Temple University
College of Liberal Arts

Cybersecurity in
Application, Research
and Education Lab

2025 SOCIAL ENGINEERING EVENT

Engage with us at the Social Engineering (SE) Event!

WHY JOIN US?

Help students understand the **relevance of the human factor and the role of social engineering** in cyberattacks and cybersecurity! Engaging in this international virtual event will help develop a well-rounded next generation workforce that takes a holistic approach to cybersecurity.

WHY DOES SE MATTER?

Social engineering (SE) is a technique used by cybercriminals to psychologically manipulate individuals into disclosing sensitive information (passwords) and providing unauthorized access (downloading and executing malware files). SE is used in an assortment of cybercrimes, such as ransomware, scams and frauds, disinformation, etc., and causes numerous harms such as financial loss, recovery and productivity costs, disruption to operations, and loss of reputation. Despite its relevance, SE is downplayed in cybersecurity training and education.

It can be hard to practice SE on someone or an organization as it involves ethical and legal issues. The SE event allows students to experience SE in a safe and ethical way.

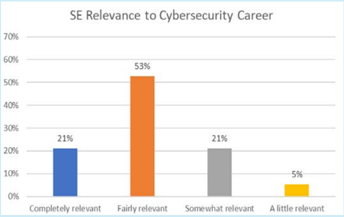
WHO IS THE AUDIENCE?

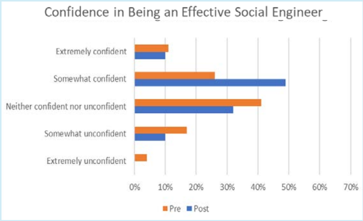
High school, undergraduate and graduate students.

For more information about supporting about supporting the SE event, please contact care@temple.edu or visit sites.temple.edu/care

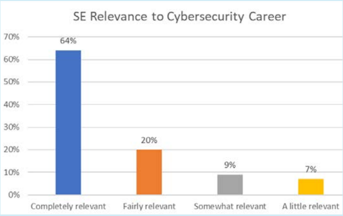
PAST YEARS' ATTENDEE STATS

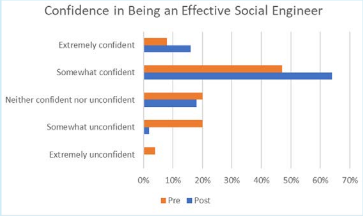
2021



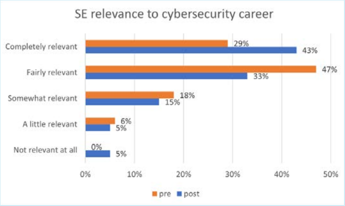


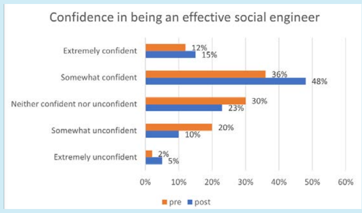
2022





2023





2025 SE COMPETITION THEME:

CRITICAL INFRASTRUCTURE AND SOCIAL ENGINEERING

Critical infrastructure (CI) are systems that are so vital to our society that their incapacitation or destruction would have a debilitating impact on national security, economic stability, public health, safety, or everyday operations. Social engineering (SE) attacks can help cybercriminals gain access to these systems and sensitive data, thereby posing a grave threat to CI.

Temple University's Cybersecurity in Application, Research & Education (CARE) Lab is challenging full-time high school and college students (aged 14+) to gain first-hand cyberattack and cybersecurity experience by participating in a creative and unique virtual SE event!

NO CYBERSECURITY EXPERIENCE IS REQUIRED. All disciplinary backgrounds are welcome!

PREMISE: The CARE Lab has been brought in to help a local critical infrastructure that has been hit with a cyberattack. Your team will serve as a CARE Lab representative and engage with victims to develop an attack playbook using the ATT&CK framework, identify the point of entry, and ascertain the role and extent of SE in the attack. Students will write formal reports and present their findings on the many ways SE manifests specific to the case study, and more generally, and make recommendations on how best to protect CI from these attacks.

