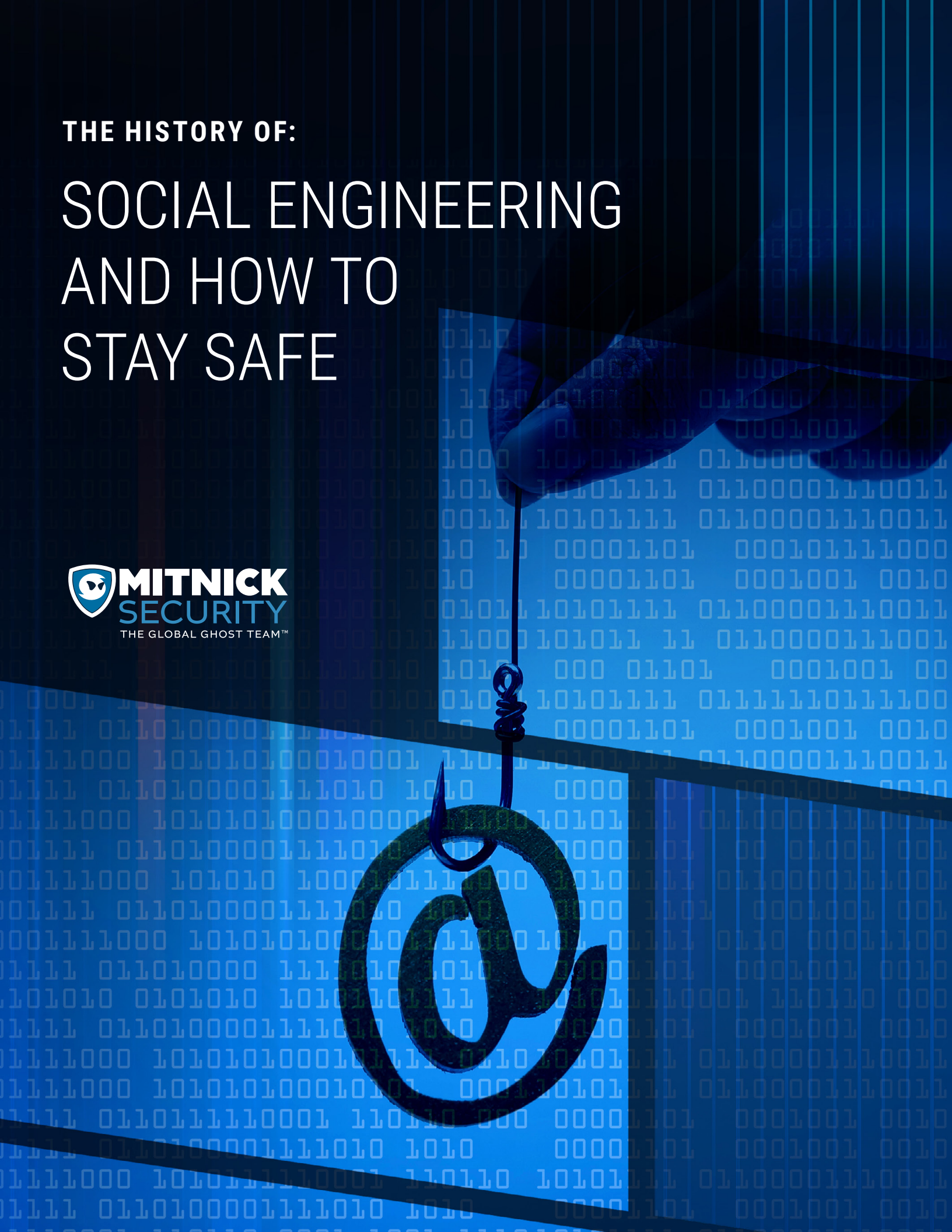
THE HISTORY OF:

SOCIAL ENGINEERING AND HOW TO STAY SAFE



MITNICK SECURITY
THE GLOBAL GHOST TEAM™

Contents

Social engineering is a concept that's been around for millennia. But it's a practice that's evolved and developed dramatically over time— especially since it's received a formal name and increased digital notoriety in the last two decades.

This comprehensive guide will cover how social engineering originated and transformed throughout its lifespan.

