

Social Engineering

Blurring reality and fake: A guide for the insurance professional



www.cybcube.com



Deception and disguise are criminal methods that are as old as time.

Numerous examples - from Ulysses and his Trojan Horse in Greek Mythology, to Fagan, the pickpocket, in Charles Dicken's Oliver Twist - reinforce the long history of criminals achieving their goals by hoodwinking targets into believing that an interaction is something that it is not.

Today, that deception is largely being carried out in the non-physical realm. Recent huge strides made in technology take historic social engineering techniques to new levels in terms of both scale and sophistication.

In this paper, we will outline some of the forms of social engineering and explore some of the criminal motivations for carrying out these attacks. We will take a deeper dive into four developing areas of social engineering, which we believe should be on

the radar of insurance professionals, as they become more widely used.

Cyber insurance products do - and will continue to - cover claims from social engineering attacks. This paper is designed to educate insurers on developing strains of social engineering, so they can engage with their clients meaningfully on their cybersecurity and risk management strategies against these new attacks.

CyberCube invests heavily in cybersecurity expertise - both human capital with deep experience in the cyber security domain and also in data sources and security signals that might flag vulnerabilities and risk areas.

This paper combines those resources, to offer some pointers on what warning signs enterprises should be alert to, and how insurers could address this growing trend before it becomes a major claims event.

Definitions

In the broadest context, social engineering is a defined domain within social sciences that focuses on efforts to influence particular attitudes and social behaviours. In recent years, there has been recognition that social engineering plays a huge part in the execution of cyber security attacks. Specifically, social engineering in a technical context can be defined as the act of exploiting human weaknesses to gain access to personal information and protected systems and it relies on manipulating individuals rather than hacking computer systems to penetrate a target's account.¹



¹ [https://en.wikipedia.org/wiki/Social_engineering_\(security\)](https://en.wikipedia.org/wiki/Social_engineering_(security))

Social engineering - getting easier

The stages of a cyber attack that involve researching the target and manipulating their perception and behavior (referred to as “luring”) are becoming increasingly easy to conduct. Just in the past year, we have witnessed the COVID-19 pandemic leveraged during the luring phases of attacks involving people invited to click on links or open files in order to find out more information about the virus only to discover that this action allows for a criminal to stage a ransomware attack or steal some personal credentials.

Increasingly, workers today are hyper-connected, data-rich and often blur the lines between their public and private information. A person working from home, for example, most likely uses many of the same technical resources (e.g. laptop, network infrastructure, telephone) for their private conversations as they do for the public ones. This same IT infrastructure will also be utilised for both personal and business purposes. Electronic communication such as email and, in particular, social media platforms further prepare the ground for sophisticated social engineering by cyber criminals.

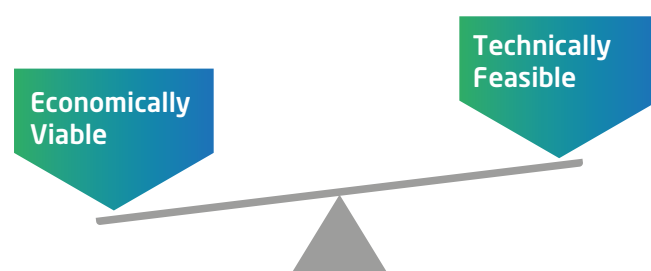
Even prior to the COVID-19 pandemic, people were physically meeting less and the tools that replace these physical interactions were becoming more ubiquitous. In turn, these very same tools started to become

almost perfect vectors for social engineering attacks. More and more of our data has to be online today in order for service providers, governments and others to make use of it and provide us with service. People have created digital avatars of themselves (for the purposes of engaging with social welfare or interacting with the banks online, for example) and these digital identities are proving to be just as valuable as physical human targets have been for centuries.

Importantly, the definition of a trusted relationship has also changed significantly in recent years. Historically, a criminal leveraging social engineering techniques would have had to imitate a close relation or colleague in the physical world. Now, the spoofing of an email address or the creation of a fake social media account may be sufficient.

