(EasyDMARC, 2022)

The Human Factor

Preventing Social Engineering Attacks as an SME

Topics Of Discussion

- What is social engineering?
- Why is it successful?
- How can it be prevented?
- What are some difficulties in prevention?
- Final thoughts

What is Social Engineering?

(ExpressVPN, 2021)

Social engineering focuses on the manipulation of human psychological factors rather than network or system vulnerabilities to extract sensitive data (Cains et al., 2015).

High-Level Human Factors (CERT, 2014)

- **Lack of knowledge and memory failure**
  - Tends to coincide with Man-in-the-Middle attacks (Erkkila, 2011; Mohanakrishnan, 2022)

High-Level Human Factors (CERT, 2014)

- **Lack of knowledge and memory failure**
  - Tends to coincide with Man-in-the-Middle attacks (Erkkila, 2011; Mohanakrishnan, 2022)
- **Faulty reasoning and judgment**
  - Tends to coincide with Phishing attacks (Butavicius et al., 2015)

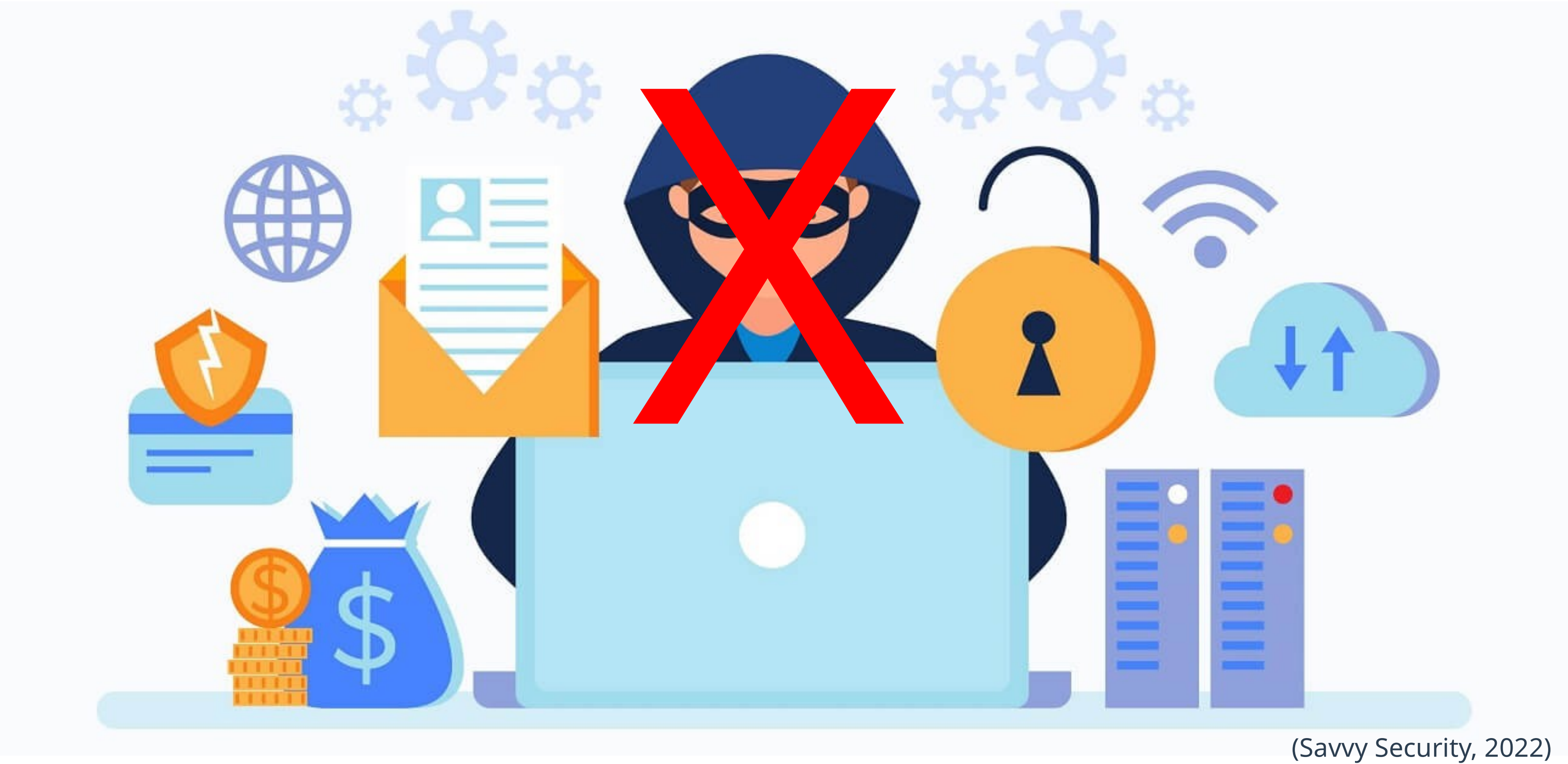
High-Level Human Factors (CERT, 2014)

