**▼ This November 2017 selection was written by Lindsey McKenzie, a technology writer for InsideHigherEd.com, an online publication devoted to issues in higher education in the United States and worldwide. It reports on one university's efforts to get its students to be vigilant about a persistent problem: the use of weak passwords that compromise their own personal accounts and the security of the campus network as a whole. McKenzie highlights the challenge to campus technology professionals: figuring out a creative way to make a compelling argument to a well-defined audience. As you read, take note of not only the aims of argument at play but also the additional benefits that the campaign described here reaped. Consider as well why we chose to begin this chapter on privacy with a discussion of passwords on campus.**

## Getting Personal about Cybersecurity

**LINDSAY McKENZIE**

Today's students may be digital natives, but that doesn't mean institutions can count on them to protect themselves from cyberattacks.

A recent survey by the technology firm CDW-G found that the No. 1 cybersecurity challenge facing IT professionals on

campus is educating users about security policies and practices. Among students surveyed, just 25 percent dubbed the cybersecurity training or education efforts on their campus as very effective.

***IT***
information technology.

One institution, however, may have found a way to reach students—by making them, and their pets, the stars of a cybersecurity-awareness campaign.

Speaking at the annual meeting of **Educause** in Philadelphia this month, representatives from the University of Massachusetts at Amherst shared how they leveraged students' love of social media and personalized content to encourage them to up their cybersecurity game.

***Educause***
a U.S. nonprofit organization seeking "to advance higher education through the use of information technology."

"There was a recognition that we needed to do something different, something fun," said Iris Chelaru, web communications manager at UMass. While previous awareness campaigns had been informative, they failed to connect with students on a personal level, said Chelaru. Cybersecurity awareness is a bit like public health awareness, she said—"things that we have to do but that we don't want to."

As students are both creators and curators of content online, who better than them to advise and help design an awareness campaign, Chelaru said. She and her team worked with the student government and other campus organizations to design an approach that was both informative and “warm and fuzzy,” said Chelaru.

Rather than presenting information on multiple security risks, as the university had previously, UMass officials decided to pick just one issue—weak passwords—as the center of their campaign. Pet names emerged as something that students regularly use as passwords, but that can be easily guessed, said Chelaru. With this in mind, the team created a website where students can create posters with pictures of their pets, underneath the tagline “My name is not a good password.”

University of Massachusetts, Amherst

*Posters from the Getting Personal About Cyberspace campaign at UMass Amherst*

**The campus Internet security professionals found that their campaigns were more effective when they connected to their audience—students—on a personal level.**

**LINK TO Chapter 1, Appealing to Audiences.**

"We were thinking about things that are familiar to students and that they know, maybe something from home that they miss," said Chelaru. The posters, which could be easily shared on social media, saw much more engagement from students than previous campaigns did, said Matthew Dalton,

chief information security officer at UMass Amherst.

Though the campaign started with posters of student pets, it quickly broadened, said Dalton. To make the campaign even more interactive, the team created giant photo frames that students could pose with in real life, under the same “My name is not a good password” banner. The team set up tables in areas with high student traffic at lunchtimes in October as part of National Cyber Security Awareness Month and offered prizes to encourage engagement. Soon the football team’s mascot, Sam the Minuteman, and the university administration were in on the campaign.

While Dalton and colleagues hailed the campaign as a success, evaluating its impact has been tricky, he acknowledged. They have seen a decrease in student account breaches, but Dalton said he can’t be sure this campaign is responsible, as opposed to other security work the team has done. It would be difficult to track whether the campaign had actually resulted in behavior change without cracking student passwords to check if they contain pet names, said Dalton. But he is planning to look at whether password change activity has risen, he said.

Dalton said that the password campaign, now entering its third year, continues to have an impact because it doesn’t overload students with information. Where previously students might have been referred to the National Institute

of Standards and Technology's guidelines on how to create a good password (make them complicated, change them regularly, include numbers and special characters, etc.), now students are just being made to think about what makes a bad password. The details come later, when the students actually log in to change their passwords, said Dalton.

Though the impact on student behavior is not yet known, the institution views the campaign as a success for other reasons, said Dalton. First, all the posters and photos shared on social media had strong institutional branding. Second, the campaign had support and engagement from the university administration, including backing from the vice chancellor for information services. Third, students were able to take ownership of the campaign. "People were willing to become part of the message," said Dalton. "With any participation event, that's key—especially with security awareness."

RESPOND●

1. What problem gave rise to the arguments made by the UMass Amherst cybersecurity campaign described in this selection? How did the IT professionals define the rhetorical situation? How did their understanding of the rhetorical situation shape their response? What sorts of research did they do? Whose help did they enlist? Why? (Reviewing Chapter 1's discussion of the rhetorical situation may be helpful in thinking about this question.)

2. What is your response to the solution that the students at UMass Amherst came up with? Do you think you would likely find it convincing enough to move you to action, that is, to pay attention to the security on your own computer account—to make passwords complicated and not likely predictable, to change them regularly, and to include numbers and special characters? Why or why not?
3. How would you characterize the argument made by this selection: is it an argument of fact, one of definition, an evaluative argument, a causal argument, or a proposal? Why? (The discussion of stasis theory in Chapter 1 may prove useful here.)
4. **THINKING CRITICALLY** What were the unforeseen consequences of the campaign described here? Why are they important? What does a situation like this one teach us about the nature of argument and its potential consequences or benefits?
5. Imagine you were given the task of creating a proposal to address the problem of cybersecurity on your campus by raising student awareness of the issue. Is there a solution that you believe might be more effective than the one used on the UMass Amherst campus? Working individually or in small groups, **construct a proposal argument** containing a plan for addressing this challenge. (Chapter 12 offers a discussion of proposal arguments.)

**Although you've likely never considered it, producing an effective cartoon requires an interesting and complex set of rhetorical skills. Cartoonists have a limited amount of space to convey their messages. The five cartoons included here range from a single panel to four panels, the latter representing a widely syndicated cartoon strip. A cartoon's message has to be pithy—much like a tweet—and it has to combine one or more images with words. The words, of course, may take the form of a caption, or they may be part of the image. The images have multiple functions: they have to capture the reader's attention, but they must also thrust the reader into a narrative, a story, one that unfolds almost instantaneously.**

**Cartoons likewise have to rely on the two-edged sword of humor—always risky—to make their point. In this regard, even simple cartoons represent sophisticated visual rhetoric—multimodal arguments—that merit careful attention. Furthermore, cartoons must be timely, speaking to a current topic of interest or debate; in short, they must seize the kairotic moment, as discussed in Chapter 1. As you consider the five cartoons in this selection, all of which consider aspects of privacy, use your rhetorical skills to analyze how each of the cartoonists manages to pack what is often an implied but powerful argument into such a small package.**