A Review of Online Teaching Materials for Social Engineering

Denish O. Otieno
Department of Computer Science
Texas Tech University

Introduction

- There has been a **noticeable increase** in social engineering attack across the world.
  - Especially those that use **phishing**, **vishing**, and **smishing**, Williams et al (2022).

- **Despite** the prevalence of social engineering attacks, **education** about social engineering and how to defend against it is "**lacking"**.
  - Instead, the focus of cybersecurity education has been heavily concentrated on technical skills, Williams et al (2022).

- Recognizing the gap:
  - This presentation reviews literature in an attempt to improve social engineering education.

Social Engineering Attacks

Social Engineering Attacks

- No **person or organization** is **immune** to Social Engineering Attacks.

- The Federal Bureau of Investigation's 2020 Internet Crime Report notes that the **total financial loss** from social engineering attacks i.e.;
  - Business email compromise,
  - Phishing scams, and
  - Confidence fraud/romance scams,

- Totaled more than **$2.52 billion -** (2020 Internet Crime Report).

Social Engineering in The Education Sector

Education Sector Vulnerabilities

- Thai Nguyen and Sajal Bhatia (2020) state that **higher education institutions** are faced with an increasing **vulnerable landscape**.

- Every year there are **massive migrations** of **local**, **national**, and **international** **high school graduates**, **transfer students**, **faculty** and **employees** hire.
  - All interfacing with higher education institution information technology systems, adding hundreds to thousands of dynamic vulnerabilities.

- These individuals need to adapt to the information technology/information systems to be able to conduct their duties as students, employees or professors.

Education Sector Vulnerabilities

- Attackers are turning to social engineering tactics to **circumvent the technical securities** in place.
  - Social engineering is the deliberate act of manipulating an individual or group of individuals into giving access to confidential and unauthorized information voluntarily.

- In higher education institutions a **vulnerable landscape** of students, teachers, faculty, and staff exists.

- At times students from **high schools**, **universities**, and **colleges** **transition into employment** without receiving proper social engineering education hence **bringing human vulnerabilities** to their workstations and jobs.

Education Sector Attacks

- Professor, Nir Kshetri, a professor of management from the University of North Carolina at Greensboro, states that **cyberattacks did hit schools** and **colleges harder than any other industry** during the **pandemic**,Nir Kshetri (2021).

- In 2020 alone, including:
  - The costs of downtime,
  - Repairs and
  - Lost opportunities,
- The **average ransomware attack costed educational institutions $2.73 million**.

- That is reported to be **$300,000** more than the next-highest impacted sector (distributors and transportation companies).

Education Sector Attacks

- Nir Kshetri (2021), documents that from August 14th to September 12th, 2021.
  - Educational organizations were the **targets** of over **5.8 million malware attacks**, or **63%** of **all** such **attacks**.

- **Ransomware attacks** alone impacted **1,681 U.S. schools**, **colleges** and **universities** in **2020**.
  - Globally **44%** of **educational institutions** were targeted by such attacks.

- Individuals at every level in higher education institutions are mandated at one point to provide personal information's when entering the institution's ecosystem.

- **Attackers** merely **need** to conduct a **single** social engineering **engagement** mission on an **unprepared** higher education **institution** and gain **access** to a **treasure** trove of valuable information.

Importance of Social Engineering Awareness and Training

Importance of Social Engineering Awareness and Training

- While every year there are incremental advances in information technology/information systems products, they still **fail to secure** the **human operators**, Corradini (2020).

- Thai Nguyen and Sajal Bhatia (2020) theorizes that:
  - The lack of awareness and knowledge of social engineering tactics is the main factor in increased social engineering attacks.

- **Technical** and **non-technical** individuals do not need to understand the weaknesses in an information technology/information systems system.
  - However, they need to be aware of the tactics used by attackers.
  - In that If a person sees something suspicious, they can report.

Importance of Social Engineering Training in Non-technical Fields

- Rege and Bleiman, (2021) point out that people from **all fields** are **exposed** to social engineering attacks and,
  - Thus, people from all fields **should be trained** about it.

- However, people from **non-technical backgrounds** i.e.;
  - Languages,
  - Business, or
  - Law, etc.
- Often feel as though they do not have the skills to be involved with cybersecurity.