1 What is Social Engineering?

Have you ever received a suspicious email from what appears to be your boss asking you to complete an urgent task? What about a voice memo telling you your car warranty is about to expire, and you need to renew it— right now— before it's too late?

Both are prime examples of social engineering, wherein a threat actor attempts to manipulate or deceive a user. The threat actor's goal is often to convince the target to disclose private information or procure money— or to perform an action that could, in turn, give the hacker access to said info or funds.

Most social engineers are after any and everything they can get their hands on— knowing that the more leverage they have, the more they gain.

How Does Social Engineering Work?

The key purpose of social engineering is to gain access to private information or money quickly. A social engineer could slowly peck away at digital reinforcements and search for weaknesses to hack a company if they wanted to. However, it's often easier to trick a person on the inside than it is to crack air-tight cybersecurity measures. Once in, the hacker knows how to acquire the goods; they just need to find an initial foothold.

The Art of Deception

Instead of imploring brute force to attack cybersecurity barriers, social engineers are masters of the art of deception.

These cunning engineers use the principles of human psychology to build trust with a user— often someone directly associated with their targeted organization— knowing that the person may be their "in."

It all starts with selecting a brand and choosing human target(s). From there, a social engineer typically creates a believable pretext— a false story used to acquire money or information to breach a system— specific to the victims he's after.

What makes social engineering different from a typical con or fraud is that these attacks usually involve a series of highly calculated steps— methodically planned to slowly reach an end goal— using principles of human psychology to manipulate the target.

A Brief Example of Social Engineering

A social engineer typically begins by scouring the Internet for open source intelligence (OSINT), digging through public information to select specific users to manipulate. Let's say the social engineer begins by searching LinkedIn for everyone who works for a particular organization. For example, we'll call the company Tea Castle, an online retailer of loose-leaf tea.

On LinkedIn, the engineer can see each employee's job title, who they work under, how long they've been an employee, the accounts they manage, etc. From there, the engineer may silo down by department, choosing, for example, to target marketing personnel instead of the tech-savvy IT team. The engineer then looks up the social media profiles of the marketing team individuals, discovering core knowledge of their lifestyles and personal info.

He sees that the VP of Marketing posted a public picture showing her working remotely on Instagram, saying she's thrilled to work from her favorite cafe and enjoy a local tea. The social engineer notes this, wondering what remote security vulnerabilities he may be able to exploit, knowing she'll likely have high-permissions access in the organization. He jots down that she uses a MacBook, the exact shop she's working from, and the possible location of where she lives based on her proximity to the cafe. He keeps scrolling and notices she likes to work from the cafes on Fridays.

> **All the information the social engineer gathers contains crucial plot pieces, helping to weave together a deceitful narrative. The engineer uses this knowledge of the target to strategically plan nefarious scenarios against the VP.**

Through more OSINT hunting, the social engineer finds a tea shop out of state called Steepers. He creates a fake email address, mimicking the lookalike domain used on the tea owner's website. Posing as the owner of Steepers, the social engineer constructs an email for the VP of Tea Castle, introducing himself as Steeper's CEO, and asking if she'd be interested in sampling their hand-blended teas. He even goes a step further by singling out Steeper's Earl Gray, saying it is his favorite (knowing from the VP's posts that she also likes this type of tea). The VP replies that she'd love to sample their best-selling teas, and the social engineer now has a way in. He pulls a Steeper's tea list sample from their site and drops malware into the PDF.

The bad actor waits until Friday at 3 p.m. to reply with his second phishing email, knowing that the VP is probably out enjoying tea and more likely to be excited about trying more. Then, he sends her the PDF, hoping she's using public WiFi at the shop and not on a secure VPN or home network. Once clicked, this attachment sneakily injects the VP's computer with malware, giving the bad actor a doorway into her corporate system. He may continue the conversation with the VP for a bit, especially if he needs more information to get past more barriers in her system and needs to launch another posed cyberattack.

2 The Early History of Social Engineering

While computer technology has only advanced enough to spur the idea of security-based social engineering for the past few decades, people have been using the principles of human psychology to manipulate others for hundreds of years.

