Social Engineering Attacks | How to Recognize and Resist The Bait

By SentinelOne

Published: 2023-10-19 · Archived: 2026-04-29 02:13:51 UTC

While much of cyber news often revolves around novel malware strains and high-profile data breaches, one threat that often flies under the radar relies on human vulnerability rather than technical vulnerabilities: social engineering attacks.

This type of attack exploits people's most innate tendency to trust, comply, and share information. This is what makes these attacks exceptionally effective. Using psychological manipulation, cybercriminals behind these schemes are then able to trick users and organizations into giving up sensitive information, granting access to secure systems, or transferring funds.

As businesses and organizations rely more on interconnected systems and digital communication, they become more exposed to the dangers of social engineering. Part of countering this growing threat is understanding the psychology behind social engineering. Recognizing these tactics and the psychological triggers that attackers exploit can empower users and organizations to take proactive measures against the risks.

This blog delves into the intricacies of social engineering attacks, exploring the various forms they take and the underlying psychology behind these attacks. By mapping out the motivations and tactics used by attackers to exploit users' cognitive biases and emotions, business leaders can learn how to recognize and resist attacks and stay one step ahead of cybercriminals.

The Fundamentals of Social Engineering Attacks

Social engineering attacks are multifaceted and ever-evolving making them an evergreen threat to individuals and businesses. These attacks draw on human psychology and social dynamics to manipulate users into divulging performing actions that compromise security, data, and assets.

Social engineering has become a bread-and-butter tactic for cybercriminals with recent reports finding a staggering 464% increase in email-based attacks in the first half of this year compared to 2022. Further, when considering such attacks per organization within the same time frame, researchers note a 24% increase, underscoring email as the leading attack vector used by cyberattackers.

Understanding the fundamentals of social engineering is critical for businesses and organizations, as it can help them recognize, defend against, and mitigate the risks these attacks pose in the short and long term.

Phishing

Phishing is one of the most common forms of social engineering. It typically involves sending fraudulent emails that appear to be from a reputable source, such as a bank or a trusted colleague. The goal is to trick the recipient into clicking on malicious links or providing sensitive information, like login credentials or financial details.

Spear Phishing

Spear phishing is a more targeted form of phishing. Attackers conduct extensive research on their victims, crafting highly personalized emails that are much harder to distinguish from legitimate communications. They often target individuals such as privileged admins that have access to valuable information or financial resources within an organization.

Pretexting

In pretexting attacks, the attacker creates a fabricated scenario or pretext to obtain information. This often involves impersonating someone with authority or a legitimate reason for needing sensitive data, such as supporting a customer, complying with IT support personnel, or granting approval for multi-factor authentication (MFA).

Baiting

Baiting attacks entice victims with an attractive promise, like a lucrative job offer, free software downloads, movies, or music. Once the victim takes the bait and downloads the file, malware is delivered, compromising the victim's device and potentially spreading through the network.

Multi-Channel Attacks

Multi-channel social engineering leverages various communication platforms to manipulate and deceive individuals or organizations. Instead of relying on a single channel like email, attackers combine various communication methods, including email, phone calls, social media, and even physical interactions. This creates a convincing illusion of legitimacy and credibility, making it more challenging for targets to discern the fraudulent nature of the attack.

Pulling Back the Curtain | The Psychology Behind Social Engineering

Regardless of the type of attack, the role of psychological manipulation is key to successful attacks, exploiting the intricacies of human emotions, cognitive biases, and social dynamics. Human users can be tactfully manipulated into serving the attacker's objectives.

The Psychology of Persuasion | Understanding the Attacker's Mindset

Being aware of the manipulation strategies employed by attackers helps develop a heightened sense of skepticism, making it more challenging for social engineers to succeed.

Psychological manipulation involves a range of tactics that leverage fundamental aspects of human behavior:

- Trust and Authority – Social engineers often assume roles or identities that inspire trust. Whether posing as a trusted colleague, a senior executive, or a knowledgeable IT technician, they exploit the natural inclination to comply with authority figures and follow social norms.
- Reciprocity – By offering something of apparent value, even if it's as simple as a small favor or free software, social engineers stimulate the instinct of reciprocity. When people feel they've received something, they're more likely to return the favor, which can involve sharing information or granting access.
- Fear & Urgency – Creating a sense of urgency or fear in targeted victims is a common tactic. This can include warnings of impending threats, account compromises, or financial loss, which then pushes the targeted victim to act hastily without critical evaluation.
- Social Proof – People tend to follow the crowd or conform to social norms. Social engineers often use this bias by showing that others have already complied with their requests, suggesting that the target should do the same.
- Bonding & Connection – Building rapport and forming a connection with the target is a powerful tool. Social engineers may feign common interests, offer compliments, or appear as genuinely likable individuals to lower the target's guard and increase their willingness to cooperate.
- Fear of Missing Out (FOMO) – Creating the illusion of scarcity, whether it's a limited-time offer or an apparently 'exclusive' opportunity, plays on the very human fear of missing out. This compels the targeted victims to take action quickly, often without thinking things through.
- Commitment & Consistency – People tend to remain consistent with their prior actions and statements. Social engineers exploit this by encouraging small commitments or decisions that align with the targeted victims' objectives. Once an individual commits to something, they are more likely to follow through with related, more significant requests, making them more susceptible to manipulation.