- Williams et al (2022), document that this thought process needs to shift,
  - So that people, **students** from **nontechnical fields graduate** into the professional world with **enough education** and **training** to **lower** their (and others') **susceptibility** of falling for social engineering attacks.

Importance of Social Engineering Training in Non-technical Fields

- Jones et al., 2021 in "**How do non experts think about cyber attack consequences?**" document that **non experts**:
- **Do not always comply** with **warning messages**, i.e.; nonexperts decide to not guard their passwords or online privacy.
  - **Do not install** system or **application updates** and do not **use encryption** or **two-factor authentication**.

- Nonexperts **do not fully understand** warning messages, especially when warning messages **use technical terms**.

- Nonexperts **do not always trust** warning messages.
  - i.e., some nonexperts **think** that **viruses** are **buggy software**.
  - Some think **attacks** only **target** those who are **wealthy** or **important**.

- Nonexperts **think compliance will cost** them,
  - i.e., **System** or application **updates** may **include updates**, which **will require** them to **relearn** how to use the software and thus make it more difficult to complete their work.
- The above builds into the importance of training and awareness for non-technical fields.

Importance of Social Engineering Training Across Education Levels

- While many **companies have advanced technical defenses**, **awareness** and **training** of social engineering is often **absent** or **lacking**, Williams et al (2022).
  - Furthermore, social engineering or awareness is often not taught in school curricula.

- The **extent** of **social engineering education** is **unclear,** and it can be logical to expect that social engineering education is **more common** in **higher education** as it is a more specialized field, Williams et al (2022).

- Even so, it is **difficult** to grow the field when students are **not being introduced** to it until they seek it out through higher education.

- Instead, social engineering education should **start** as **early** as in **K-12**.
- **Early education** would also introduce students to a field they otherwise may not have known even existed until they have **already chosen** a **career path**.

The Challenge

- There exist relatively few programs that directly teach social engineering to technical students, let alone to non-technical or multidisciplinary students, Twitchell (2006).

Sample of Proposed Social Engineering and Awareness Training Model

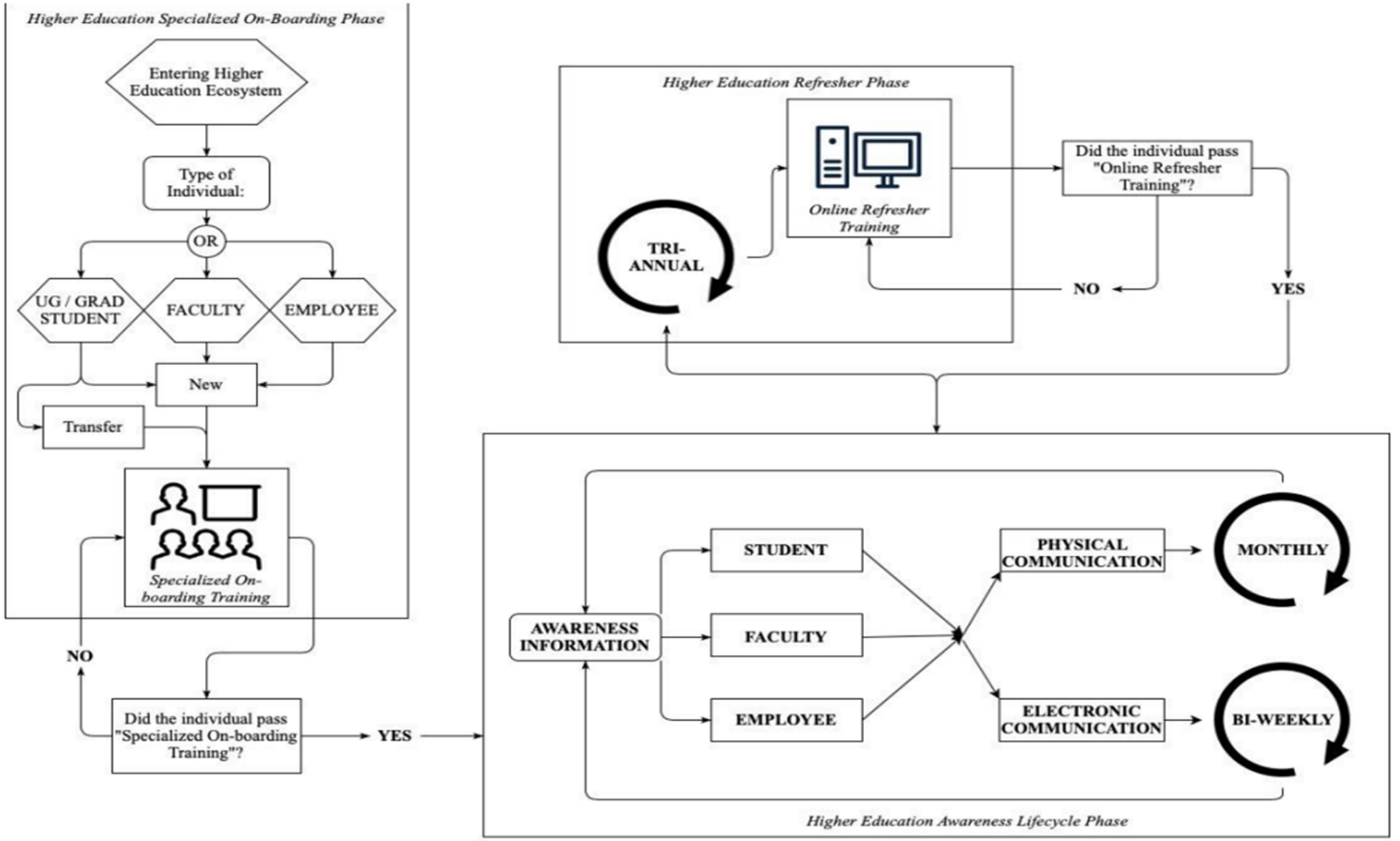
Higher Education Training Lifecycle Model