COMPETITION DATES (ALL VIRTUAL)

Orientation: TBD

Live event: Fridays, Saturdays, and Sundays

9am - 4pm ET

Graduate: TBD |

Undergraduate: TBD | High school: TBD

Closing ceremonies: TBD

REGISTRATION

Applications NOW open! Register your team by TBD

https://sites.temple.edu/socialengineering/register/

PRIZES FOR EACH TRACK

1st: $3,000

2nd: $2,000

3rd: $1,000

TEAM SUBMISSION REQUIREMENTS

1. Team Name
2. Institution Name
3. Team details: number of members, full names, email addresses, profile photos, short bios
4. Faculty advisor details: full name, email address

5 30 second PSA video on CI (any sector) cyberattacks and SE. Click here to see sample PSAs

PARTICIPATION REQUIREMENTS

1. Parental permission (if under age 18)
2. Code of conduct waiver (agree not to cheat)
3. Media consent waiver (generated audio/visual content can be shared publicly)
4. Pre- and post-event survey

SPONSORSHIP TIERS

THROUGHOUT EVENT	***Bronze $5K****	***Silver $10K*****	***Gold $20K******	***Platinum: $50K******
Logo on website	●	●	●	●
Social media recognition	●	●	●	●
Organization Profile on CARE Lab website		●	●	●
1-DAY ORIENTATION				
Logo on holding slide during orientation talks	●	●	●	●
Attend orientation talks	●	●	●	●
3-5 minute promotional video that plays during orientation		●	●	●
Sponsor a Q&A, an Ask-Me-Anything, or keynote			●	●
LIVE COMPETITION				
Sponsor SME can participate in the event as a "CARE Lab" employee during **ONE LIVE** competition day	●	●	●	●
Sponsor SME can participate in the event as a "CARE Lab" employee during **TWO LIVE** competition days		●	●	●
Sponsor SME can participate in the event as a "CARE Lab" employee during **ALL LIVE** competition days			●	●
Prizes for winning teams are presented by sponsor along with sponsor-branded certificates 1st, 2nd, and 3rd place for each level: high school, undergrad, and grad			●	●
Live 1 hour seminar at Temple University or Zoom			●	●
Tour & lunch-n-learn in downtown Philadelphia				●

**Bronze: 1 sponsor spot, **Silver: 3 sponsor spots, ***Gold: 5 sponsor spots, ****Platinum: unlimited sponsor spots.*

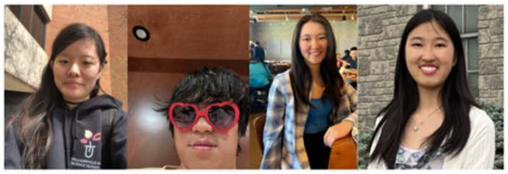
Silver, Gold, Platinum: List of student CVs for internships & entry level positions

2023 METRICS AND STUDENT TESTIMONIALS

THE WINNERS

High School Track

1st place
VIMISA



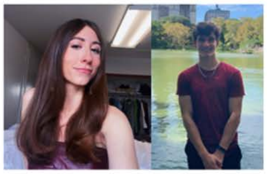
2nd place
Williamsville East High School

