COLLEGE OF LIBERAL ARTS

DON'T BE A HACK

Learn How to Teach Social Engineering Cybersecurity

SOCIAL ENGINEERING is when cybercriminals attempt to influence someone to take an action that's likely not in their best interests. If you want to teach your students cybersecurity skills for defending against the latest social engineering techniques, you need a playbook. Temple University's Cybersecurity in Application, Research and Education (CARE) Lab wants to share that playbook with you.

SOCIAL ENGINEERING EDUCATORS WORKSHOP

On Saturday, February 25th, the CARE Lab will host high-school and collegiate educators for a six-hour virtual workshop on social engineering tactics and persuasion techniques.

Following an introduction, you'll be put into groups for social engineering case studies. You'll practice live exercises in shoulder surfing, pretexting, open-source intelligence (OSINT), phishing and vishing. Then, we'll discuss the ethics of educating on cybercrime, share some student perspectives and discuss potential follow-ups for you and your peers.

ELIGIBILITY:

Full-time educators (high school and higher education institutions), age range 18+.

All educators participating in the workshop will be required to complete a workshop evaluation survey.

Select middle/high school educators will be compensated for their time at the rate of $25/hour.

Each participant must also complete an audio-visual release waiver. This allows organizers to use images, audio, text, and video generated during the event for promotion and dissemination via conferences, publications, and podcasts.

To participate in the workshop, please register at
sites.temple.edu/care/social-engineering/educator-workshop

This event and evaluation are considered research and are part of the education and outreach efforts of NSF Award # 2032292.