- **Lack of knowledge and memory failure**
  - Tends to coincide with Man-in-the-Middle attacks (Erkkila, 2011; Mohanakrishnan, 2022)
- **Faulty reasoning and judgment**
  - Tends to coincide with Phishing attacks (Butavicius et al., 2015)
- **Casual values and attitudes about compliance**
  - Can lead to many attacks, such as physical artifact attacks or malicious insiders (Esmail, 2015; Raywood, 2018)

How Can Social Engineering Be Prevented?

(Savvy Security, 2022)

How Can Social Engineering Be Prevented?



(Savvy Security, 2022)

How Can Social Engineering Be Prevented?

(Survey Legend, 2021)

Organisation level

How Can Social Engineering Be Prevented?

(Survey Legend, 2021)

Organisation level

(Tada, 2021)

Employee level

How Can Social Engineering Be Prevented?

Culture

(Al-Darwish & Choe, 2019)

(Survey Legend, 2021)

Organisation level

(Tada, 2021)

Employee level

How Can Social Engineering Be Prevented?

Culture

(Al-Darwish & Choe, 2019)

Training

(Butavicius et al, 2015)

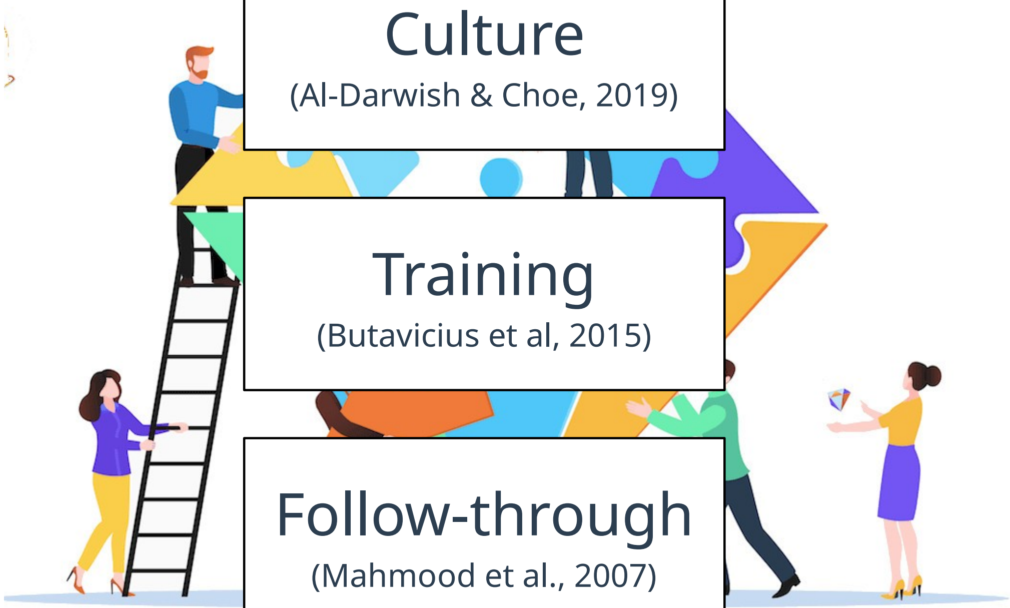
(Survey Legend, 2021)

Organisation level

(Tada, 2021)

Employee level

How Can Social Engineering Be Prevented?



