Cybersecurity Career Paper: Security Awareness Training Specialist

In today's ever changing digital landscape one of the most vital roles in the cybersecurity department is security awareness training specialist. These professionals specialize in everything online training and are responsible for designing and implementing training programs that educate and entice employees and the general public about safe online practices. Unlike technical cybersecurity roles focused on software and infrastructure this career relies on social science principles to influence human behavior and decision-making. These specialists must understand the technical side of cybersecurity but more importantly they must understand how people think, learn, react, and respond to risk. These core traits are the reasons people fall for online attacks in the first place and understanding them is pivotal to effective training.

Integration of Social Science Principals

Everyone hates sitting through boring yearly training and this role needs to understand that and work to make annual or monthly training fun and enticing. I think a good example of this is the Cyber Awareness Challenge that is put on by the DOD. If you haven't had the luxury of being required to take the Cyber Awareness Challenge its about an hour long game that trains you on the DOD cybersecurity information. I think internal security awareness training specialists should be able to create and administer training that is a little better than death by powerpoint. They have to take into account people's attention spans, cognitive biases, habits, and loss aversion, all things critical for important cybersecurity training. Understanding people's habits is probably one of the biggest things required for good training, something as easy and nice as holding the door for someone may have to get trained on depending on the company's policy for scanning into a building. They must also take into account employees not understanding what is at stake, they may see a phishing email as a joke but unknowingly clicking or downloading something from these emails could put entire systems at risk. Most importantly the training specialist must understand people's attention span and time value. Like I said previously no one wants to sit through long boring training sessions, so understanding that and tailoring the courses accordingly is important.

Application of Key Class Concepts

Several key class concepts are directly applicable to these careers. First, the idea that human factors in cybersecurity play a much bigger role than machines in the security system. Secondly, social engineering is the biggest cyber risk in the world and is happening all around us all the time. Everyone is susceptible to social engineering no matter how technically inclined you are. Third, Cultural relevance is important to understand especially if you are working with a multinational organization, understanding people's background can help you determine how private they may keep themselves online and how susceptible they may be to a phishing attack.

Relationship to Society

This role becomes the bridge between technical cybersecurity and the everyday person allowing normal employees or people to understand why certain things have to be done and protections have to be in place. Using real world examples and bringing threats close to home is the most effective way to educate the public on how important cybersecurity is. The DOD has been putting millions of dollars towards updating the United States cybersecurity defense and it's long overdue. The digital world is dangerous and without effective training people such as the elderly or under privileged may fall behind. This is why constant education is the only way to curb social cyber threats.

Conclusion

The Security Awareness Training Specialist serves as a powerful force in educating employees and the public about ongoing cyber techniques and threats. By using technical knowledge they can provide effective and enticing education to build trust and increase resilience not just within organizations but across society. They play a huge role in ensuring that cybersecurity is not just a technical endeavor, but a human-centered mission that reflects the diversity of the people it involves.

References

Beu, N., Jayatilaka, A., Zahedi, M., Babar, M. A., Hartley, L., Lewinsmith, W., & Baetu, I. (2023). Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation. Computers & Security, 131, 103313. https://doi.org/10.1016/j.cose.2023.103313

Defense Security Cooperation Agency. (n.d.). *Cyber Awareness Challenge DS-IA106.06* [Online training course]. Center for Development of Security Excellence. Retrieved August 5, 2025, from https://www.cdse.edu/Training/eLearning/DS-IA106/ cdse.edu+6

The importance of cybersecurity education in school. International Journal of Advanced Research in Engineering and Technology (IJARET), 11(6), 226–233. https://d1wqtxts1xzle7.cloudfront.net/63758855/1393-JR41920200627-85760-wvnlow-libre.pdf

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K.-K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security, 119, 102754. https://doi.org/10.1016/j.cose.2022.102754