The First Record of Social Engineering: The Trojan Horse Attack

Are you familiar with the story of the Trojan Horse trick, first mentioned in the famous novel The Odyssey? The story takes place in 1184 B.C., and the Trojans and Greeks are warring. After a 10-year siege, the Greeks realized they had to get crafty to defeat the Trojans. They constructed a giant wooden horse and hid some of their army inside. The rest of the military sailed away, appearing defeated.

The Trojans fell for the trick; dragging the wooden statue past their protective barriers as a trophy for their long-overdue victory. At night, the Greek soldiers waiting inside of the horse snuck out and unlocked the gates around their city— sneaking in the rest of their armed forces who returned. The Greeks then used the element of surprise to destroy the city of Troy from the inside. Therein lies the first recorded instance of social engineering.

Fast forward centuries later, Kevin Mitnick helped to popularize the concept of "social engineering" as we know it today in cyber security through various techniques and methodologies.

Kevin Mitnick and Social Engineering in the 1990s

When Kevin was on the run from the FBI, he was working at a well-respected law firm in Denver, CO. One day, he read a magazine at a newsstand listing all the best manufacturers of mobile handsets such as Nokia, Ericsson Fujitsu, NEC, and Motorola. Because of his keen interest in cellular phones, he was hooked on pursuing the source code of each manufacturer. In hopes of being able to communicate privately and avoid arrest at this time, Kevin sought to manipulate the technology inside the once high-tech MicroTAC Ultra Lite cell phone by Motorola.

He began his social engineering siege by calling the directory to get the phone number for Motorola (a common practice before the popularity of Google). During Kevin's eight transfers prior to connecting with the VP, he learned a very interesting fact: Motorola has a research center in Arlington Heights. Under the pretense of an employee from the Arlington branch, Kevin asked again to connect with the Project Manager for the Ultra Lite. The VP gave Kevin the Project Manager, let's say, Pam's, extension, but she was on vacation. She left a contact number on her voicemail to reach another person in her absence. We'll call her Alicia. Kevin called Alicia and asked if Pam left on vacation yet to create the illusion that he and Pam had connected prior, making his story more believable.

He then told Alicia that Pam promised him she'd send him the Ultra Lite source code but said that if she couldn't before leaving, Alicia could send it. He then instructed her on how to zip the files, since there were hundreds to package. Alicia asked him to hold while she went to grab her Security Manager to help. Kevin panicked, but to his surprise, she returned with the security person's username and password to the proxy server to upload the file!

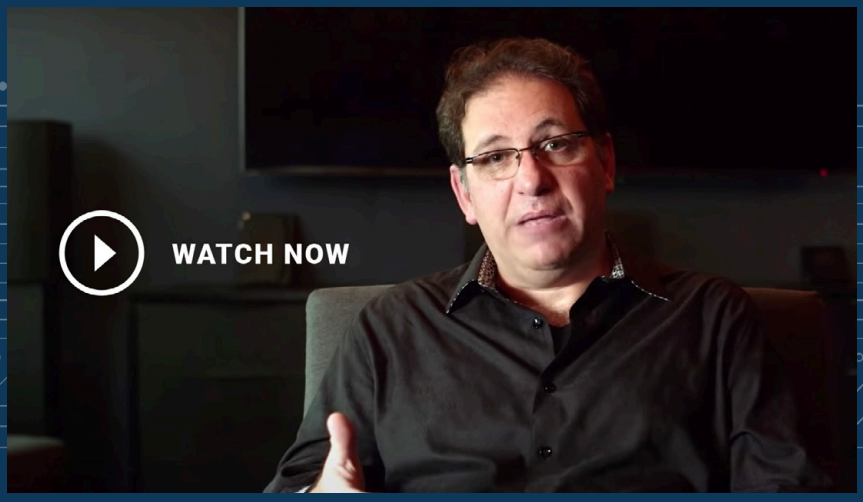
This clever narrative helped Kevin complete his mission and walk away with the source code. Although he didn't end up doing anything with the code, this type of highly sensitive property information could have easily been sold for high profit, or been used as blackmail against Motorola for a generous payout if in the hands of a hacker.

The Evolution of Social Engineering in Cybersecurity

While there's no arguing that the Trojan Horse story and Kevin's Motorola exploit denotes powerful examples of manipulation, modern social engineering ploys involve more direct relationship-building and clever storytelling over digital technology.