As the availability of personal information increases, so criminals are investing in technology to exploit this trend. A balance has to be struck between the economic viability and its technical feasibility (see below).

Finding the “economic vs technological sweet-spot”



Where a sweet spot emerges (i.e. a solution becomes both technically feasible and economically attractive), we will often see aggressive adoption in the emerging technique which, in turn, leads to major and influential trends in behavior.










“ ”

digital identities are proving to be just as valuable as physical human targets have been for centuries

Attack methods: today

Traditionally, social engineering techniques have been categorised as either physical or non-physical (often termed "Technical" where computer systems are used as the basis for attack). Physical manifestations of social engineering involve a physical act on the part of the criminal that grants access or steals information. Non-physical social engineering involves use of authority, playing on emotions such as greed,

curiosity and anger as well as the use of impersonation. The intersection of "non-physical" and "technical" social engineering (sometimes referred to as "socio-technical") is where criminals are mostly focused today. Using computer systems to engage in psychological trickery has already proved to be fruitful for today's cyber criminal and innovation in this area should be expected to continue.

Social engineering style	Attack type	Typical vectors
Physical social engineering 	Dumpster diving Tail-gating 	Trashcans, open access to property, office reception areas 
Technical social engineering 	Password hacking Online profiling 	Malware, unsecured networks & systems, social media 
"Socio-Technical" engineering 	Phishing Watering holes 	Email, compromised websites 

Where are criminals investing?

To predict what the future holds for social engineering techniques in the world of cybersecurity, CyberCube conducted research to understand the current and predicted behaviours of cyber criminals and analysed trends. This research leveraged both data that the company collects in order to model insurance risk as well as insights collected via the dark web as part of our adversarial threat intelligence efforts.

Use of phishing techniques are now well-established in cyber crime (these having attained the “sweet spot” some time ago). These social engineering techniques will continue to develop in terms of maturity and

sophistication in the coming years. There are new, emerging techniques, that we believe will fundamentally change the cyber threat landscape and that are becoming rapidly both technically feasible and economically viable.

Here, we focus on three major innovations that could be impactful within the next 2-4 years.

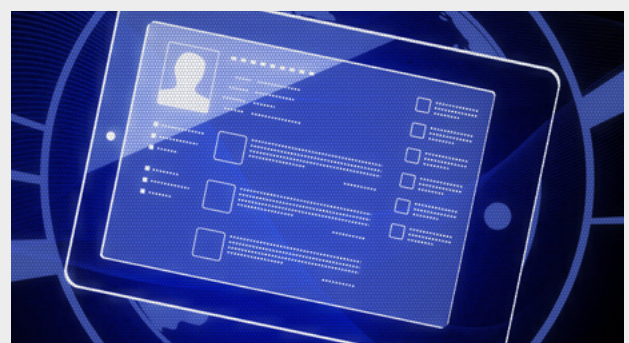
- Social profiling at scale
- Deep Voice mimicry
- Deep Fake video mimicry (with special mention of “Mouth Mapping” technology)

Advanced social profiling at scale

Social profiling is the process of constructing a target’s character profile using their social data. It has long been the staple of the research phase of socially engineered attacks. Historically, targeted social data has mainly existed in the physical realm, perhaps in physical bank records that can be retrieved through dumpster diving or through stolen medical files.

Today, social profiling is largely carried out online (reflecting the transfer of personal information to digital media) and involves the application of certain data science processes to generate a target’s profile using technology. The digitisation of personally identifiable

information (PII) has created a huge opportunity for criminals to profile their targets online. This would be enough of a problem if it were limited to hacks of medical databases, banking networks and so on but the problem and potential impacts grow exponentially given the popularity of social media platforms such as Facebook and LinkedIn.



Active social media users are a gift to social engineers, especially when combined with official records such as driving licenses, passports, medical records and banking information. Consider the following statement, taken from an actual social media account in the real world (and anonymized here):



Tweet

@XBank I urgently need to generate a bank statement from work, can you help?"



