Combatting Social Engineering

Although ransomware, data breaches and other large-scale cyberattacks are frequently in the headlines, it is easy to overlook the common thread that runs through many of these incidents: social engineering. According to Verizon's *2022 Data Breach Investigations Report,*[1] 82 percent of breaches involved social engineering tactics, and other sources estimate the percentage to be even higher. It is a big problem, and it does not look like it is going away anytime soon.

As a case in point, consider the recent breach of the ride-hailing service Uber.[2] Apparently, the attack originated when a lone hacker impersonated an Uber staff member and then deceived an actual Uber employee into revealing user credentials. From there, the hacker was able to obtain sysadmin privileges to gain access to highly confidential financial and customer data.

The Uber attack used one of the more common social engineering tactics: impersonation, which is sometimes referred to as pretexting. By masquerading as a member of Uber's IT team and ratcheting up the frequency and urgency of demands for credentials, the hacker eventually appeared to be legitimate to the target. Luckily, it appears the hacker was more interested in notoriety than financial gain, and Uber later reported that sensitive customer data were safe.

The human element means that social engineering cannot be completely averted by a simple plug-and-play technology or a software patch.

Overall, cybersecurity is well understood only by the dedicated security practitioners who strive to keep network and cloud resources safe. Many of the technologies involved are complicated, and a confusion of acronyms permeates the industry. Yet social engineering typically does not involve elaborate technologies or strategies. Instead, it employs tactics related to human psychology, which is more easily explained and understood in the context of cybersecurity.

Further, the human element means that social engineering cannot be completely averted by a simple plug-and-play technology or a software patch. It requires education to increase the general awareness of cybersecurity basics across the entire organization. And with social engineering, it is equally important to understand both how these attacks operate and why they succeed.

Many security services—such as antivirus, antimalware and intrusion prevention—usually rely in part on signatures and other indicators to identify and

CHUN LI

Is director of technical marketing at Hillstone Networks. In his role, he leads the global strategic planning and go-to-market execution of products and solutions and technology evangelism. Before Hillstone, Li worked at Cisco Systems in both product management and technical marketing roles. During his tenure in technical marketing, Li was responsible for driving go-to-market initiatives and product development and evangelizing new products and solutions in close alignment with customers and end users. Li has been a featured speaker for events and webinars worldwide.

thwart potential threats. Other protective strategies, such as security policies and procedures, require knowledge of how users should interface with network elements—in other words, human interaction. However, the psychological aspect of social engineering requires that system engineering balance the full gamut of user needs across both technical and nontechnical roles to address security gaps.

But the narrative on social engineering is not necessarily all doom and gloom. There are multiple ways of thwarting these types of attacks—mostly involving user education, but also through technology solutions that can help defend against them.

How Social Engineering Works

From the 30,000-foot view, social engineering tactics can be generally categorized into three types: phishing, impersonation and physical exploits. A curious commonality among these social engineering techniques is that, anecdotally, the frequency of occurrences seems to decrease as the level of effort required rises. For example, while phishing attempts are depressingly commonplace, the more targeted types of attacks are reported less frequently.

Phishing

Phishing is by far the most common social engineering tactic in use today. According to the 2022 Verizon report, nearly 70 percent of social engineering breaches were attributed to phishing and its variants.[3] Phishing messages can be quite elaborate, using a legitimate organization's logo and font to appear more realistic. Or, like the age-old Nigerian prince advance-free scam,[4] they can be very basic and quasi-personal.

A phishing attempt usually prompts the recipient to take some type of action (e.g., update account information, reject a purchase for an amount) to avoid a negative repercussion for failing to comply (e.g., account suspension, credit card charge). A particularly sinister form of phishing is blackmail, in which the attacker threatens to publish false embarrassing or incriminating information if demands are not met. Currently, this form of phishing seems to be more prevalent in countries that have morality-based laws or regulations.

Phishing variants include vishing (via telephone) and smishing (via text messaging), both of which use nonselective tactics similar to phishing. Unlike other subtypes, spear phishing and whaling are highly targeted and customized approaches. A spear phisher researches a target via social media and other means, then tailors the attack to generate a higher chance of success. Whaling is a form of spear phishing that targets executives and other high-profile individuals. Both tactics may contain elements of impersonation (pretexting).