- Mohammed and Apeh (2016) present that, **schools need a model** that assists in **raising** the **awareness** about social engineering as well as provide for the:

1. **Education** of **school staff** about social engineering, its **risks**, **tactics** and **countermeasures**.

2. **Evaluation** and **measurement** of employee **susceptibility** to real-world social engineering attacks.

Higher Education Training Lifecycle Model



Thai Nguyen and Sajal Bhatia (2020)

Innovative Methods of Teaching Social Engineering

Innovative Methods of Teaching Social Engineering

- Findings reported by Bransford et al (2000) on **how people learn** and Jensen (2005) in **Teaching with the Brain in Mind**, about effective teaching and learning strategies highlight the importance of:
- Using **appropriate** just-in-time learning stimuli.
- **Engaging** students' **preconceptions** prior to teaching them new concepts.
- Providing **deep foundational** knowledge.
- Helping students make **appropriate connections** within the **context** of a conceptual framework.
- **Organizing** knowledge in ways that facilitate information **retrieval** and application.
- Allowing students **more opportunities** to define learning goals and monitor their progress in **achieving** them.

Challenges in Teaching Social Engineering.

- Balasubramanian et al. (2006), in **Innovative methods of Teaching Science and Engineering in Secondary Schools** find the following challenges to be the **most demanding** in **teaching science** and **technology** in **schools**:
- **Motivating** all students.
- **Increasing** the **cognitive skills** of **resource-deprived students**.
- **Sustaining** student **engagement**.
- **Addressing** students' **preconceptions**.
- **Creating time** to participate and **contribute effectively** during individual, teams' discussions etc.
- Promoting greater **social collaboration within** and **between teams**.
- **Resolving problems** with **group dynamics**.
- **Coping with** students' "**Been There**, **Done That**" **attitude**.
- Inducing students to **build well thought** out **designs** while **advancing** their **metacognitive skills**.
- Constantly **developing genuinely interesting challenges** and **activities**.