Post

"I hate my job, I hate my job, I hate my job"

Statements such as these reward the cybercriminal with the ability to "get personal" with a target quickly and to approach that target with certain contexts that make interaction seem natural. A person asking their bank for help, as seen in the first example, is the perfect target for a reverse-social engineering attack (where a bogus entity – in this case, a bank - is set up to contact and interact with the target). A person online complaining about

their job could be targeted by a bogus recruitment consultant who could extract personal information as a trusted party, over time.

To use the banking example here and build out an example scenario, imagine a criminal gang looking for posts like this and then setting up a bogus entity that did a good job of pretending to be the target's bank. They would contact the target (reverse social engineering), convince that target that they are legitimate, respond to the target's initial query (thus, building trust and rapport) and extract credentials, possibly during the course of several interactions. The attack would likely end with the target's bank account being emptied or, worse, their credentials being used to extort large amounts of money via loans or mortgages.

Until recently, social engineers have worked case by case to build targeted social profiles (see example below). These are generated through analysis of structured information, social media posts, pictures, notice of social interactions such as holidays and birthdays and many other data.

Building a targeted social profile

	Personality traits	Interest	Wants	Vulnerabilities
Self image	Confident Expressive Determined	Fitness Exploration Growth	Recognition Advancement Administration	Failure Idleness Triviality
Social life	Experienced Wide social circle	Travel Other well being	Influence Valued opinion	Projections Low impact Ignored
Professional life	Consultant Instructor	Position of influence	Leadership Management	

Build rapport

Triggers

Good social profiles provide an ability to build effective rapport with a target and to trigger that target into certain actions that assist the criminal in their endeavour.

Criminal investment in the area now focuses on the application of Artificial Intelligence (AI) and automation, allowing the activity described above to be parallelised, with millions of social profiles being built on demand and with the ability to tailor this activity to the specific needs of the criminal.

The injection of vast scale into socially engineered attacks will have a couple of effects. Firstly, the cybercriminals will be able to take advantage of a law of averages to ensure return of investment for the attack. The more people are targeted, the more likely the criminal is to see a return. Secondly, we will start to see large accumulations of loss since the attacks now systematically target hundreds or even thousands of businesses, in parallel. This is a dynamic that should be of great interest and concern to the insurance industry.

Fake voice

Computer-generated, voice synthesized speech has been utilised since the 1970's and human-like computerized speech has grown steadily more convincing and viable over the past few decades. More elusive, however, has been the ability to mimic specific (targeted) voices with a computer system. Creating a convincing voice, capable of complex dialogue that is indistinguishable from the original human target, is a challenge.

Once again, AI, ML and, in particular, neural networks (computer networks that are built using a similar structure to the human brain) are proving to be game-changers in this field. These technological approaches alongside the ever-growing capacity and performance of computer systems are now being leveraged to make the mimicking of specific voices possible. What previously seemed impossible from a technical perspective is now made possible through the ability of a computer system to learn through iteration and leverage new kinds of processing resources and system architectures.

Furthermore, we are starting to see a "technically feasible/economically viable" balance that is enabling cost effective, off the shelf solutions to solve this problem for both criminals and for legitimate use-cases.

The majority of investment being made in this area by criminals is evident in two main areas, the first is "voice conversion". This technique involves the sampling of two voices (a "source" and a "target") and the application of specialist software to convert one to another. The second technique is "text to voice" which allows a mimicked, synthesized voice to be instructed to "say" whatever the user of the software submits via a text interface.

Both of these techniques are applicable in both legitimate and in criminal contexts. Voice conversion could be used, for example, to provide anonymity to an individual in certain online contexts. It could also be used by criminals to mimic the voice of a loved one and fool a target into giving up confidential

information. Text to voice technology is already being used by podcasters and professional educators to create and edit voice-over material. In a criminal context, it has been seen in the wild “editing” recordings of influential targets to manipulate their audiences and public opinion.