Impersonation

Impersonation involves an attacker masquerading as someone else, as in the Uber attack example. It typically entails background research and the creation of a fake situation, or pretext, which is then used to convince the target to take a specific action. Often referred to as pretexting, because of the false scenario used by the attacker, this type of social engineering relies on perceived legitimacy to succeed.

An attacker might impersonate a leader in an organization or an authority figure to gain information, such as network access credentials (as in the Uber case), customer lists, confidential business data or other critical knowledge. Attacks have resulted in the approval of false invoices or wire transfer requests, sometimes resulting in losses of millions of US dollars.[5]

A closely related type of attack is reverse social engineering, a ploy attackers use to convince targets to let them fix manufactured problems.[6] An attacker might pose as a representative of an organization's IT department or even a representative of a major vendor such as Microsoft to gain the target's trust. Often, the attacker will try to gain direct access to the user's computer via remote desktop protocol (RDP), which provides an open door to all information contained therein.

Physical Exploits

Although they are less common than other social engineering attack types, physical exploits can have devastating impacts. Baiting, for example, involves leaving infected media (e.g., USB drives) where users can find, pick up and use them. (The bait media are sometimes called "road apples."[7]) Baiting is anything but frivolous; the bait media typically include an executable that will download malware onto the user's machine upon insertion.

Tailgating is simply accompanying a legitimate employee or other authorized visitor through a secured entry door. This practice can give intruders access to confidential information within secured areas, at least until they are discovered.

Other Types of Social Engineering

Two other social engineering tactics to be aware of include watering hole and *quid pro quo* attacks. In the watering hole approach, an attacker targets one or more websites that are commonly used by an organization and then finds a website vulnerability that allows malicious content to be installed, which then infects site visitors.

"*Quid pro quo*" means something for something.[8] This type of approach can be quite similar to a pretexting exploit, with the attacker offering a fix for a nonexistent problem, or it can resemble baiting, with the attacker trading a physical item (such as a t-shirt or chocolates) for information desired by the hacker.

The Enemy Is Us

Social engineering works by getting inside people's heads, which means anyone who is able to connect to the enterprise network is a potential attack vector. A social engineering attack may leverage perceived familiarity, as with household name brands such as Microsoft or Netflix, or with supposed authorities such as the US Internal Revenue System (IRS), the US Social Security Administration or someone high on an enterprise organization chart. Other tactics might include reciprocity (as in *quid pro quo*), scarcity (limited quantities or time) or fear of missing out on something others have.

Attackers often use threats or escalation to achieve their aims, essentially triggering a sense of urgency in the target that can override reason. For example, in the Uber incident, the attacker barraged the Uber employee with requests to confirm login information, and then escalated to impersonating an IT staff member via WhatsApp.

As to why these types of threats succeed, researchers have put forth various theories, but they are all tied to human behavior. A recent study found that one in three employees were likely to click on links in a phishing email, and 60 percent opened emails without being confident of their legitimacy.[9] With dismal statistics such as these, it is tempting to throw up one's hands in defeat. Yet, given the high stakes, it is imperative to have a multilayered defense plan in place.

Attackers often use threats or escalation to achieve their aims, essentially triggering a sense of urgency in the target that can override reason.

Defending Against Social Engineering Exploits

With employees as the weakest link in the security infrastructure, education is the first line of defense against social engineering exploits and other insider threats. Given that the hybrid workforce has become far more common, training is even more essential.[10]

To a trained eye, phishing and similar tactics are usually quite easy to detect. Some of the hallmarks of these exploits often include:

- **Typos**—Misspellings, incorrect grammar and punctuation errors are much more common in bogus emails than in legitimate messages. Larger organizations (e.g., Microsoft, FedEx) typically employ a review process that reduces or eliminates these types of errors.
- **Unrelated or misspelled domains**—A phishing message will often come from an unrelated domain or a domain name that differs from a legitimate domain by only one or two characters.
- **Shortened or unrelated URLs**—Phishing attempts might include a truncated URL (such as a bit.ly address) as the click-through link or a legitimate-looking link that reveals something entirely different when a cursor hovers over it.
- **Deceptive subject lines**—The attacker might feign familiarity with the recipient or organization or express urgency.

