GUIDE

A Campus Culture of Cybersecurity

How to teach your faculty, students, and staff to be more secure

WITH SUPPORT FROM Bank of America Merrill Lynch

THE CHRONICLE of Higher Education®

A Campus Culture of Cybersecurity

A professor at a research university receives an email from his college's dean, asking him to download departmental data. The faculty member clicks a link to a page branded with institutional logos and enters his university log-in. But instead of a download, he's redirected to a webpage that tells him he's been ensnared in a fake spear-phishing effort by the university's cybersecurity office. It alerts the professor that the email could have been a very real scam and offers tips on how to spot such attempts in the future.

The subterfuge, which a growing number of higher-education institutions employ, is one example of how colleges are trying to prevent cyberattacks and fraud. As the threats grow, cybersecurity is a growing concern among college leaders. Managing those risks requires not just good technological tools and procedures but also creating a culture where people are aware of the threats and how to best manage them.

Colleges need strategic, campuswide communication efforts to create individual awareness and develop motivation for good habits, says Valerie Vogel, interim director of the cybersecurity program at Educause, the education-technology association. This advice applies to the full spectrum of colleges,

Colleges need strategic, campuswide communication efforts to create individual awareness and develop motivation for good habits.

A Campus Culture of Cybersecurity was written by Julianne Basinger. The Chronicle is fully responsible for the report's editorial content.

although research institutions, for one, face threats that are more varied, including intrusions by hackers who are organized and financed by foreign governments.

"Campuses want to educate students, faculty, and staff so they'll think more carefully about the impacts of their use of technology and data," Vogel says. "They do this by not adopting a one-size-fits-all approach to this type of training, because what works well for students may not work for faculty or staff. Colleges and universities know that their training has to be customized."

In developing communications and training about cybersecurity, as with any endeavor to create personal motivation, positive reinforcement and fun work better than dire warnings and punishment. Information-security staff members must also be strategic about how often to communicate, since many people on a campus are already overwhelmed by the volume of emails and social-media posts they receive not just at work but in their everyday lives, says Eric Weakland, director of the information-security office at American University. "We need a way to get their attention, and for them to realize, hey, this could affect me."

Among colleges and universities that have made cybersecurity a top priority, some have found innovative and comprehensive ways to educate and motivate people about good security practices. This report looks at three of them: Harvard University, the Rochester Institute of Technology, and Texas A&M University.

'SECURITY INSIDERS'

Harvard University has upped its cybersecurity game in recent years after a couple of well-publicized breaches in 2015 by international hackers. The university has taken a comprehensive approach that now includes uniform, two-factor log-in authentication; required specialized training in cybersecurity for all information-technology staff; security orientations for postdoctoral researchers as well as all staff members; and a communications campaign about cybersecurity awareness, with

At Harvard U., the IT security office collects electronic devices for secure destruction. It also leads education efforts on campus about cybersecurity.

Harvard U.

advertising that appears in locations across the campus and even on the side of the university's shuttle buses.

Yet Harvard's strategy is also tailored to the varied needs and concerns of individuals and departments, including safeguarding the health-care data and human-subject research information that some areas of the university collect and keep. "It's driven by risk level," says Sandy Silk, Harvard's director of IT security education and consulting. "You have to look at what are the assets that are valuable and need protecting most, because your money won't protect everything. There's never enough budget to protect everything at the same level, and it doesn't make fiscal sense to do that."

To help various departments choose cybersecurity-awareness strategies that will best fit their individual cultures, Harvard's information-technology office created a program called Security Insiders, Silk says. The people selected to be these cybersecurity ambassadors are the department administrators, administrative assistants, and faculty to whom others in the department look for guidance in their daily work. Every couple of months, the office sends them a box of communications materials and ideas on ways they can remind the people they work with about cybersecurity; the "insiders" then select which strategies might work best for the particular culture and needs of their department or area. For some, one effort might be a poster with a poll, stationed by the elevator, where people can add yes or no stickers saying whether they use a password manager.

Harvard's information-technology office also sends brief, easy-to-use matrices on cybersecurity that are tailored to a department or area's specific needs. The matrices inform people how to best categorize, share, and store particular types of data; how to safely collaborate with colleagues at Harvard and around the globe; and how to correctly delete and destroy information.