However, because many social engineers conduct attacks on complex, interconnected devices, it's harder to trace a breach now than it was in the '90s through the early 2000s. Plus, even when an attack launches, the breach is often undetected, with the target sometimes having no idea they've been compromised until it's far too late.

In fact, the average "dwell" time for a hacker is 43 days. During this time, a hacker could dig deeper into a system, gradually uncovering more private data for financial gain. Often, it isn't until the threat actor takes the quest too far and is accidentally discovered through suspicious activity or boldly reveals themselves that the attack is even detected.



3 Types of Social Engineering

Social engineers have more than a few tricks up their sleeves for deceiving unsuspecting targets:

Phishing

Just like real fishing, hackers throw out digital bait of their own when social engineering, a practice often referred to as "phishing."

Although at its root, phishing attempts share a core purpose of tricking a target into performing an action or revealing information, the practice comes in many forms. For example, amateur hackers send out mass correspondence— casting a wide net and hoping to trick a large pool of recipients. But more often than not, these generic messages are often too impersonal to fool anyone.

Most advanced hackers bait one at a time; they research and obtain deep knowledge of each victim and craft a unique narrative that is hyper-relevant to the individual. This is called "spear phishing."

Common Phishing Methods

PHISHING EMAILS

These are emails that have malicious intent. Whether it's a seemingly normal message with an infected attachment or one that tricks readers into clicking on a spoofed URL that captures their login credentials, phishers often get crafty in your inbox.

VOICE PHISHING (VISHING)

Sometimes, bad actors use the influence of a friendly voice to their advantage. Voice phishing is any form of phishing that takes place over the phone. These are voicemail messages asking you to call back to take immediate action and often leverage fear to get callbacks.

SMS PHISHING (SMISHING)

Threat actors know millions of people own a cell phone and will message you directly to compromise you. This may be a text message telling you you're late on a payment and to pay on the attached link to avoid a late fee, wherein the hacker captures your login information or banking details.

Pretexting

Pretexting is the narrative the hacker invents based on their researched knowledge of you to fool you into believing its legitimacy.

THE MAKINGS OF A GOOD PRETEXT

The success of the pretext is dependent on how strategically the hacker can piece together a believable scenario, as well as their ability to pivot the conversation back in their favor should their pretext be questioned.

"I'm always on the watch for little signs that give me a read on how cooperative a person is," Kevin Mitnick shared in his book The Art of Deception. He playfully explains how he assesses a victim's cooperativeness on a scale "that runs from 'you sound like a nice person, and I believe everything you're saying' to 'call the cops, alert the National Guard, this guy's up to no good.'"

A bad actor must tread softly on the fine line between these two states, for just one red flag passed to management or IT could burn the source, meaning the targeted company is too vigilant of suspicious activity to be a plausible target for another attempted social engineering scheme in the future.

Common pretexts involve impersonating someone you know or another trusted source, with a clearly explained reason why they're asking you for information or to take action. An example of this includes impersonating a client or a high-level employee of the targeted organization to gain personal information, such as payment information, credentials, or data.

Baiting

Baiting occurs when a hacker dangles something tempting before you, hoping you'll take action.

This could be an email with a provocative video clip (sometimes called a honeytrap) or a document labeled "Confidential." Sometimes, the bad actor won't even ask you to click it, hoping your curiosity will be enough.

Tailgating

Just like a driver hugging the back of your car on the road, some social engineers trail closely behind an employee entering a building to gain access to a restricted area that would normally require a fob or code. These threat actors usually have a clever pretext— dressed as a delivery person carrying boxes or as a friendly face with a dozen donuts for the staff— creating a false sense of trust to let them through the door behind their tailgated target.

Quid Pro Quo

Quid Pro Quo is a social engineering technique where the hacker offers to help the target in exchange for information or access.

This could be someone posing as a member of your IT team saying they need your computer password to make a necessary system update or the promise of a free music streaming subscription if you sign up for a fake streaming service. Ultimately, the engineer promises to provide a service or item in exchange for you providing something.

4 Common Social Engineering Tactics

Social engineers are such savvy information swindlers because they understand the psychology of influence. According to behavior psychologist Robert Cialdini, people influence others in seven main ways.