Although email security gateways can block many social engineering attacks,[11] a program to elevate cybersecurity awareness can help further reduce an organization's vulnerability. Regular updates on recent attacks, training sessions during employee onboarding, and presentations by guest speakers can drive improved security.

Much as perimeter security has evolved to include layered defenses, protections against social engineering attacks can and should include tiered defenses beyond email security gateways.

Phishing simulations created in-house or by third-party vendors can be effective. For example, Microsoft Defender for Office offers a suite of tools for employee training and awareness building, including simulations.[12] Several organizations also offer nontraditional social engineering training via gamification.[13] Many employees, especially millennials and younger, may learn more effectively via gamified cybersecurity education.[14]

Depending on the environment, targeted training may be warranted for certain users, such as for executives who may be subject to whaling attempts or systems administrators and others who manage high-value, high-risk assets, for example.

Organizational Ground Rules

A particularly damaging form of social engineering attack may use impersonation of a superior to convince a subordinate to divulge security credentials, transfer funds or take a similar action. These exploits can succeed because, ultimately, an organization is built on employees trusting one another, often sharing personal information to become more likeable and relatable.

Cybersecurity efforts can and should include setting overall ground rules—for example, that certain types of requests will never come from a superior, and should be rejected, no matter how convincing they may seem. Business processes should include checks and balances to ensure that an attacker cannot bypass the process through intimidation or subterfuge.

Business processes have become even more important as the workforce has become more distributed, with the work-from-home model far more common than it was prior to the COVID-19 pandemic. A pretexting attack, for example, may impersonate a superior whom the target employee has never met or interacted with before. The absence of solid processes and policies can contribute to much greater chances of success for attackers—and conversely, greater risk of breaches or other damages for organizations.

Adding Layered Defenses

Much as perimeter security has evolved to include layered defenses, protections against social engineering attacks can and should include tiered defenses beyond email security gateways. Cases in point: Multifactor authentication (MFA)[15] and zero trust[16] strategies can help thwart the various social engineering threat actors who attempt to forge or steal network credentials. Both options add one or more points of verification before an attack can succeed in penetrating defenses. A strong password policy is yet another form of defense.

Multifactor Authentication

MFA is available in multiple forms that can be used with a variety of devices—from smartphones to personal computers—with systems from locally hosted infrastructures to the cloud and Software as a Service (SaaS). The basic premise of MFA is combining something that is known (e.g., a password) with something that is physically possessed (e.g., a smartphone, token or other device). The latter may use active directory, a hardware or software token, text or voice confirmation via mobile phone, or even biometrics.

Standards, including fast identity online (FIDO)[17] and OAuth,[18] have led to more interoperability and conformity among authentication and authorization methods. However, the chief objections to MFA continue to be both the added time and complexity required for logins, and the expense.

Zero Trust

Zero-trust network access (ZTNA) is a relatively new concept that has been gaining quite a bit of interest recently. Its premise is never trust, always verify, meaning that it eliminates implicit trust of users and devices. In so doing, it can deliver extremely granular access control along with improved scalability, reliability and flexibility.

Another differentiator for ZTNA is that it employs a user-to-application method instead of being networkcentric. This approach extrapolates security beyond the network perimeter to encompass cloud,

SaaS, data center, intravirtual machine traffic and other elements in the hybrid network. It breaks down borders and siloes to protect data wherever they exist—architecturally, geographically or within any other construct.

While sometimes thought of as a replacement for secure sockets layer (SSL) virtual private network (VPN), ZTNA can happily coexist as an overlay for the older technology and eventually replace it. ZTNA helps address the dissolving network perimeter and expands security further into hybrid cloud architectures. For users, it can be almost transparent, reducing the time and difficulty of logins. However, implementation can require a major effort, both tactically and strategically.

For those entrusted with cybersecurity, it is imperative to understand how these threats operate and why they succeed.

Strong Passwords

The use of strong passwords and the avoidance of using the same password for multiple sites or purposes are foundational to security. Among end users, the chief objection to strong passwords is typically that they cannot possibly remember them. However, password managers for businesses are affordable—typically just a few US dollars per month per user.[19]

Ironically, upper management is often the most resistant of all to the use of strong passwords.[20] The case needs to be made for accepting the minimal cost of a password manager vs. incurring the potentially enormous costs of a data breach, ransomware attack or other cyberattack.

