Welcome to *The Human Factor: Preventing Social Engineering Attacks as an SME*. Today we will discuss

- what social engineering is
- why it's successful
- how it can be prevented
- some difficulties in it's prevention
- and some final thoughts

So, firstly, what is social engineering? Social engineering focuses on the manipulation of human psychological factors rather than network or system vulnerabilities to extract sensitive data. In this presentation we will focus on three high-level human factors that fit this description.

The first human factor is

- Lack of knowledge and memory failure.
    - This factor tends to coincide with man-in-the-middle attacks, which trick victims into disclosing sensitive information by pretending to be a popular or trusted website.
    - This is a popular form of attack because employees, especially those in non-IT roles, don't know, or have trouble remembering, the various checks one should perform when visiting a website, such as verifying the URL, making sure the site uses HTTPS, and has an up-to-date SSL certificate.

The second human factor is

- Faulty reasoning and judgment

- This factor tends to coincide with phishing attacks, where victims are sent malicious emails asking for sensitive information. As positive email experiences over time builds trust, this habituates the email process and deten-desensitizes certain phishing characteristics, such as feigning authority to induce fear, that an attacker can take advantage of.

The third human factor is

- Casual values and attitudes about compliance
  - This factor can lead to many attacks. Physical artifact attacks is one, where a victim is given a malicious CD or USB drive that can infect their system or the company network. Another is malicious insiders, like an employee who steals company secrets to sell to the highest bidder.
  - Preexisting beliefs are the determining factor in compliance attitudes, and this presents a unique obstacle when providing training because the organization must convince the employee that their security preferences and protocols should take precedence.

So, in light of these factors, how can social engineering be prevented?

Prevention comes with the cooperation of two levels of company behaviour:

- the organization level and
- the employee level

At the organization level, companies should have

- a security-minded culture; one which prioritizes specialized training, rewards compliance with security protocols, and encourages peer accountability.
- Secondly, training should be based on the needs of the employees. Surveys and focus groups can be conducted to assess gaps in relevant knowledge which can then be applied to training programs to provide holistic security understanding at the employee level.
- Finally, a culture of follow-through encourages employees to match what they've learned in training to their behaviour on the ground. If protocols are taught but not enforced, employees have no incentive to follow them. This is an important yet nuanced aspect of safety culture that requires a strong motivation at the executive level to prioritize security practices in the workforce.

These organization-level factors should lead to employee

- motivation
- capability
- and opportunity

If the company culture expects compliance, employs tactics to reward or encourage compliance, and avoids incentivizing non-compliance in high-stress situations, then employees are more likely to comply with security protocols.

So, how might this be applied to the human factors previously outlined?

For lack of knowledge and memory failure it's important to first identify weaknesses and strengths in employees' knowledge. Surveys, questionnaires, or focus groups can facilitate the collection of this data, and influence the content of relevant training programs.

Employees should always know the how and why of what they're being asked to do. Logic is an essential factor in security compliance, so cultivating this deep understanding at the employee level can instill mindfulness and responsiveness.

It's also important to consider the learning capacity of employees by their position in the company. A data entry clerk wouldn't need the same high-level understanding as, say, the CTO; but she would need to understand her role in the security matrix.

Now, with faulty reasoning and judgment, a culture of questioning and a team-backed atmosphere are important for mitigation. Asking teammates and superiors about the authenticity of an email or phone call, and not facing punishment or admonishment for doing so, would instill a level of trust among employees and management, and could foster the desire to be more proactive about verifying unusual requests at every level.

Training and testing are also important with this factor. Employees need to know how to avoid lures sent out by malicious actors, and organizations should facilitate simulations to provide helpful feedback without admonishment. Avoiding phishing scams can be incredibly intuitive, so compassion for mistakes during simulations and training exercises should be present to reinforce a culture of questioning.

Lastly, when dealing with casual values and attitudes about compliance, research has shown that both benefits and consequences are not full-proof deterrents to non-compliance. That said, it is still important to incentivize following the rules.

Emphasizing the benefit of compliance over non-compliance should go a long way to incentivize cooperation regardless of preexisting beliefs. Following through with consequences and rewards are very important in this regard. Employees need to be able to trust what they've been told.

Of course, difficulties can arise when trying to implement a comprehensive security policy. The budget, time, and training capabilities of the organization are all factors in successful social engineering prevention and the proper balance of these factors depend on the individual circumstances of the companies themselves.

But at the employee level it is important to integrate an understanding of how low-level psychological factors can circumvent security protocols no matter the quality of training, time, and capabilities.

Low-level psychology is innate in all humans, and is completely dependent upon personality. These factors allow humans to cooperate in society and are a requirement of socialization. That means they are low-hanging fruit for malicious actors to manipulate. An employee with a high desire to be liked could be vulnerable to faking supplication, while a high level of gullibility could be vulnerable

to faking authority or inducing fear. Understanding of how these innate drives can override common sense are crucial to comprehensive social engineering prevention.

At the same time, implementation of security policies must satisfy all legal and ethical guidelines during training and simulation processes. This can actually hinder security policy implementation if measures taken to monitor employees violate their ethical and legal rights.