"We do this so it's there in front of them when they need it, and it's not going to be a search to find answers," Silk says. "We look for what it is that we can expect a person to actually achieve. If it's too difficult, then IT has to figure out a way to simplify that."

"You have to look at what are the assets that are valuable and need protecting most, because your money won't protect everything."

DIGITAL SELF-DEFENSE

To win the attention of staff members at the Rochester Institute of Technology, a creative communications campaign and training program aims to make security awareness fun, with a martial-arts theme. The online training is couched as a "Digital Self Defense Dojo" and features the institute's tiger mascot wearing a martial-arts robe. Staff members on the campus can earn various "belts" for completing training on ways to recognize cybersecurity threats and best responses to them. People who earn the belts are also entered in drawings for gift cards to the campus store.

The dojo is part of an annual communications plan that Rochester's information-security office creates to determine which topics need to be emphasized, based on current risks and individual and departmental needs. "A communications plan doesn't sound like a big deal, but most tech people don't even think about doing that sort of thing," says Ben Woelk, program manager for Rochester's information-security office.

With the plan in place, his office each month

Rochester Institute of Technology

The Rochester Institute of Technology awards "Digital Self Defense Dojo Badges and Belts" to employees who display good cybersecurity habits. Here, a member of the college's advancement team displays his awards.

focuses on presenting information about a different cybersecurity topic, such as awareness of phishing attempts, to students, faculty, and staff members through social-media posts, as well as posters on the campus. Rochester also sends simulated phishing emails to educate people on campus about how to best recognize and respond to those attacks. People on campus who fall for the self-phishing are guaranteed anonymity, so that the education can occur without fear of punishment or blame, Woelk says.

CYBERSECURITY GAMES

To raise cybersecurity awareness on its campus, Texas A&M University has turned to online video games. For the past eight years, the university has developed annual cybersecurity games that are designed to be fun and engaging, while educating students, faculty, and staff members about how to be safe in cyberspace.

The games are released in October, which is National Cybersecurity Awareness Month. This past October, the game was an online version of the board game Life, with Aggie-themed animation and a focus on educating people about not automatically clicking on random pop-ups that say they should update their antivirus software. Participants received small prizes such as football towels or frozen yogurt. The 10 highest scorers were entered into a drawing to receive an Apple Watch.

"We work really hard to make sure that the questions and answers and things that we're teaching them are more than just common sense," says Lacey Baze, the university's associate director of IT product strategy and communication. "We're giving them real tips that they can use in both their personal and professional lives."

During the rest of the year, Texas A&M has other communications campaigns to raise awareness via social media, newsletters, and emails. Even there, the IT division takes care to use innovative

"We work really hard to make sure that the questions and answers and things that we're teaching them are more than just common sense."

visual presentation and graphics to make the messaging fun. Emphasizing how good cybersecurity hygiene can benefit people in their personal lives helps grab their attention, and those good habits then can carry into their computer and data interactions with the university, Baze says.