Culture

(Al-Darwish & Choe, 2019)

Training

(Butavicius et al, 2015)

Follow-through

(Mahmood et al., 2007)

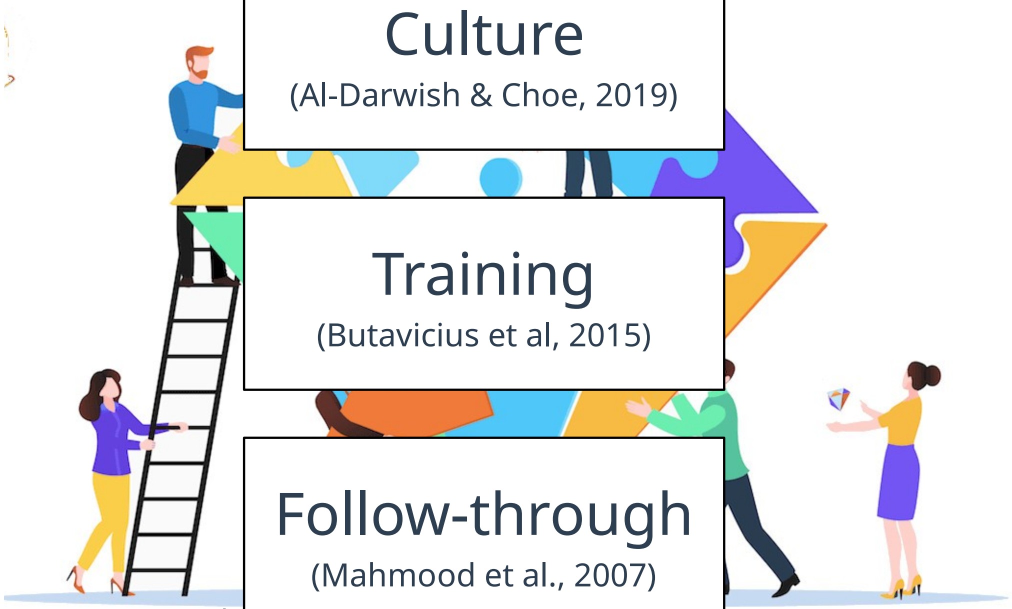
(Survey Legend,

Organisation level

(Tada, 2021)

Employee level

How Can Social Engineering Be Prevented?



Culture

(Al-Darwish & Choe, 2019)

Training

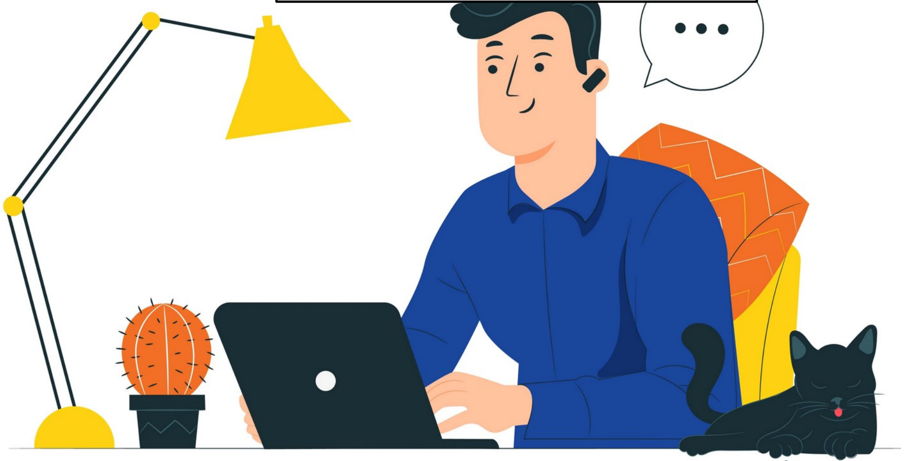
(Butavicius et al, 2015)