Companies must safeguard themselves, but not at the expense of the privacy of the individual. Device and personnel regulation must be in line with GDPR statutes, as well as ethical regulations. Spyware, excessive logging, excessively specific phishing lures, and draconian policies should be avoided.

So, in conclusion, in this presentation we have discussed the importance of social engineering in cybersecurity prevention, common human factors that can facilitate malicious attacks, how companies can promote a secure culture and provide comprehensive training, and ethical and legal considerations. I hope these topics have provided a foundation of understanding to better prevent social engineering in your company, and thank you for your kind attention.

References

Allsopp, W. (2009) *Unauthorized Access: Physical Penetration Testing for IT Security Teams*. West Sussex, UK. Wiley: 53 – 70.

Al-Darwish, A.I. and Choe, P. (2019) 'A Framework of Information Security Integrated with Human Factors'. In: *A. Moallem (ed.) HCI for Cybersecurity, Privacy, and Trust*. Orlando, FL: Springer: 217–229.

Benbasat, I., Bulgurcu, B., and Cavusoglu, H. (2010) 'Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness'. *MIS Quarterly*, 34(3): 523–548. doi:10.2307/25750690.

Butavicius, M., McCormac, A., Parsons, K., & Pattinson, M. (2015) Breaching the Human Firewall: Social Engineering in Phishing and Spear-Phishing Emails. In: *Australasian Conference on Information Systems*. Adelaide, AUS: 1 – 10

Cains, G., Henshel, D., Hoffman, B., & Kelley, T. (2015) Trust as a Human Factor in Holistic Cyber Security Risk Assessment. In: *6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015)*: 1117 – 1124.

CERT Insider Threat Center (2014) *Unintentional Insider Threats: Social Engineering*. Pittsburgh, USA. Carnegie Mellon University: 11 – 38

ENISA (2018) Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. [online] Available from: https://www.thehaguesecuritydelta.com/media/com_hsd/report/228/document/WP2018-O-3-3-2-Review-of-Behavioural-Sciences-Research-in-the-Field-of-Cybersecurity.pdf

Erkkila, J-P. (2011) Why We Fall for Phishing. In: *CHI 2011 Conference on Human Factors in Computing Systems*. Vancouver, British Columbia: 1 – 8

Esmail, S. (2015) 'eps1.1_ones-and-zer0es.mpeg', Mr. Robot. USA.

GDPR (2018) General Data Protection Regulation (GDPR). [online] General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/

Mahmood, A., Pahnila, S. and Siponen, M. (2007) '40th Hawaii International Conference on System Sciences', in. IEEE: 1–10

Malan, M.M., Mouton, F., and Venter, H.S. (2013) 'Social Engineering from a Normative Ethics Perspective'. In: *2013 Information Security for South Africa* [Preprint]. doi:10.1109/issa.2013.6641064.

Mohanakrishnan, R. (2022) Man-in-the-Middle Attack Detection and Prevention Best Practices | Spiceworks. [online] Available at: https://www.spiceworks.com/it-security/data-security/articles/man-in-the-middle-attack/

Nobles, C. (2022) 'Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem'. *HOLISTICA – Journal of Business and Public Administration*, 13(1), (49–72). doi:10.2478/hjbpa-2022-0003.

Raywood, D. (2018) Top Ten Cases of Insider Threat | Infosecurity Magazine. [online] Available at: https://www.infosecurity-magazine.com/magazine-features/top-ten-insider-threat/

Images

brgfx (n.d.) Free Vector Isolated Justice Scales Symbol on White Background | freepik.com [online] Available at: https://www.freepik.com/free-vector/isolated-justice-scales-symbol-white-background_30833713.htm#query=justice%20scale&position=0&from_view=keyword&track=ais

EasyDMARC (2021) How to Protect Against Social Engineering Attacks? [online] Available at: https://easydmarc.com/blog/how-to-spot-the-top-5-social-engineering-attacks/

ESET (2023) Social Engineering (in cybersecurity). [online] Available at: https://www.eset.com/int/social-engineering-business/

ExpressVPN (2021) The Art of Social Engineering: Are You Being Conditioned? [online] Available at: https://www.expressvpn.com/blog/the-art-of-social-engineering/

Productivity Guy (2020) Why Failure is Good for Success. [online] Available at: https://www.youtube.com/watch?v=7OueYsXsO4U

Roser, C. (2017) The Carrot and the Stick | AllAboutLean.com. [onine] Available at: https://www.allaboutlean.com/employee-motivation-1/carrot-and-stick/

Savvy Security (2022) What are Social Engineering Attacks and 5 Prevention Methods. [online] Available at: https://cheapsslsecurity.com/blog/social-engineering-attacks-and-prevention-methods/

Survey Legend (2021) 4 Types of Organizational Cultures (+ Best Culture Examples). [online] Available at: https://www.surveylegend.com/research/types-of-organizational-culture/

Tada (2021) Get to Know Employee Perks and Their Benefits for Employees. [online] Available at: https://blog.usetada.com/en/get-to-know-employee-perks-and-their-benefits-for-employees

Vantage Circle (2023) The Difference Between Teamwork and Team Building. [online] Available at; https://blog.vantagecircle.com/teamwork-and-team-building/