Cognitive Biases | Fertile Grounds Exploited by Social Engineers

Cognitive biases are deeply ingrained in how people think and make decisions. Cybercriminals focus on manipulating these biases to meet their malicious goals.

- Anchoring Bias – relying too heavily on the first piece of information encountered, even if it is irrelevant. Cybercriminals use anchoring bias to set an initial reference point that heavily influences a target's subsequent decisions. For example, in a negotiation for a fraudulent deal, attackers might suggest an extravagantly high initial price, thus anchoring the target's perception of what is reasonable.

- Confirmation Bias – the tendency to seek out, interpret, and remember information in a way that confirms one's preexisting beliefs or expectations. Social engineers leverage this bias by providing fake evidence or information that aligns with the target's preconceived notions, making the target more likely to trust and comply with their requests.
- Recency Bias – the tendency to give more weight to recent events or information. Social engineers exploit this bias by timing their attacks strategically, ensuring their requests align with recent experiences or news. This makes it more likely for the victim to accept the request without due scrutiny.
- Overconfidence Bias – the overestimation of one's abilities, knowledge, or judgment. Attackers capitalize on this bias by encouraging targets to trust their own judgment in making decisions that benefit the attacker. Victims may believe they are too savvy to fall for scams, leaving them vulnerable to manipulation.

Rising Trends In Social Engineering

Recent developments in generative artificial intelligence (AI) are a cause for concern in the context of social engineering schemes. AI could be used by attackers to craft sophisticated threat campaigns that manipulate human behavior. Automating data collection and creating persuasive messages can significantly enhance the potential impact of such attacks.

The rise of deepfake technology has also introduced a new avenue for social engineering attacks where AI can be used to deceive a targeted victim into believing false information. Deepfakes leverage machine learning (ML) algorithms to create highly realistic images, audio, and videos that can easily fool viewers into thinking they are authentic. Deep fakes could allow attackers to impersonate high-profile individuals, such as senior leadership or government authorities, as a key part of their requests for access and information.

Recognizing Social Engineering Red Flags | Avoiding the Hooks, Lines, and Sinkers

Training and awareness programs can help teach employees about these biases and how they are used in social engineering attacks. To a trained eye, social engineering schemes are fraught with red flags. Learning how to recognize and resist these warning signs is how businesses can defend their sensitive data and keep their users safe from cyberattackers.

These are six of the most common triggers to look out for:

Red Flag #1: Out of the Blue Requests

One of the primary red flags in social engineering is receiving unsolicited requests or communications. Be cautious of unexpected emails, phone calls, or messages asking for sensitive information, money, or assistance. Cybercriminals often rely on the element of surprise to catch their targets off guard.

Red Flag #2: Feeling Under Pressure

Social engineers often employ tactics that create a sense of urgency and pressure to act quickly. They might claim that a situation requires immediate attention, or that failure to comply will lead to severe consequences. These

pressure tactics are designed to override rational thinking and encourage hasty actions.

Red Flag #3: Unverified Sources & Contacts

If a request or communication comes from an unverified or unfamiliar source, treat it with skepticism. Verify the identity of the sender through a secondary means outside of the initial communication platform. Since social engineers can easily impersonate trusted individuals or entities, confirm all requests independently and directly with the person or company they claim to be.

Red Flag #4: Issues With the Content

Pay close attention to the content of the communication. Check for inconsistencies, misspellings, or unusual language that may suggest a fraudulent message. Cybercriminals often make mistakes in their attempts to deceive, and these errors can serve as warning signs.

Red Flag #5: Emotional Manipulation

Social engineers frequently employ emotional manipulation to sway their targets. Be wary of messages that evoke strong emotions, such as fear, excitement, or sympathy. When emotions cloud judgment, individuals become more susceptible to manipulation.

Red Flag #6: Requests for Sensitive Information or Credentials

Perhaps the most obvious red flag is a request for sensitive information or login credentials. Legitimate contacts rarely ask for private information through unsolicited messages. Be cautious when providing personal or confidential data, especially when prompted via email or messaging platforms.

Conclusion

Social engineers capitalize on human psychology, cognitive biases, and our innate tendency to trust all in effort to slip past set security measures. Recognizing the red flags and understanding the evolving techniques of social engineering attacks is critical for businesses building an effective defense against these types of attack.

The threat landscape for social engineering attacks continues to evolve, requiring a proactive and adaptive approach to defense. To stay steps ahead of cybercriminals, businesses and organizations must be vigilant in recognizing and resisting these attacks to mitigate the short-term and long-term risks they pose. By educating employees and implementing robust security measures, leaders can significantly reduce their vulnerability to social engineering attacks and safeguard their operations and sensitive data.

SentinelOne is ready to help business and organizational leaders build a proactive cybersecurity stance against social engineering-based threats through continuous threat detection and response capabilities and autonomous threat hunting. Contact us today or book a demo to learn more.
