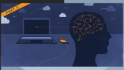
10 Steps
The Integrated Model of the Interdisciplinary Process By: John Peck

STEP 1

Define the problem/state research question

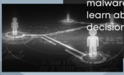
This step involves identifying the gaps in knowledge or understanding that can be addressed through interdisciplinary research. A example of this that relates to Cybersecurity is "How do social engineering techniques exploit human vulnerabilities to gain unauthorized access to computer systems?"



STEP 2

Justify using an interdisciplinary approach

Learn as much as you can about the relevant fields that can help solve the research problem. Learn the main ideas, theories, methods, and approaches that are used in each discipline. I need to comprehend the technical elements of cybersecurity, such as network protocols, encryption algorithms, and malware detection, gain an understanding of computer science. Also I need to learn about psychology to better understand how people behave and make decisions related to cybersecurity.



STEP 3

Identify relevant disciplines

Familiarize with the relevant disciplines that can contribute to addressing the research problem. Gain an understanding of the key concepts, theories, methodologies, and approaches within each discipline. I will analyze the research problem using the lenses of computer science, psychology, and social sciences. This interdisciplinary approach allows me to understand both technical vulnerabilities and the psychological manipulation used in social engineering attacks.

STEP 4

Conduct the literature search

Identify and define the key terms and concepts that are used across the selected disciplines. Establish a common language to facilitate communication and understanding between different disciplinary perspectives. For example, ensuring that terms like "phishing," "malware," and "social engineering" are understood by both technical and non-technical people.

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1

STEP 5

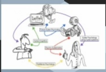
Develop adequacy in each relevant discipline

Explore existing interdisciplinary theories, frameworks, or models that can guide research process. These theories will provide a foundation for integrating different disciplinary perspectives. To develop adequacy in the discipline of cybersecurity, you need solid foundation of knowledge and skills by studying core concepts, following industry standards, certifications which I have. Additionally, actively participate in cybersecurity communities, collaborate with professionals from related fields, and stay informed about ethical considerations and legal frameworks. I could also goto a psychologic facility to learn more about what they do.

STEP 6

Analyze the problem and evaluate each theory

This step aims to understand the underlying concepts, assumptions, and methodologies of each theory within its respective discipline. I can gain insights from multiple disciplines and develop a more in depth understanding of the research problem in Cyber.



STEP 7

Identify conflict between insights and their sources

Conflicts can arise between different insights and their respective disciplinary sources. These conflicts can occur due to variations in theoretical perspectives, methodologies, assumptions, or even conflicting empirical findings. Technical insights from cybersecurity may focus on system vulnerabilities, network protocols, and encryption algorithms, while psychological insights may emphasize human behavior and decision-making processes. Conflicts can arise when technical solutions overlook psychological factors or when psychological insights disregard technical vulnerabilities.

STEP 8

Create common ground between insights

This step try to look for areas of shared understanding among the conflicting insights. Identify concepts, themes, or findings that align across disciplines, even if there are disagreements on certain aspects. This can help build a foundation for integrating insights I can collaborate with cybersecurity and psychologists to collect and analyze data.

STEP 9

Construct a more comprehensive understanding

To construct a comprehensive understanding in interdisciplinary research, integrate key insights from multiple disciplines, bridge disciplinary gaps, and synthesize concepts and theories, while validating and refining the understanding through interdisciplinary collaboration and communication. Integrate data and insights from technical and psychological analyses to understand the interplay between technical vulnerabilities and human factors in cybersecurity.

STEP 10

Reflect on, test, and communicate the understanding

Share research findings through academic papers, presentations, and industry collaborations. Provide recommendations for designing user-aware security systems, educating users about social engineering risks, and implementing technical controls to mitigate cyber threats.