In March 2019, criminals used AI-based software to impersonate a chief executive’s voice and demand a fraudulent transfer of €220,000 (\$243,000) in what cybercrime experts described as an unusual case of AI being used in hacking.

The mimicking of a specific voice is resource intensive with the most advanced systems needs around 15 minutes of raw material and several hours of computer processing time to create realistic and believable

voices. This makes many applications of this technology unviable in the context of our technical feasible/economically viable balance. Given the focus and investments that are being applied to this domain, however, we would expect to see full viability of “fake voice” occur in the next two years. At that point, cyber attacks such as vishing (attacks carried out through bogus and malicious phone calls) will become a major source of concern for both businesses and individuals alike. Within a three-to-five year period, we would expect that full voice conversion and text to voice will be fully commoditized services, available on your mobile phone and creating mimicked voices almost instantaneously. This will have serious economic and political ramifications in the context of cyber crime.

Deep fake

The creation of video that realistically simulates an individual’s physical characteristics and speech have become known as deep fakes. Deep fakes (or fake video identities) leverage AI and Machine Learning (ML) to create “photo-realistic” simulations of certain individuals interacting with a video camera.

This technology has been steadily growing in sophistication for several years but use of deep fake in the identity theft domain has yet to materialise as a major source of concern. It is interesting to reflect, however, on the potential impact of this technology since COVID-19 and increased use of video conferencing services. Many security researchers are

now predicting that deep fakes could become a major security threat in the 2021-2022 period.

Once again, we are likely to see both legitimate and illegal use of this technology in the coming years. Early adopters here are likely to appear in various parts of the entertainment industry. Legitimate entertainment applications such as “faceswap” are demonstrations of early commercialised applications that are helping to generate revenue with the technology and drive down the cost of application in the field. Criminal use of deep fake technology is yet to materialise fully but targets could be political figures (particularly those who

have large online presence) and business leaders (imagine the effect that a “fake Elon Musk” giving insider trading tips might have on the investor community, for example).

As with all use-cases involving AI and ML technology, the key to good results is good data that the system can use to achieve its objectives. Raw data, in the case of deep fakes comes in the form of video, pictures and audio samples of a targeted individual. When it comes to media celebrities, politicians and business leaders, there is no shortage of media available to feed the deep fake engines. According to Business Insider, people took 1.2 trillion digital pictures and videos in 2017.² A large percentage of these found their way onto the Internet for public consumption via social media and smartphones had a major part to play in this trend. Assuming more recent years have seen even further growth in these numbers, source data is rarely a problem for the deep faker.

Given the trends in deep fake technology as they relate to the technical feasible/economically viable balance, we predict that deep fake and related technologies will extend initially from video (mainly for entertainment purposes) and will be a major contributor to digital identity theft.

In the 2021-2024 timeframe, deep fake video will likely infiltrate domains such as politics. Politicians are on camera frequently, often in stationary positions. This creates an opportunity for politically-motivated groups to spread false messages, manipulate audiences and damage reputation through the use of this technology.



Mouth mapping

A particularly interesting area of innovation is in the technology of “mouth mapping”, invented by students and the faculty at the University of Washington, Seattle.³ Here, targets can be made to say anything in very realistic simulations that even the trained eye would find hard to distinguish from reality.

This technology is likely to lead to viral political videos that instill fear, uncertainty and crime. It is also applicable to social media and web conferencing (particularly relevant in a post-pandemic era). Mouth mapping is

interesting because it complements existing deep fake and fake voice technologies and is particularly well suited to political and journalist targets (ie. talking heads sitting in a fixed position and talking to camera).



² <https://www.businessinsider.com/12-trillion-photos-to-be-taken-in-2017-thanks-to-smartphones>

³ http://grail.cs.washington.edu/projects/AudioToObama/siggraph17_obama.pdf

Conclusion

Insurers and cyber defenders should track progress in the area closely and ensure that the risk management frameworks, security strategies, analytics tools and catastrophe models take this emerging threat into consideration.

