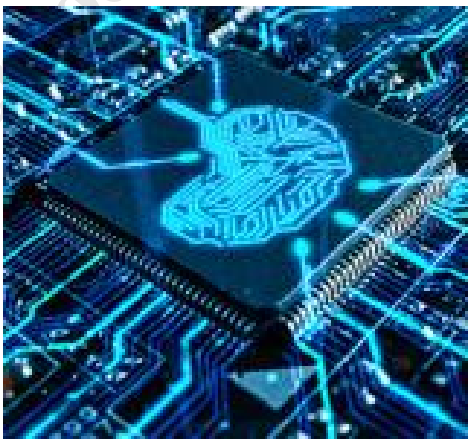
www.pipelinepub.com
Volume 21, Issue 1

Preventing Social Engineering Attacks

By: Mark Cummings, Ph.D



Social engineering attacks are a very serious problem that GenAI is turbocharging. Existing solutions focusing on training and procedures are helpful but insufficient. Organizations need automated social engineering defensive tools. Existing large vendors lack the technology, expertise and economic incentives to provide these fully adequate solutions. The best way to get them is for large organizations to partner with innovators, thereby speeding up the process of bringing these solutions online.

What Is Social Engineering?

Social engineering attacks involve manipulation to get innocent people to do nefarious things on behalf of attackers. To affect their manipulation, attackers employ some form of deception to make the innocent people convinced that they are doing something that is “good” and “right,” or at least good for them personally.

While social engineering cybersecurity attacks have been problem for some time, the advent of GenAI has made the problem much greater. Several years ago, executing a successful social engineering attack took some skill and, in many cases, sophisticated technical knowledge. But now, with GenAI, that is no longer true. Not only does GenAI remove the skill and knowledge barrier, it also makes Deep Fake attacks possible. The result is that 98 percent of cyberattacks have an element of social engineering.

Pre-GenAI Example

Social engineering is used to gain unauthorized access to credentials that give attackers access to applications and cyber infrastructure that can be used to cause damage, extort funds, steal intellectual property, gain access to information that allows attacks on large numbers of organizations and individuals, etc.

An example of such a social engineering attack that used a simple telephone is the attack on the MGM Grand Hotel and Casino in Las Vegas. Staff at a technical support help desk got a phone call. The caller said that he was the most senior system administrator in the company. He said that he was traveling and had lost his phone with all his user IDs and passwords. He said his phone was locked, so he wasn't worried about information getting out. But there was a very serious situation. He needed to do a system update right away. To do that he needed a new set of credentials. He was able to convince the help desk staff member to give him that new set of credentials. With that new set of credentials, the bad actor loaded a ransomware attack.

The resulting ransomware attack had dramatic effects that damaged the company, its customers, and its brand. For example, the key cards no longer opened room doors. Guests were left without access to their belongings and the front desk couldn't check people in or out. The casino floor had to shut down. It took a week and cost the company $109 million to get its systems back up and running, all in addition to the brand damage and consequential loss of revenue it suffered.

GenAI Examples

AI has given bad actors a new set of tools to create more powerful ways of deceiving people. It removes the skill barriers. Now a six-year-old can launch a social engineering attack. It removes human physical barriers. Don't have a good voice? GenAI can give you a good one. It can be used to identify promising targets and to gather the information needed to make the attack. Maybe the most significant capability is the Deep Fake one. GenAI can actually generate voices, images, sounds, and video that make the attacks very effective.

A recent attack we call the GenAI CFO illustrates the deep fake capability. A Hong Kong-based finance department staff member of a multinational corporation got a message purporting to come from the CFO in the U.K. talking about a secret financial transaction. Although he was suspicious, he was nevertheless maneuvered into a video call with what appeared the CFO and several employees of the corporation he recognized confirming the need for the transaction. The staff member effected a $25.6 million transaction based on what he saw and heard in the call. Unfortunately, the "people" he recognized in the video call were actually Deep Fakes created by GenAI. The corporation lost millions as a result of this GenAI-enabled social engineering fraud.

There is also evidence of GenAI using social engineering for itself to gain credentials and/or access to cyber infrastructure and/or applications. In one recorded case, an AI system was able to manipulate a person into performing a CAPTCHA for the AI system by pretending to be a visually impaired person seeking help. Current experience indicates that in such attacks the AI system is seeking access to another system it does not have authorized access to. This may be for: totally hallucinated reasons; for a misguided implementation of instructions it received in its creation, development, training, maintenance, use; or other reasons we don't understand.

AI systems are now providing bad actors with fake image IDs for social engineering attacks. Images of IDs, such as driver's licenses and passports, are often used in online transactions. Bad actors can use

the fake IDs for cybercrimes, such as: fraud, privacy invasion, abuse and harassment of individuals, and more. For example, ID images taken with a computer camera are used in online notarization services and KYC (Know Your Customer) transactions. One example of KYC online transactions involves the sale of dangerous biologic substances. Researchers concerned about the use of AI systems to create bioweapons recommend use of KYC techniques by those selling RNA and DNA materials.

With advanced 3D printing it may be possible to create physical versions of these images, thus creating counterfeit physical IDs. IDs that can be used in execution of physical criminal activities.

Current Defenses Are Not Enough

The current solution offered by major vendors to stem the social engineering threat is focused on training and procedures. But while training is clearly helpful in defending against cyberattacks it is not by itself enough. Moreover, most of the cyber defense tools offered by major vendors in the market today rely on finding attack signatures (patterns in data previously found to be associated with particular types of cyberattacks). Some of the newer technology solutions have tried other ways of finding patterns of attacks. Unfortunately, by the time these patterns have been identified in transaction data, indicating that a social engineering attack has taken place or is underway, it is already too late. The attack has already been successful.

So, what can a large organization do to protect itself?

Large cybersecurity tool vendors are economically successful with their products based on currently well understood technologies and competencies. Extending these existing competencies will not provide what is needed to protect against social engineering. Moreover, these vendors lack a motivating incentive to develop and try something completely new.

The most likely place that a solution to social engineering will emerge from is a new innovative technology entrant. The best way that large organizations can speed up the process that produces this kind of innovation is to partner with emerging vendors bringing innovative technology. In other words, large organizations need to work with innovators to develop and implement effective social engineering defenses.

Conclusion

Social engineering attacks are a very serious problem that GenAI is turbocharging. Existing solutions focusing on training are helpful but insufficient. Existing large vendors lack the technology, expertise, and economic incentives to provide fully adequate solutions. Organizations need automated social engineering defensive tools that are not currently available. The best way to get them is for large organizations to partner with innovators, speeding up the process of bringing these solutions online.