Understanding these principles can help you better educate your employees on some common social engineering tactics hackers use.

Social engineers use reciprocation not as a kind gesture, but as a compliance tactic for getting private data.

Reciprocity

Social engineers understand that giving back when we receive is human nature. Most of us feel obligated to repay someone for a favor, gift, invite, or kind gesture, so bad actors often bait their target with a little offer.

Let's say your employees get an email saying they'll receive a $10 Amazon gift card for anonymously filling out a survey from the IT department asking how well they're handling digital security. Unfortunately, it's actually from a spoofed recipient masquerading as a trusted source. Yet, because it looks like an email from your own IT team and your employees will receive a reward— you scratch IT's back by filling this out, IT will scratch yours by giving you a gift card— your employees may be inclined to give pertinent details about your security to a hacker. Employees who fill out the survey may even receive a legitimate gift card, to reduce arousing suspicion, a small price for the cyber criminals to pay for a wealth of information aiding in a mass-scale hack.

Scarcity

We want what we can't have, especially when we perceive it as rare or hard to come by. That's why those emails we receive saying, "Order now! Only 10 left!" often make us impulse-buy a product we don't really need.

Social engineers often capitalize on scarcity to influence targets, creating a clear divide between "you can have this now" and "you can never have it again." This may be a bad actor emailing an employee a special offer for a new tool your team could really use. Bad actors use scarcity to create a sense of urgency, making you less inclined to think before taking action or sharing information.

Authority

Hackers often pose as managers or members of the C-suite to trick lower-level employees into conceding to a request. The infamous “wire transfer” social engineering tactics are a prime example of authority at play.

A social engineer may know a manager is out of the office and create a spoofed email address to ask a staff member to route money from one location to another since the boss is busy or on vacation. Because an authority figure demanded the action, some employees may do it without thinking, fearing reprimand from management for hesitating.

Social engineers imitate a person of importance quite often, using a false sense of authority and urgency to get their way.

Liking

We’re more willing to help someone we find likable than someone with characteristics or traits we dislike. According to Kevin Mitnick in his book, The Art of Deception, the main tools a social engineer needs are “sounding friendly, using some corporate lingo, and…throwing in a little verbal eyelash-batting.”

A prime example of the liking principle in action would be a charismatic voice phisher. The social engineer rings you up, claiming to be an authoritative source— perhaps a vendor— and cracks a few jokes, maybe even compliments you or your company. But he’s also waiting to use his charm to his advantage.

Commitment & Consistency

People want to see themselves as consistent with their word. Social engineers often leverage this need for self-preservation by building a slow, steady rapport with a target and requesting small commitments to achieve their strategic goals.

A hacker may email you a friendly correspondence, pretending to be a happy customer who wants to thank you for how incredible your product is. A few weeks go by, and the bad actor commits to their ruse, emailing you again to see if you’d be interested in some lifestyle photos of your product set up in his office to share on social media. You concede, and he sends over what he promised to establish trust. You thank him, and he asks you to promise to keep him in mind for influencer marketing help in the future. You love the content, and you agree without hesitation. So the next time he emails you a few images, you eagerly open the attachment, only to download malware.

Consensus & Social Proof

Hackers know that people rely on the actions and opinions of others to determine their own. That's because we innately trust that it must be a safe or wise choice if others are doing or saying one thing.

Social engineers create crafty pretenses using "proof" from what others have done to convince you to do the same. For instance, a hacker might call and ask an employee for sensitive information, like a daily changing code, and when they resist answering, they'll say something like, "I don't understand, Linda shared this with me last week."

Social engineers often couple this strategy with the "authority" tactic when their pretext begins to backfire, threatening lower-tiered employees to comply or they'll pull a manager into the conversation for resisting the request.

Malicious manipulators capitalize on shared struggles or experiences to make a relatable connection with their target for a quick "in."

Unity

We all want to feel that others can relate and empathize with us when in need. Social engineers will use pretenses to make themselves as relatable as possible, creating a sense of unity between themselves and their target to build trust before deceiving.

Social engineers use their open source intelligence research to understand the inside knowledge of your organization, like staff names and clock-in times.