Online Teaching Materials for Social Engineering

Social Engineering Books

1. Learn Social Engineering: Learn the art of human hacking with an internationally renowned expert 1st Edition, Kindle Edition by Dr. Erdal Ozkaya (Author).
2. Social Engineering: The Science of Human Hacking 2nd Edition by - Christopher Hadnagy (Author).
3. Social Engineering: The Art of Human Hacking by Christopher Hadnagy (Author), Paul Wilson (Foreword).
4. Unmasking the Social Engineer: The Human Element of Security 1st Edition by Christopher Hadnagy (Author), Paul F. Kelly (Editor), Paul Ekman (Foreword).
5. Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails by Christopher Hadnagy (Author).
6. Social Engineering in IT Security: Tools, Tactics, and Techniques 1st Edition by Sharon Conheady (Author)
7. No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing by Johnny Long (Author), Kevin D. Mitnick (Series Editor).
8. Low Tech Hacking: Street Smarts for Security Professionals by Jack Wiles (Author), Terry Gudaitis (Author), Jennifer Jabbusch (Author), Russ Rogers (Author), Sean Lowther (Author).
9. The Art of Deception: Controlling the Human Element of Security by William L. Simon (Author), Kevin D. Mitnick (Author), Steve Wozniak (Foreword).
10. The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data by Kevin Mitnick (Author).
11. The Social Engineer's Playbook: A Practical Guide to Pretexting by Jeremiah Talamantes (Author).
12. Hacking the Human: Social Engineering Techniques and Security Countermeasures by Ian Mann.
13. Human Hacking: Win Friends, Influence People, and Leave Them Better Off for Having Met You by Christopher Hadnagy (Author), Seth Schulman (Author)
14. Cybersecurity: An Essential Guide to Computer and Cyber Security for Beginners, Including Ethical Hacking, Risk Assessment, Social Engineering, Attack and Defense Strategies, and Cyberwarfare by Lester Evans (Author).
15. Hacking for Beginners: A Step by Step Guide to Learn How to Hack Websites, Smartphones, Wireless Networks, Work with Social Engineering, Complete a Penetration Test, and Keep Your Computer Safe by Julian James McKinnon (Author).
16. A Gentle Introduction to Social Engineering Attack and Prevention by Stephen Haunts (Author).

Social Engineering Books

1. Social Engineering: The Art of Deception, Psychological Warfare, and Mind Manipulation by Steve Smith (Author).
2. Cybersecurity: A Simple Beginner's Guide to Cybersecurity, Computer Networks and Protecting Oneself from Hacking in the Form of Phishing, Malware, Ransomware, and Social Engineering by Quinn Kiser (Author).
3. How to Hack a Human: Cybersecurity for the Mind by Raef Meeuwisse (Author), Marina Meeuwisse (Foreword).
4. Practical Social Engineering: A Primer for the Ethical Hacker by Joe Gray (Author).
5. Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks by Tim Rains (Author).
6. Social Engineering Theory and Practice: Exposing the reality of Government manipulating their citizens by Mr. Mark R. Blum (Author).
7. Cybercrime through Social Engineering: The New Global Crisis by Christopher S. Kayser (Author).
8. Tavistock Institute: Social Engineering the Masses by Daniel Estulin PhD (Author).
9. Computer Networking Beginners Guide: An Easy Approach to Learning Wireless Technology, Social Engineering, Security and Hacking Network, Communications Systems (Including CISCO, CCNA and CCENT) by Russell Scott (Author).
10. Social Engineering and Nonverbal Behavior Set 1st Edition by Christopher Hadnagy (Author).
11. Social Engineering Penetration Testing: Executing Social Engineering Pen Tests, Assessments and Defense 1st Edition by Gavin Watson (Author), Andrew Mason (Author), Richard Ackroyd (Author).
12. Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats 1st Edition by Bill Gardner (Author), Valerie Thomas (Author).
13. Social Engineering - The Science of Influence by Yossi Dahan (Author).
14. Ethical Hacking: The Ultimate Guide to Using Penetration Testing to Audit and Improve the Cybersecurity of Computer Networks for Beginners, Including Tips on Social Engineering by Lester Evans (Author).
15. Understanding Social Engineering Based Scams 1st ed. 2016 Edition by Markus Jakobsson (Editor).
16. Cybersecurity: What YOU Need to Know about Cybersecurity, Ethical Hacking, Risk Assessment, Social Engineering & How to DEFEND YOURSELF from Attacks by Ralph Voss.