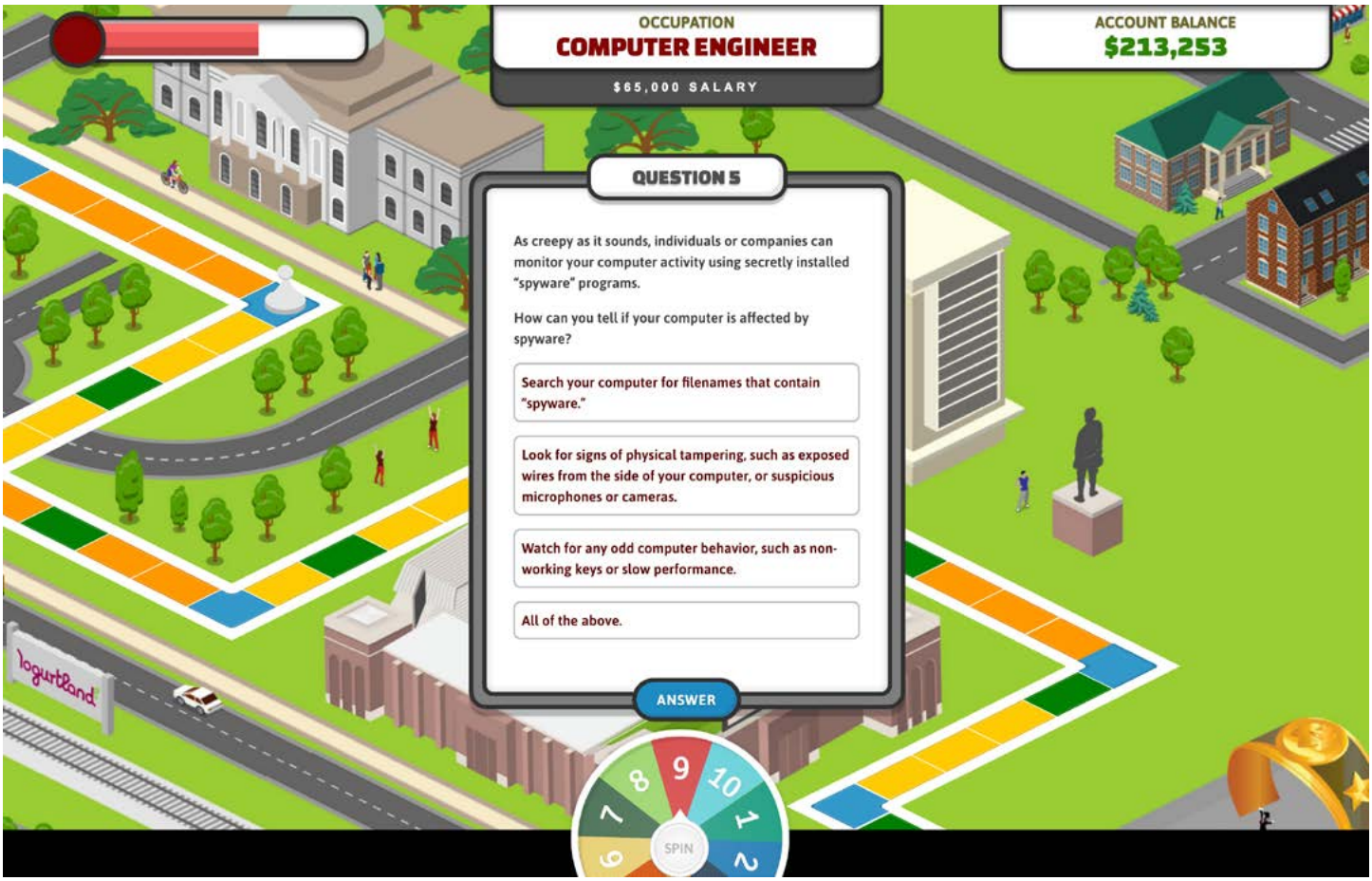
Michael Sardaryzadeh, Texas A&M's chief information-security officer, notes that beyond the general awareness campaigns, the university has also begun hosting an annual conference that brings in national industry experts to talk about issues and trends in cybersecurity, before audiences of students, faculty, and staff members. Part of the goal is for the conference's presence and advertising on the campus to help foster an internal culture of cybersecurity awareness, he says.

Creating a culture of cybersecurity requires identifying a higher-education institution's top information-security risks and then crafting communications strategies that are tailored to the personal and professional needs of individual students, faculty, and staff members. A growing number of institutions are making this a priority, but some colleges still struggle for sufficient resources and staffing to adequately manage cybersecurity, says Vogel, at Educause.

Even so, information-technology staff members at higher-education institutions often collaborate with their peers at other colleges to flag new cybersecurity threats and brainstorm on ways to deal with them, notes American University's Weakland.

Institutions also share ideas on communication strategies for fostering cultures of cybersecurity on a campus, including sending simulated phishing emails to faculty members that appear to be from their college's dean. "Nobody will say you can ever fully resolve your risks, because they keep changing," says Susan Grajek, Educause's vice president for communities and research. "So the question for institutions is how they can affordably safeguard information, through policies and proactive steps such as educating people and assessing where security is vulnerable."

Texas A&M developed an online game, "Aggie LIFE," to teach students and faculty members about cybersecurity.



Texas A&M

THE CHRONICLE
of Higher Education®

1255 Twenty-Third Street, N.W.
Washington, D.C. 20037

(202) 466-1000 | Chronicle.com