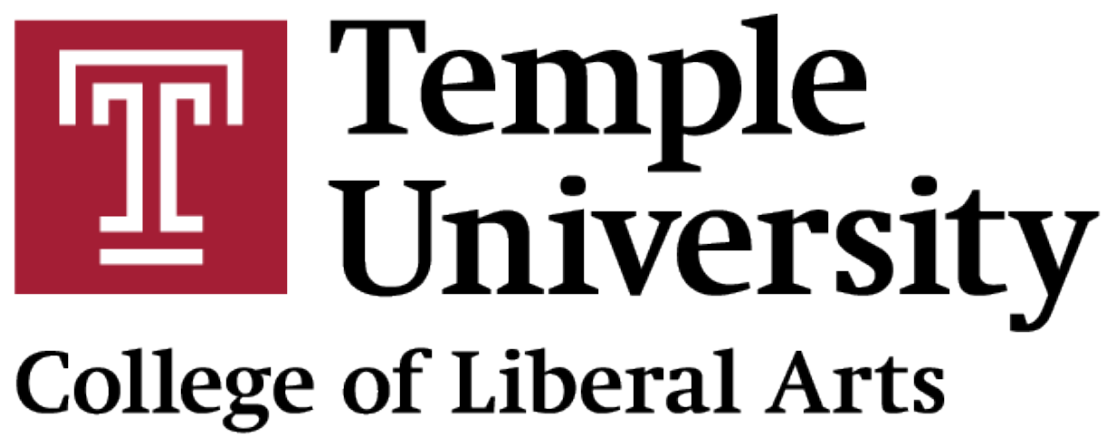


SaTC: EDU: Educating STEM Students and Teachers about the Relevance of Social Engineering in Cyberattacks and Cybersecurity



Cybersecurity in Application, Research and Education Lab

Aunshul Rege
rege@temple.edu
Award: 2032292



Challenge

- In 2020, 85% of breaches involved the human element and 36% of breaches involved phishing, a form of Social Engineering (SE), up 11% more the previous year
- SE attacks can result in damages ranging from \$25,000 to multi-million dollars for direct financial loss, recovery cost, productivity loss, It can also result in reputation damage
- Despite the relevance of the human factor and substantial loss resulting from its exploitation in cyberattacks, the cybersecurity curriculum does not focus on SE

Solution

- Educate students via SE Capture the Flag (SECTF) competitions & hands-on course projects for classrooms
- Educate the educators via free workshops
- Disseminate free resources for research and education

Scientific Impact

- Improve cybersecurity training that goes beyond purely technical learning to ensure the inclusivity of all STEM fields
- Generate new curricula and methods of instruction, emphasizing the relevance of the human factor in cybersecurity
- Foster partnerships between SE experts, social scientists, industry, government, and non-profits

NICE Framework Success Story

The NICE Framework Success Story document details the development of the NICE Framework for Cybersecurity, its organizational profile, project drivers, and success metrics. It highlights the framework's focus on social engineering and its impact on cybersecurity education and workforce development.

Broader Impact

- Train next generation cybersecurity workforce
- Understand adversarial mindset
- Best defense is good offense
- Educate the educators via workshops, course projects, repositories, analytical frameworks, and webinars
- Improve diversity in the cybersecurity workforce