Follow-through

(Mahmood et al., 2007)

(Survey Legend,

Organisation level



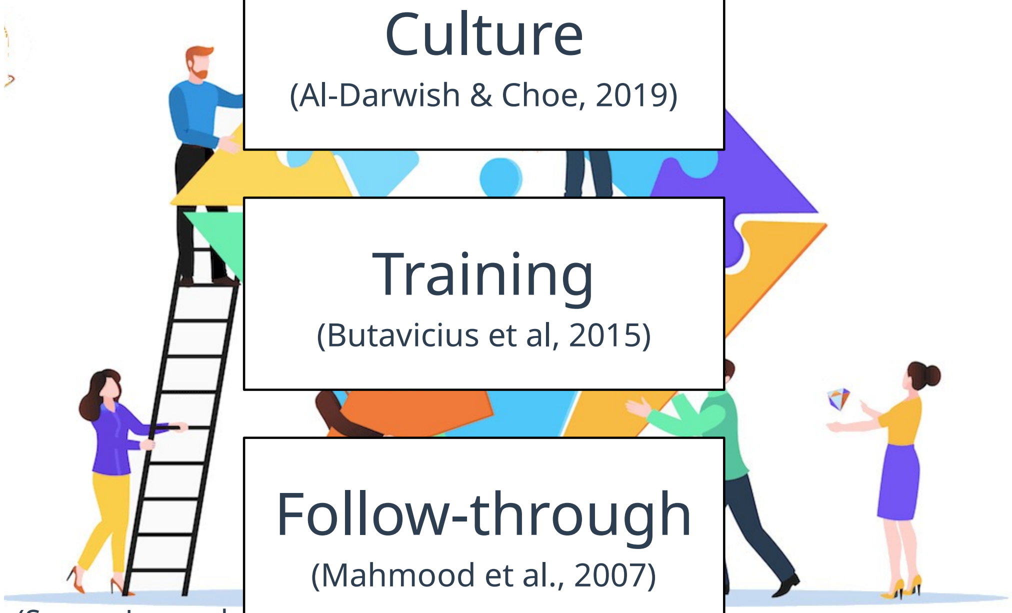
Motivation

(ENISA, 2018)

(Tada, 2021)

Employee level

How Can Social Engineering Be Prevented?



(Survey Legend,

Culture

(Al-Darwish & Choe, 2019)

Training

(Butavicius et al, 2015)

Follow-through

(Mahmood et al., 2007)

Organisation level

(Tada, 2021)