Online Courses

1. Learn Social Engineering From Scratch: https://www.udemy.com/course/learn-social-engineering-from-scratch/
2. Social Engineering | Cybrary
3. Lesson 3 – Social Engineering: The Oldest Hack | Teaching Security
4. Course Projects – CARE Lab: Cybersecurity in Application, Research & Education Laboratory (temple.edu)
5. The Complete Social Engineering, Phishing, OSINT & Malware: https://www.udemy.com/course/learn-malware-social-engineering-and-osint-for-hacking/
6. Learn Social Engineering & Open-source Intelligence (OSINT): https://www.udemy.com/course/hack-people-instead-of-systems-social-engineering-basics/
7. Social Engineering: 13 Social Engineering attacks explained!: https://www.udemy.com/course/social-engineering-for-absolute-beginners/
8. Anti Phishing and Email Security Training: https://www.udemy.com/course/organisational-email-security-staff-training/
9. Social Engineering Expert (Full-course): https://www.udemy.com/course/social-engineering-expert-full-course/
10. Cyber Security Social Engineering - Hacking Human Firewalls: https://www.udemy.com/course/cyber-security-social-engineering-hacking-human-firewalls/
11. Complete Cybersecurity Bootcamp: https://zerotomastery.io/courses/learn-cybersecurity-bootcamp/
12. Ethical Hacking: Social Engineering: https://www.pluralsight.com/courses/ethical-hacking-social-engineering
13. Security Awareness Training: https://www.coursera.org/learn/security-awareness-training?irclickid=3-Dzv0SWxxyNROLw36W9MwuAUkASeM3y0zJ90w0&irgwc=1&utm_medium=partners&utm_source=impact&utm_campaign=3408194&utm_content=b2c
14. Cybersecurity in Healthcare (Hospitals & Care Centres): https://www.coursera.org/learn/cybersecurity-in-healthcare?irclickid=3-Dzv0SWxxyNROLw36W9MwuAUkASeMWa0zJ90w0&irgwc=1&utm_medium=partners&utm_source=impact&utm_campaign=3408194&utm_content=b2c
15. Ethical Hacking: Social Engineering: https://www.linkedin.com/learning/ethical-hacking-social-engineering?src=aff-ref&trk=aff-ir_progid.8005_partid.3408194_sid._adid.449670&clickid=Ti8XYhV-JxyNTPGUCT1Qm1WmUkASeJ0a0zJ90w0&mcid=6851962469594763264&irgwc=1
16. Cybersecurity Awareness: Social Engineering: https://www.linkedin.com/learning/cybersecurity-awareness-social-engineering-14308872?src=aff-ref&trk=aff-ir_progid.8005_partid.3408194_sid._adid.449670&clickid=Ti8XYhV-JxyNTPGUCT1Qm1WmUkASeJwT0zJ90w0&mcid=6851962469594763264&irgwc=1

References

1. Jones, K. S., Lodinger, N. R., Widlus, B. P., Siami Namin, A., Maw, E., & Armstrong, M. E. (2022). How do non experts think about cyber attack consequences?. Information & Computer Security, 30(4), 473-489.
2. K. Williams, R. Bleiman and A. Rege, "Educating educators on social engineering Experiences developing and implementing a social engineering workshop for all education levels," 2022 IEEE Integrated STEM Education Conference (ISEC), Princeton, NJ, USA, 2022, pp. 188-194, doi: 10.1109/ISEC54952.2022.10025154.
3. 2020 Internet Crime Report", January 2020, [online] Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
4. Nguyen, T., & Bhatia, S. (2020, December). Higher education social engineering attack scenario, awareness & training model. In Journal of The Colloquium for Information Systems Security Education (Vol. 8, No. 1, pp. 8-8).
5. Corradini, I. (2020). *Building a cybersecurity culture in organizations* (Vol. 284). Berlin/Heidelberg, Germany: Springer International Publishing.
6. Rege, A., & Bleiman, R. (2021, December). Collegiate Social Engineering Capture the Flag Competition. In *2021 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 1-11). IEEE.
7. Mohammed, S., & Apeh, E. (2016, December). A model for social engineering awareness program for schools. In *2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)* (pp. 392-397). IEEE.
8. Twitchell, D. P. (2006, September). Social engineering in information assurance curricula. In Proceedings of the 3rd annual conference on Information security curriculum development (pp. 191-193).
9. Nir Kshetri (2021, September). Cybercriminals use pandemic to attack schools and colleges. In GCN The Technology Transforming State and Local Government, [online] Available: https://gcn.com/cybersecurity/2021/09/cybercriminals-use-pandemic-to-attack-schools-and-colleges/316131/
10. Bransford, J. D., Brown, A. L., & Cocking, R. R. (2000). How People Learn: Brain, Mind, Experience, and School. Washington DC: National Academy Press.
11. Jensen, E. (2005). Teaching with the brain in mind. ASCD.