A cybercriminal may know after previous rapport with an employee, for instance, that your staff hates having to use their fobs every time they want to enter the building. The engineer tailgates one of your workers, pretending to be a new employee who forgot their fob. She banters about how annoying it is to always remember your fob and introduces herself as the new receptionist working for a neighboring department. The social engineer mentions the manager by name and has a relatable pretense for rushing to get to work on time, much like your almost-late employee is now. The real employee feels unified in their struggle and lets her through the door with a smile and laugh, saying, "don't be late!" as he walks the other way and grants a stranger full access to the building.

5 Things You and Your Employees May Not Know About Social Engineering

The point is: no one is 100% safe from being the victim of a social engineering attempt. This is an important point to drill home to your entire team and anyone you work with.

Social engineers don't go after one department or individual in your organization exclusively, making it difficult to know who could become the next target.

While you may think these hackers would go after lower-tiered employees, it all depends on the information the bad actor is after and who they think can lead them to it.

Those that are susceptible to social engineering include but are not limited to:

- Entry-level employees
- C-suite executives
- Vendors
- IT managers

Social engineers do meticulous research on your industry, brand, and individuals within your organization. It's how they acquire and leverage base information, credentials, passcodes, or poor security measures. The bad actors do in-depth, extensive research and develop a strategic plan with many steps before beginning their conquest.

When a social engineer makes their first point of contact, they have already formulated the tactics and methods they'll use to compromise your business and rehearsed and perfected their pretense. They'll know your company's inside lingo, specific details about your teams and staff members, your office location, and other bits of information that could be useful in painting a convincing portrait of authority and trust with unsuspecting targets. Many people mistake social engineers as smooth talkers who fly by the seat of their pants, but their process is a lot more methodical and calculated than that.

Some software developers will spend weeks developing a fake website to capture user credentials or steal information and another few weeks devising how they'll drop the payload without suspicion.

You Might Not Notice an Attempt or Attack

In most hacking scenarios, the bad actor does not want to be detected— throughout the entire exploit. That's because the longer they can sit within your system unnoticed, the more likely they can gain deeper access to exploitable information.

With this in mind, hackers often launch an attack in stealth, compromising a device or an entire network quietly, with your organization none-the-wiser. You could click on an infected link in a phishing email or download malware from a fake update triggered by a lookalike WiFi network and never know that someone can now access your corporate network.

You could even unintentionally download spyware onto your device and have a threat actor recording your actions by capturing your keystrokes as you type in usernames and passwords. Or they may tap into your device's audio or video functionality to hear your conversations and view your webcam.

6 The Biggest Social Engineering Attacks in History

(2019) Toyota BEC Scam

A subsidiary of Toyota Boshoku Corporation was fooled by a crafty social engineering scheme last year— one that cost the brand greatly. This particular business email compromise (BEC) scam was actually quite simple: a hacker targeted the inboxes of the car corp's finance and accounting department's emails, impersonating a business partner of the Toyota subsidiary requesting payment to a specific account.

While $37 million might sound like an outrageous request, large-scale businesses like Toyota see requests of this nature often, and an unsuspecting worker transferred the funds to the social engineers' account.

Objectively speaking, this is a plausible mistake. But what makes this hack so cringe-worthy is that it was the third acknowledgment of an attack on Toyota that year alone, according to the CEO of their security company. The first was in Australia in February 2019, then again in Japan that March before the attack on Zavantem, Belgium's European headquarters of Toyota Boshoku in September.

LESSON LEARNED

Toyota had been subject to multiple cybersecurity attacks in early 2019, so for an employee— later that same year— to approve a financial request without verifying the need for the transaction and the identity of the recipient is, no doubt, unacceptable.

This is a classic case of "fool me once, shame on you. Fool me twice, shame on me" on Toyota's part for not prioritizing extensive cybersecurity awareness training after a series of targeted attacks. If you've noted suspicious cybersecurity attacks on your business within the last two years, we highly recommend educating your staff on what previously happened as well as possible threat scenarios to look out for, while simultaneously improving your current defense gaps.

(2020) Shark Tank Spear Phish

Barbara Corcoran, of the ABC show Shark Tank, lost a large chunk of change in February 2020 to a savvy social engineer. The hacker took to the inbox of Corcoran's bookkeeper, spoofing the email address of the TV star's assistant and requesting $388,000 funds to be wired to an Asian bank with an attached invoice for real estate renovations.