Conclusion

Sadly, social engineering attacks will be around for the foreseeable future, as they are easy and affordable to execute and can be extremely lucrative for attackers. For those entrusted with cybersecurity, it is imperative to understand how these threats operate and why they succeed, and to take advantage of the essential security tools available to combat them.

Endnotes

1 Verizon, *2022 Data Breach Investigation Report*, USA, 2022, *https://www.verizon.com/business/resources/T39a/reports/dbir/2022-data-breach-investigations-report-dbir.pdf*
2 Bajak, F.; "Serious Breach at Uber Spotlights Hacker Social Deception," AP News, 17 September 2022, *https://apnews.com/article/technology-social-media-hacking-73a37d3f1e67ec5832ccd10a8e02c7e6*
3 *Op cit* Verizon
4 Leonhardt, M.; "'Nigerian Prince' Email Scams Still Rake in Over $700,000 a Year—Here's How to Protect Yourself," CNBC Make It, 18 April 2019, *https://www.cnbc.com/2019/04/18/nigerian-prince-scams-still-rake-in-over-700000-dollars-a-year.html*
5 iC^3 Federal Bureau of Investigation Internet Crime Complaint Center, *Internet Crime Report 2020*, USA, 2020, *https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf*
6 CompTIA, "What Is Social Engineering? The Human Element in the Technology Scam," *https://www.comptia.org/content/articles/what-is-social-engineering*
7 Dictionary.com, "Road apple," *https://www.dictionary.com/browse/road-apple*
8 Merriam-Webster, "Quid pro quo," *https://www.merriam-webster.com/dictionary/quid-pro-quo*
9 ISBuzz Staff, "Squish the Phish: Teaching Your Staff About Cyber Security to Slash Phishing Attacks, Experts Weigh In," Information Security Buzz, 17 August 2022, *https://informationsecuritybuzz.com/squish-the-phish-teaching-your-staff-about-cyber-security-to-slash-phishing-attacks-experts-weigh-in/*
10 Liu, T.; "Reducing Security Vulnerabilities in a Hybrid Workplace," *ISACA® Journal*, vol. 3, 2022, *https://www.isaca.org/archives*
11 Witts, J.; "The Top 11 Email Security Gateways," Expert Insights, 7 November 2022, *https://expertinsights.com/insights/top-11-email-security-gateways/*
12 Microsoft, "Simulate a Phishing Attack With Attack Simulation Training in Defender for Office 365," 12 October 2022, *https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training?view=o365-worldwide*

ENJOYING THIS ARTICLE?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

13 Zurier, S.; "'CSI: Phishing' Takes Gamification Approach to Improve Awareness Training." *SC Magazine*, 28 June 2022, *https://www.scmagazine.com/news/email-security/csi-phishing-takes-gamification-approach-to-improve-awareness-training*
14 Jenkins, R.; "How to Improve Training for Millennials Using Gamification," *Training Industry*, 2 August 2017, *https://trainingindustry.com/articles/learning-technologies/how-to-improve-training-for-millennials-using-gamification/*
15 Cybersecurity and Infrastructure Security Agency (CISA), "Multi-Factor Authentication Fact Sheet," USA, January 2022, *https://www.cisa.gov/sites/default/files/publications/MFA-Fact-Sheet-Jan22-508.pdf*
16 Rouse, M, "Zero Trust (ZTNA)," 15 November 2022 *https://www.techopedia.com/definition/34572/zero-trust-zt*
17 FIDO Alliance, "What Is FIDO?" *https://fidoalliance.org/what-is-fido/*
18 OAUTH, OAuth 2.0, *https://oauth.net/2/*
19 Glamoslija, K.; "Ten Best Password Managers for Businesses in 2023," Safety Detectives, 1 February 2023, *https://www.safetydetectives.com/best-password-managers/enterprise/*
20 Violino, B.; "Five Things You Need to Know About Executive Protection," *CSO*, 10 August 2017, *https://www.csoonline.com/article/2112401/infosec-staffing-the-six-things-you-need-to-know-about-executive-protection.html*