3rd place
Glen A Wilson High School

Undergraduate/Graduate Track

1st place
University of Nevada, Reno

2nd place
Western Michigan University

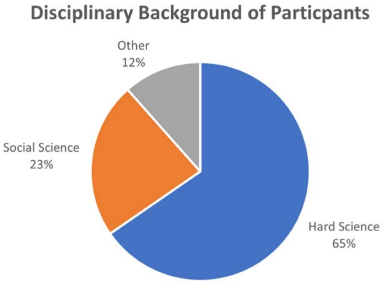


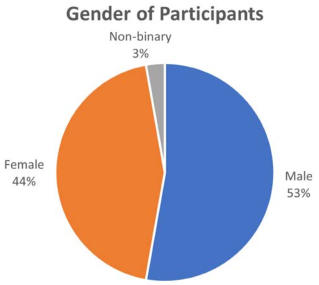
3rd place
Fordham University

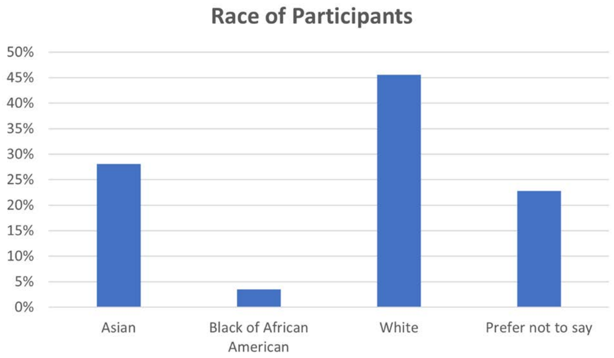
THEME

The CARE Lab helped an elderly victim of a romance scam, and “hired” student teams to serve as “fraud fighters”. Students had to interface with the victim to understand the current situation and interact with the scammer to find scam evidence. Teams submitted a formal report of their findings, including recommendations for the victim.

Website: sites.temple.edu/socialengineering/previous-events/2023-2







> *“Participating in social engineering events helped me to increase my awareness of common social engineering tactics and how to defend against them. This can include identifying and responding to phishing scams, recognizing and avoiding social engineering attacks, and understanding how to protect sensitive information from social engineering threats.”*
>
> *“This event taught me the fundamentals of social engineering. My confidence and abilities were improved upon as we digested course materials and strategized as a group. After each part of the competition, we went over things we did well and what we wanted to improve upon. We really dedicated our time which seemed to pay off in overall understanding.“*
>
> **-2023 participants**

Temple University
College of Liberal Arts | Cybersecurity in Application, Research and Education Lab

DIVERSITY, EQUITY AND INCLUSION

The CARE Lab's Commitment to Diversity, Equity and Inclusion

DIVERSITY

The CARE Lab has generated a list of 309 organizations that strive to make cybersecurity and STEM opportunities and experiences accessible to underrepresented groups: Women: 106; Black: 56; Indigenous/Native American: 11; Latinx/Hispanic: 19; Asian: 11; LGBTQIA+: 14; Youth: 58; Disability: 4; General Cyber/STEM: 25; and General Diversity: 5

We are actively working with these groups to promote the events described in this package. We have also shared this list with the wider community via our website: sites.temple.edu/care/dei/owl/. We hope that other engage with these communities for research, education, and other outreach efforts. Since the creation of this page in March 2021, this resource has been accessed **over 19K** times.

Your sponsorship will allow us to reach diverse and underrepresented groups to better serve their needs.

EQUITY

Our events do not require special tools or labs, resulting in low entry costs. Smaller universities, colleges, and high schools often struggle financially, and may not be able to purchase equipment to develop cybersecurity course projects. Our events can be implemented in high schools, 2-year, and 4-year institutions will little to no cost and free training via the CARE Lab.

Your sponsorship will allow us to keep education and training outreach efforts free for students and educators, and make it easy to incorporate creative, safe, ethical and fun experiential learning projects.

INCLUSION

Conventional CTFs require specific skills that limit participation to students possessing technical skills, such as coding, reverse engineering, hacking, cryptography, and exploitation. However, students across ALL disciplines can engage in our events; no specialized skills are required to participate. Cybersecurity is for everyone, and anyone can participate in our events!

Your sponsorship will allow for a more inclusive approach to cybersecurity education, resulting in training that is easy-to-follow and open to all fields, thus contributing to a well-rounded next generation workforce.

Temple University
College of Liberal Arts

Cybersecurity in
Application, Research
and Education Lab

This event is part of the education and outreach efforts of NSF Award # 2032292