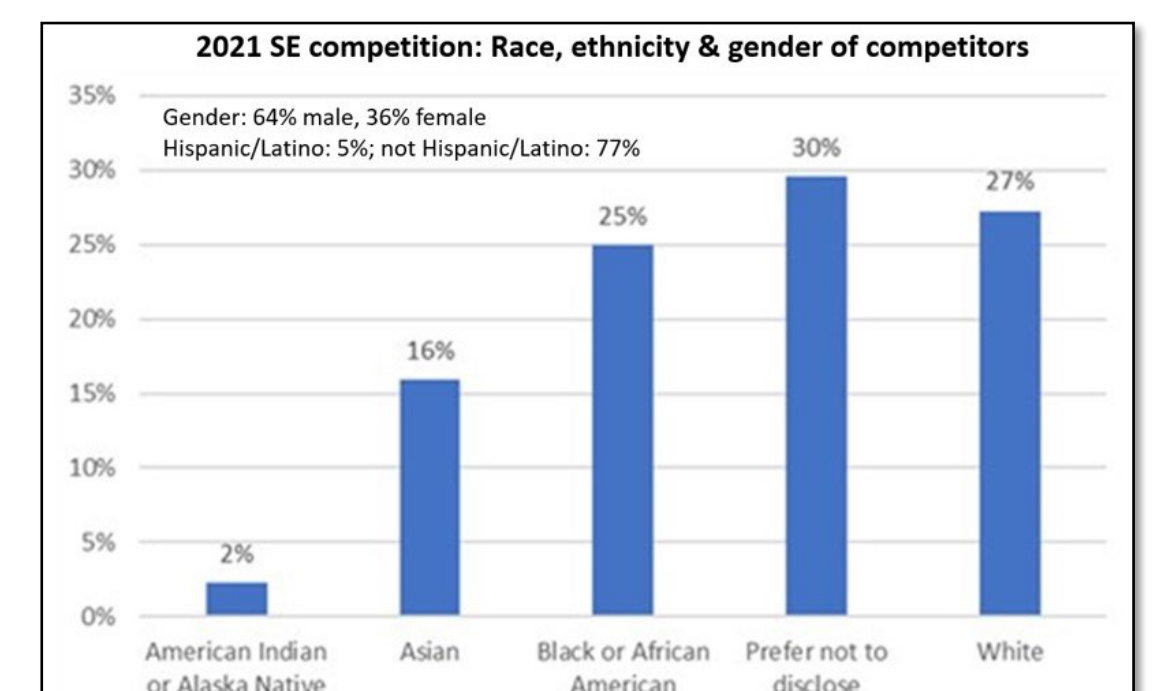
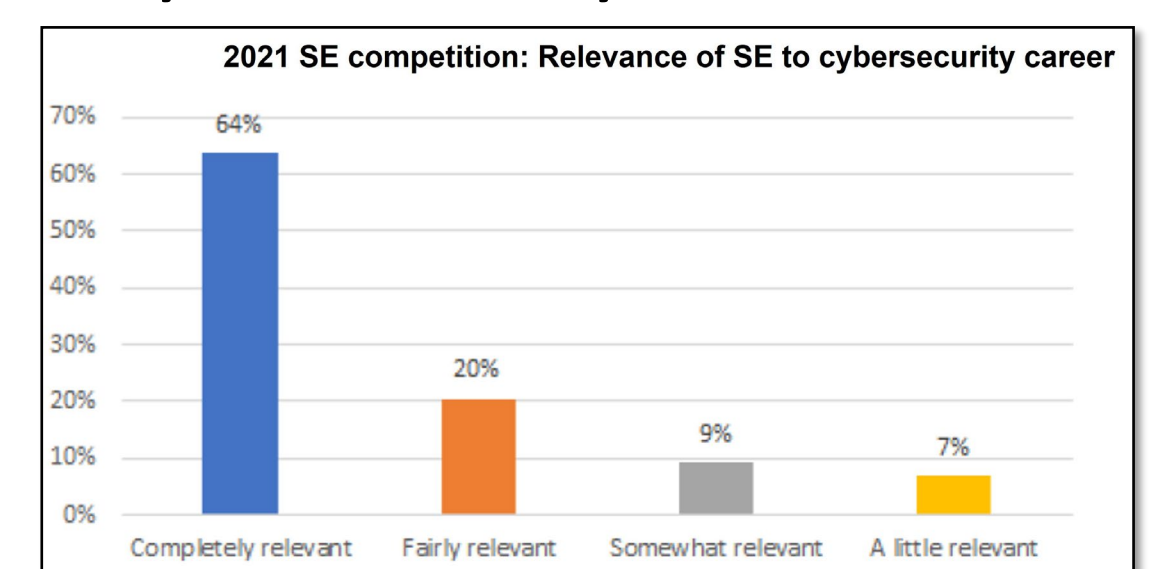
"It doesn't matter how much we are hardening our technical systems. If we still haven't [addressed the] human element... then the system will still be weak.

You learn how to do the offense, and when you learn that, you learn about the defense, and you learn that people are susceptible to [SE]."

- 2020 CollegiateSECTF Participant

"As social engineering attacks continue becoming more pervasive domestically and globally, it is critical that individuals receive proper training and education to guard against such attacks. Attending a workshop focused on social engineering is, I believe, the perfect way to begin elevating the effectiveness of how we recognize, teach, and respond to social engineering attacks."

- High school educator



2021 SOCIAL ENGINEERING PEN TESTING COMPETITION WINNERS

- High School: 1st place! VIMSIA Volts
- Undergraduate: 1st place! RCC Cyber Hawks (SUNY Rockland)
- Graduate: 1st place! Trust Us (NYU Tandon School Eng.)
- Undergraduate: 2nd place! Iridescent (University of Virginia)
- Graduate: 2nd place! Team Tay (Abertay University)
- Undergraduate: 3rd place! Night Owls (Temple University)
- Graduate: 3rd place! Tell Me Lies (Excelsior College)

FUNDERS AND SPONSORS: Google, NSF, etc.

Learn more

Event	URL
Summer SE event	https://sites.temple.edu/socialengineering/
Collegiate SECTF	https://sites.temple.edu/collegiatesectf/
SE educator workshops	https://sites.temple.edu/care/educator-workshop/
Downloadable resources	https://sites.temple.edu/care/resources/