Motivation

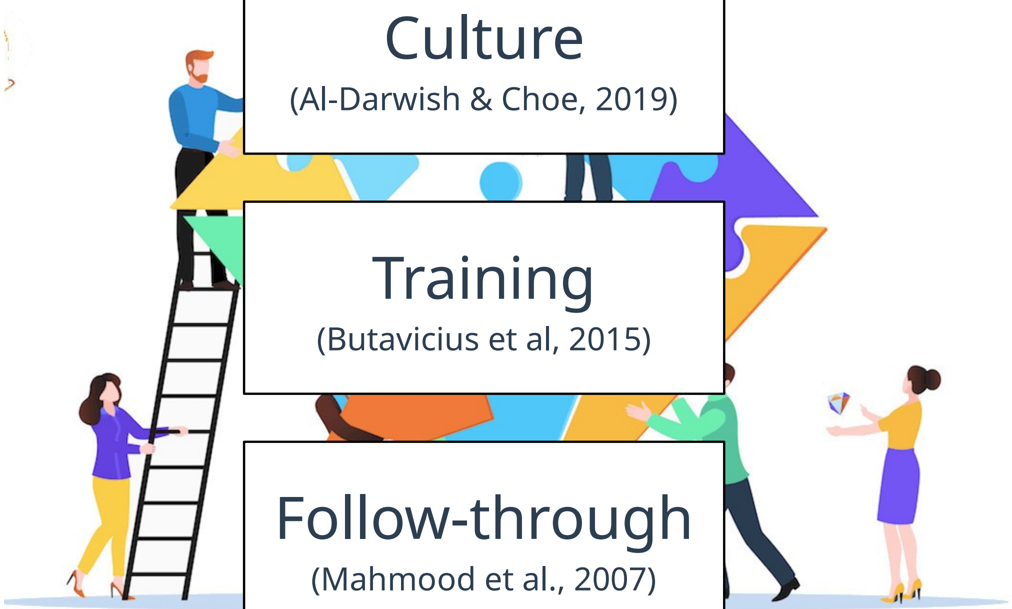
(ENISA, 2018)

Capability

(ENISA, 2018)

Employee level

How Can Social Engineering Be Prevented?



Culture

(Al-Darwish & Choe, 2019)

Training

(Butavicius et al, 2015)

Follow-through

(Mahmood et al., 2007)

(Survey Legend,

Organisation level

Motivation

(ENISA, 2018)

Capability

(ENISA, 2018)

Opportunity

(ENISA, 2018)

ada, 2021)

Employee level

Lack of Knowledge & Memory Failure (Butavicius et al., 2015; Nobles, 2022)

- Identify weaknesses and strengths in knowledge
- Identify the how and why
- Instill mindfulness and responsiveness with learning capacity in mind

Faulty Reasoning & Judgment (Butavicius et al., 2015; Cains et al., 2015; CERT, 2014; Nobles, 2022)

(Vantage Circle, 2023)

- A culture of questioning
- A team-backed atmosphere
- Training and simulations
- Trust and compassion

Casual Values & Attitudes About Compliance (Benbasat et al., 2010; Nobles, 2022; Mahmood et al., 2007)

- The carrot or the stick?
- Benefits and consequences
- Incentivize following the rules
- Follow-through culture

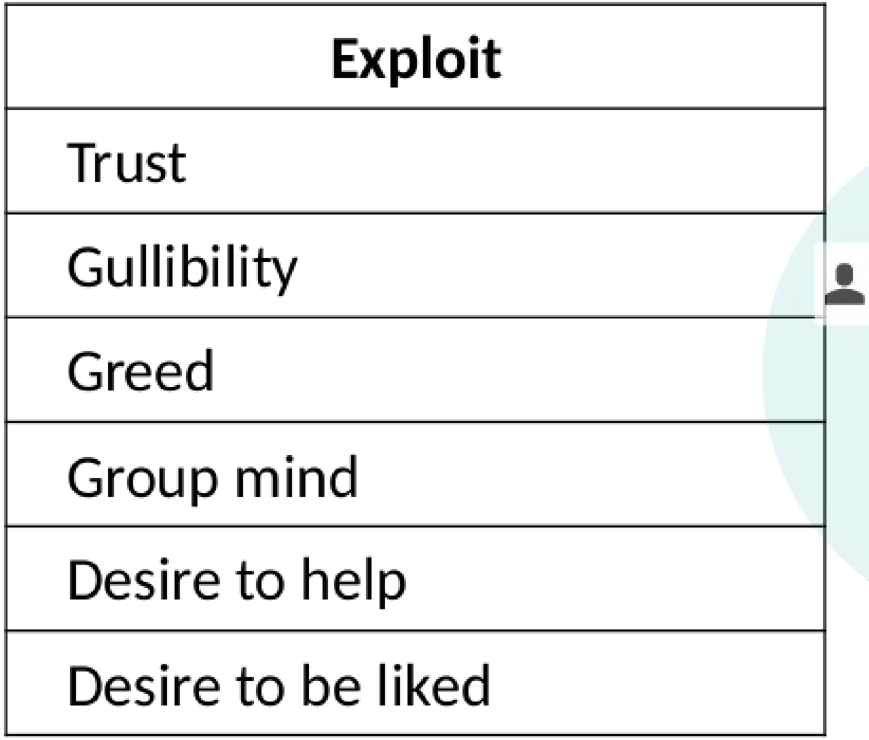
(Roser, 2017)