Because the email looked like a direct message from the assistant and the hacker responded so professionally and accurately in their email correspondence to confirm the request— a social engineer who clearly did their research into Corcoran's business affairs— the bookkeeper was fooled.

LESSONS LEARNED

This spear phishing hack could have been prevented had Corcoran's bookkeeper directly called or contacted the assistant via any other means than email to confirm the nature of the money transfer.

Always, always, always question a request you receive via email, as these messages can be easily faked. Social engineers are especially good at mimicking email addresses, creating believable assets like invoices or spoofed URLs, and weaving together a convincing story to make the correspondence seem legitimate.

(2020) Twitter Bitcoin Scam

On Wednesday, July 16, 2020, many prominent, highly-followed Twitter (now "X") users simultaneously posted "double your Bitcoin" Tweets. These social posts told their followers that if they contributed money by clicking a link, the figure would match the donation, returning double the amount.

A few of the targets in this scam were former President Barack Obama, current President Joe Biden, Elon Musk, Mike Bloomberg, and even big tech companies, such as Apple and Uber. While many of the targets deleted their tweets and locked their social media accounts, the damage was already done: The accounts targeted had millions of followers and within minutes received hundreds of contributions, reportedly totaling over $100K in Bitcoin, according to The BBC.

The hackers managed to social engineer their way into Twitter by exploiting their employees and navigating internal systems while also acquiring administrative access to high-profile usernames and passwords.

LESSONS LEARNED

The company's greatest vulnerability was its workforce, who fell victim to social engineering scams that gave threat actors access to sensitive information. Afterward, Twitter promised to enhance many critical vulnerability areas after the attack. See what areas of their cybersecurity they focused on here.

(2022) Uber Social Engineering Attack Through Slack

Uber's internal Slack platform was utilized by a threat actor to pose as an employee and access the company's network. They are thought to have elevated credentials, read sensitive data, and posted an explicit photograph. This threat actor acknowledged their victory and revealed they broke through Uber's security measures with ease by using social engineering.

LESSONS LEARNED

This social engineering scam highlights many issues regarding passwords and general cybersecurity awareness. While utilizing multi-factor authentication would be the first step to protecting passwords, it's just as vital to pair that process with credible and reputable cybersecurity awareness training.

(2022) Twilio Attack

By obtaining an employee password, a threat actor was able to access confidential customer and employee account information of Twilio, a classic case of a phishing attack.

LESSONS LEARNED

While a forensics company was hired to support the continuing investigation and Twilio's security team removed access to the hacked employee accounts as soon as the event was verified, the attack had already happened.

The most proactive solution to this would have been to prioritize cybersecurity education across the company. Your team must understand the dangers of text messages and emails, especially if there is a link included in the message.

(2023) MGM Resorts Social Engineering Attack and Data Breach

On September 11, an unauthorized group— now identified as "Scattered Spider"— launched a social engineering attack on MGM Resorts. While exact details are still under wraps, it's speculated that the attack occurred due to a lackadaisical approach to login credentials, such as using the same passwords and usernames involved in previous data breaches on MGM Resorts. With the login credentials in their possession and some extra LinkedIn profile research, they social engineered the front desk of MGM Resorts to reset the multifactor authentication for them, granting them access to all the accounts they had the login credentials for.

The results? Scattered Spider obtained access to sensitive information of several customers (the exact number hasn't been revealed) in their database. This included basic contact information but also social security numbers and driver's licenses.

LESSONS LEARNED

MGM Resorts released a statement on November 6 outlining the steps they took. After learning of the unauthorized access, they shut down certain affected systems involved in the attack. Then, they initiated an investigation with the help of cybersecurity teams and law enforcement.

All of this could have been mitigated, if not entirely avoided, if MGM Resorts had followed best practices for login credentials and educated their staff on security awareness training and layering defense. For instance, they should have never reused login credentials involved in a previous data breach. That's basically handing the hackers the login credentials. Additionally, by investing in industry-leading education for cyber security, such as Mitnick Security and our vast library of educational resources, their team could have handled the front desk situation much better.

