Corey Stokes

11/16/2025

Security Awareness and Training Specialist

Introduction

The cybersecurity profession plays a central role in protecting organizations, individuals, and society from constantly evolving digital threats. In today's modern world, cybersecurity is not only technical but deeply human, as many risks are from human behavior, decision making patterns, and social structures. This paper discusses the career of a Security Awareness and Training Specialist and explores how social science principles shape their daily work. I will discuss key course concepts applied in this career, the profession's interactions with marginalized groups, and how this cybersecurity role contributes to society.

Social Science Principles

Social science principles form the basis of understanding how human behavior promotes cybersecurity vulnerabilities. Research from psychology helps explain motivations behind hacking, employee decision making, and how people respond to digital risks. For example, studies on risk perception show that people underestimate cyber threats because they are invisible and abstract. Data from human computer interaction research is also very important; for instance, it shows how mistakes occur because interfaces are confusing or there is cognitive overload, such as clicking a phishing link.

Corey Stokes

11/16/2025

Security Awareness and Training Specialist

In the Security Awareness and Training Specialist role, these social science insights are integrated directly into cybersecurity practices. Specialists use behavioral psychology in order to design training that effectively changes employee habits through repetition, incentives, nudges, and timely reminders (van Steen et al., 2025). They use knowledge in principles of communication, sociology, and organizational behavior to mold the culture at work and to increase cooperation with security policies.

Professionals use social science methodologies, including user behavior analysis, surveys, focus groups, and interviews, among others, to establish a cybersecurity awareness or education strategy. These strategies depend on understanding emotions, attention span, and social influence—each of which comes from social science research.

Application of Key Concepts

Several major class concepts directly influence this cybersecurity role. First, incentives and misaligned incentives play a significant part in employee behavior. The Security Awareness Specialist identifies situations where secure practices feel inconvenient and coordinates with technical teams to reduce the “cost” of doing the right thing. Second, there is risk perception. Specialists design simulations and case studies that make cyber threats real and relevant to employees so they can correctly perceive risk. Social engineering concepts are the guidelines for training modules. Experts explain to employees how hackers take advantage of confidence, authority, and feelings to manipulate them. Fourth, cost benefit analysis informs how training programs are evaluated. Organizations invest in awareness programs because the potential

benefit of reduced breaches outweighs the cost of training sessions. These professionals also use tools like phishing simulations, scenario based lessons, and compliance checklists that apply these concepts to real life.

Marginalization

Cybersecurity disproportionately impacts marginalized groups. Research has shown that women, people of color, LGBTQ+ individuals, and people with disabilities are disproportionately impacted by rates of cyber harassment, identity based threats, and surveillance harms (UN Women, 2025). Security Awareness Specialists must understand such disparities in developing training and policies. The following career addresses three major challenges associated with marginalized groups. Unequal digital access can make training harder for those with less prior experience. Accessibility barriers, such as training materials that are not readable by screen readers or that assume a high literacy level. Professionals in this field help reduce these challenges by creating inclusive training, ensuring accessibility, and participating in initiatives aimed at equitable digital protection across the workplace.

Conclusion

It is a career that binds cybersecurity and social science together. Professionals in the field of Security Awareness and Training Specialists utilize psychological principles, sociological insights, and human centered research methods to design effective training programs. They apply key class concepts of incentives, risk perception, and social engineering to

strengthen organizational security. It also ensures digital fairness and works toward protecting marginalized groups. Overall, it is a crucial profession for both organizational safety and the well being of society.

References

Merritt, M., et al. (2024). NIST SP 800-50r1: Building a cybersecurity and privacy learning program. National Institute of Standards and Technology.

UN Women. (2025). Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women: FAQs.

van Steen, T., Khadka, K., & Patel, S. (2025). Driving behaviour change with cybersecurity awareness: Developing a behavioural cybersecurity strategy. Journal of Cybersecurity, 11(2).