How can the insurance industry address these trends? What can insurance professionals do to

- Engage with their clients on mitigation measures
- Select only those clients that have good risk management in place
- Consider the potential for new social engineering techniques to be deployed at scale, causing aggregation events

Risk management activities

While the cyber security industry is developing defensive tools, these are costly and it is difficult to keep pace with criminal applications. As an example, organizations are already working on AI technology that is designed to spot deep fake video.

Technology can play its part in mitigating cyber risks but to holistically defend against this threat, it is important for companies to consider People, Processes and Technology. Companies are increasingly training their employees to identify and detect social engineering attacks, and build processes for alerting such incidents and escalating them before others fall victim.

Risk selection

As always, carriers and underwriters should try to take a balanced approach when identifying and selecting the right risks. There is no silver bullet of questioning that will translate into zero losses, however, underwriters should still try to understand how a given risk stacks up to information security frameworks. Taking NIST for example, understanding how companies, Identify, Protect, Detect, Respond and Recover will provide a more holistic view of the risk.

Users of this framework would want to understand how well the company has identified their assets that could be compromised by a social engineering attack (information, data, records, funds, etc.) and what people, process and technology controls are in place to protect these assets (again largely a human control, although technology can help). They would also look at how to detect an attack with employees being well trained, as well as other mechanical processes and thresholds in place (data loss prevention, processes for payment remittance, etc.). It is also important to examine how to respond to

“ ”

There is no silver bullet of questioning that will translate into zero losses, however, underwriters should still try to understand how a given risk stacks up

the event once it has happened (escalation procedures, response plans and so forth to minimize the damage) and how well the organization can recover from the incident (data replication, reputational messaging, etc.).

Of course, given that a well-executed attack may bypass all of this, the other area for risk carriers to consider is how to limit their exposure to the event, either by sublimitting coverage for such an attack, or not offering it at all for certain industry types or absent some of the aforementioned controls. Additionally, underwriters need to adequately charge for this cover to balance out the loss potential, not only on an individual risk basis, but for a portfolio of risk affording the coverage.

Large loss potential

The insurance market will need to consider advances in social engineering when developing attack scenarios. For example, deep fake technology could destabilize political systems (perhaps on a global basis) as communications constructed from the technology become indistinguishable from the real thing. This same technology could impact the financial markets and the reputation of large corporations.

Technology can play its part in mitigating cyber risks but to understand the nature of the threat, it is important to understand the actors behind it. Multi-disciplinary experts across data science, cyber security, software engineering, actuarial modeling, the military and commercial insurance will increasingly play their part in helping to understand the psychology and motivations behind social engineering approaches.

Author

Darren Thomson, Head of Cyber Security Strategy, CyberCube

Editorial Management

Yvette Essen, Head of Content and Communications, CyberCube

Rebecca Bole, Head of Industry Engagement, CyberCube

This document is for general information purpose only and is correct as at the date of publication. The product described in this document is distributed under separate licences with CyberCube which restricts its use, reproduction, distribution, decompilation and reverse engineering. Whilst all reasonable care has been taken in the preparation of this document including in ensuring the accuracy of its content, this document is provided on an "as is" basis and no liability is accepted by CyberCube and its affiliates for any loss or damage suffered as a result of reliance on any statement or opinion, or for any error or omission, or deficiency contained in the document. This document is subject to change from time to time and it is your responsibility for ensuring that you use the most updated version. This document and the information contained herein are CyberCube's confidential and proprietary information and may not be reproduced without CyberCube's prior written consent. Nothing herein shall be construed as conferring on you by implication or otherwise any licence or right to use CyberCube's intellectual property.

All CyberCube's rights are reserved. 2020 CyberCube Analytics Inc.

United States

CyberCube Analytics
58 Maiden Lane
3rd Floor
San Francisco CA94108
Email: info@cybcube.com

United Kingdom

CyberCube Analytics
51 Eastcheap
1st floor
London EC3M 1JP

Estonia

CyberCube Analytics
Metro Plaza
Viru Väljak 2
3rd floor
10111 Tallinn



CyberCube

www.cybcube.com