Other Famous Social Engineering Attacks

While the social engineering exploits mentioned above are no doubt notorious, we rounded up the biggest and the best in a separate blog.

In our post, "The Top 5 Most Famous Social Engineering Attacks of the Last Decade," we'll dig into the story and lessons behind the:

- 2013 Target Data Breach
- 2016 United States presidential election
- 2020 Twitter Bitcoin Scam
- 2014 Sony Pictures Hack
- 2013 Yahoo Customer Account

7 How to Avoid Social Engineering Scams

Social engineering attempts will come your way, no matter how strong your security measures. It's how you prepare and react to the attempts that matter. That starts with your team.

Here are our top methods for not only educating your team but actually getting them to opt into any new cybersecurity policies you implement.

Share Examples of Social Engineering and What Went Wrong

While the technical logistics of a hack can be confusing to the everyday person, your team can, however, learn from stories. Walk your staff through the narrative of some of the most notorious social engineering attacks above, and include real examples of some of the hacking techniques we shared with you.

They should understand how the action could occur due to negligence on their part and the consequences of the attack.

Identify and Crack Down on Remote Vulnerabilities

Many businesses now have numerous remote workers, which opens up many cyber security risks you and your employees need to be aware of. Here are a few techniques that all CISOs should educate their teams about to understand and safeguard against remote threats:

- Utilize company-wide secure data storage solutions
- Ensure your employees use a private, business VPN
- Get help from a credible and experienced cybersecurity team

Invest in Professional Security Awareness Education and Training

The only sure-fire way to stay up-to-date with recent threats is to routinely remain informed on the evolution of social engineering.

While it may seem mundane to your employees, a yearly security awareness class and testing can help to ensure they're staying sharp and diligent. By giving your team access to a full training library, they can learn at their own pace through educational videos, including live threat demonstrations.

Explore our award-winning security training resources here.

Send Your Users Cybersecurity Tips

Looking for information you can send your employees to stay better on guard? These bullets are easy to share in one email and to share periodically as reminders of best practices.

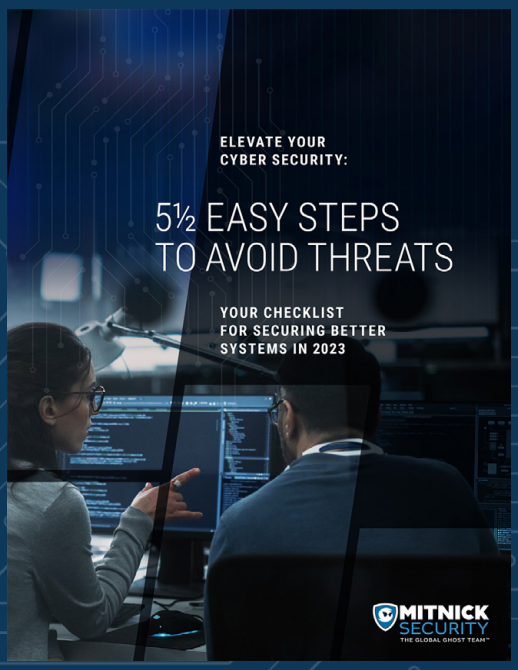
- Always think before you click attachments in emails, linked URLs, or downloads/updates.
- Never disclose personal or company information that's not public knowledge unless a person has the (confirmed) authority to know such info.
- When in doubt, verify. This includes someone's identity, sharing permissions, policies, etc.
- If you receive an email asking you to perform a questionable action from someone you know, contact them via phone or in-person to ensure it was really them inquiring.
- Look for secure URLs that begin with "https," and be cautious when on "http" URLs (the "s" being key).
- Enforce multi-factor authentication (MFA).
- Actively maintain antivirus software, firewalls, and email filters, making routine updates to patch vulnerabilities.

Find More Cybersecurity Tips Here

FREE CHECKLIST

5½ EASY STEPS TO AVOID THREATS

Download Now



Test Your Social Engineering Strength

While you can't stop social engineers from trying, educating your team on the threat landscape is your best defense for preventing a social engineering hack. Additionally, you can get help from the world-renowned Global Ghost Team™.

Curious to see how your team would stand up against social engineering tactics without any formal training?

Invest in Strength Testing Today