Difficulties in Social Engineering Prevention (Nobles, 2022)

(Productivity Guy, 2020)

Low-Level Psychology (Allsopp, 2014)

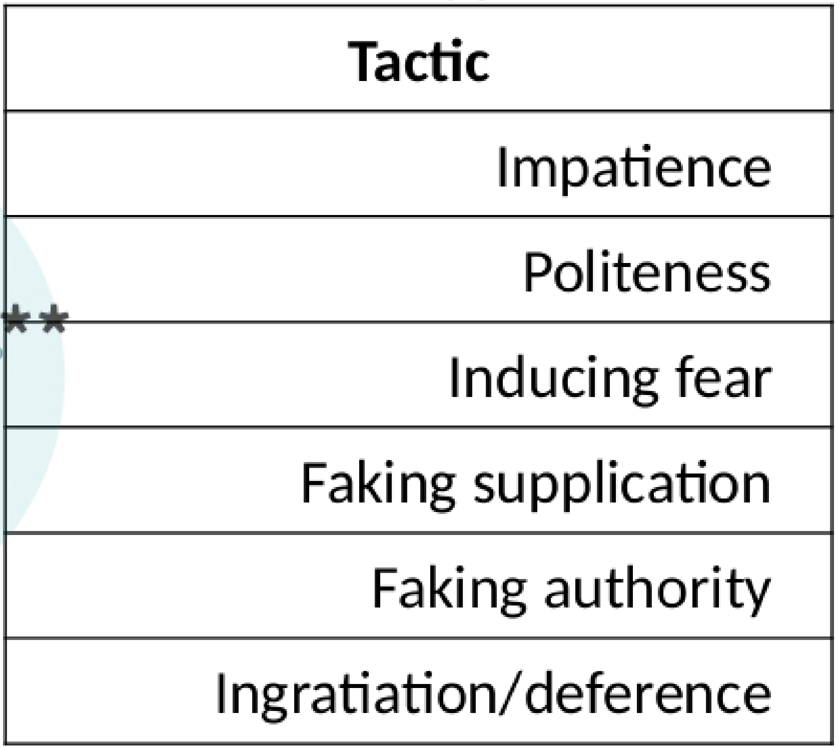
Table 1: Psychological Factors



Exploit
Trust
Gullibility
Greed
Group mind
Desire to help
Desire to be liked

(ESET, 2023)

Table 2: Tactical Approaches



Tactic
Impatience
Politeness
Inducing fear
Faking supplication
Faking authority
Ingratiation/deference

Law & Ethical Considerations (Cain et al., 2015; GDPR, 2018; Malan et al., 2013)

- Observation, privacy, and control
- Device use and restrictions
- Training, testing, and consequences

(Freepik, n.d)

Final Thoughts

Final Thoughts

- **Social engineering prevention**

Final Thoughts

- Social engineering prevention
- High-level human factors

Final Thoughts

- Social engineering prevention
- High-level human factors
- Secure culture promotion

Final Thoughts

- Social engineering prevention
- High-level human factors
- Secure culture promotion
- Legal and ethical considerations

Final Thoughts

Thank you!

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.

References

- 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/

References

- 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

Images

- 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/