By JOHN O'BRIEN

Another Fall Semester, Another School of Phish

The e-mail seemed harmless enough: a short note to the EDUCAUSE CFO, Stacy Ruwe, asking her to help me get a payment processed. It was all very friendly, first-name-basis stuff. Except that it was all a lie—a well-crafted one. If the e-mail was viewed on a cell phone, the clearly fishy address of the sender (ceo.mail@msver.com) was hidden from view. And this was the third phishing e-mail sent to Stacy from "me" that month.

It is frightening to imagine how easily one could be hooked, especially in the flurry of e-mail that comes with a new academic year. Gone are the almost nostalgic days of those "dear most beloved friend" e-mails from strangers offering millions of dollars for doing almost nothing. These amateurish attacks have been replaced with more sophisticated efforts to trick us into revealing our credentials, credit card information, or other personal data.

These attacks usually employ some sort of technical subterfuge as well, like a spoofed e-mail that appears to be from a trusted source. Ultimately, these types of scams are designed to steal money or deliver malware to your computer. Not only do these scams work, but their frequency seems to be increasing. The Anti-Phishing Working Group, a global consortium dedicated to fighting cybercrime, reported that the incidence of global phishing attacks increased by 65 percent from 2015 to 2016.[1] Perhaps the one life preserver we have for avoiding the wave of phishing attacks is that we can be trained to avoid the lure of the phishing e-mail.

From: "John P. O'Brien" <ceo.mail@msver.com>
Subject: Request For Wire Transfer
Date: May 25, 2017 at 1:03:26 PM EDT
To: <sruwe@educause.edu>

Hi Stacy,

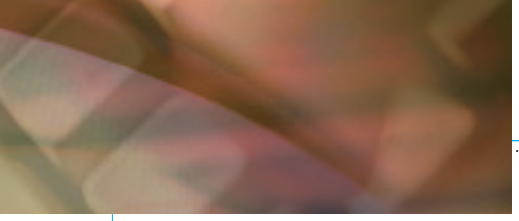
I need you to process an international W/T to Hong Kong today, Please kindly get back to me with the details needed to process an overseas payment and the transfer charges.

Regards
John

The importance of throwing out a lifeline and training members of the institutional community in good cybersecurity practices cannot be emphasized enough. The Higher Education Information Security Council (HEISC) has identified phishing and social engineering as one of the biggest information security risks facing the community.[2] Research from EDUCAUSE shows that from 2005 to 2013, 47 percent of higher education data breaches had underlying "human element" causes, which perhaps could have been mitigated or even avoided with a comprehensive cybersecurity training and awareness program covering a number of different data and IT protection practices.[3]

The month of October offers an opportunity to spotlight the importance of cybersecurity training and awareness. October is National Cyber Security Awareness Month (NCSAM), a collaborative effort to ensure that everyone has the resources needed to stay safe online. NCSAM is spearheaded by the U.S. Department of Homeland Security and the National Cyber Security Alliance. As a NCSAM champion, EDUCAUSE—along with other organizations and institutions in the higher education information

(continued on page 6)



(continued from page 4)

security community—participates in this annual campaign each October to expand cybersecurity awareness and education on campuses and around the globe.

Effective cybersecurity training and awareness is a key component of an institutional information security program. In 2015, U.S. institutions required cybersecurity training for approximately 75 percent of faculty and staff and for 1 in 4 students.[4] Support for this type of training also runs high in higher education: more than half of cybersecurity awareness and training professionals report sufficient executive support for awareness and training efforts.[5] Cybersecurity awareness and training helps institutional community members turn the tide and know the specific actions that they can take (or, more importantly, not take) to protect institutional data and IT systems. Whereas 75 percent training for faculty and staff is pretty good, the picture for the other 25 percent is not so promising.

The Annual Campus Security Awareness Campaign provides twelve different monthly cybersecurity awareness topics that can easily be integrated into campus communications.

Making cybersecurity awareness and training easy for the person providing the training, as well as effective for the people receiving the training, is a goal of the HEISC Awareness and Training Working Group. The practitioners in this working group understand the constraints of providing cybersecurity training and awareness in the higher education environment. They know, for instance, that higher education cybersecurity awareness and training programs are typically led by managers who attend to these responsibilities with only a fraction of an FTE and with budgets of less than $5,000. Ultimately, this means that cybersecurity awareness and training activities are conducted in an ad hoc manner, depending on the time and financial resources available to the training and awareness professional.[6]

To help combat the ebb and flow of time and resource constraints, the HEISC Awareness and Training Working Group has created an Annual Campus Security Awareness Campaign for institutional use, and campuses looking for materials to add to their security plan in the new academic year should give it serious consideration. The campaign is a framework designed to support information security professionals and IT communicators as they develop and enhance their own institutional cybersecurity training and awareness plans. The campaign provides twelve different monthly cybersecurity awareness topics that can easily be integrated into campus communications. Functioning like a "cybersecurity training in a box" resource, the ready-made content can be used by institutions to create a steady stream of cybersecurity awareness information for students, faculty, and staff.

This year, phishing-related topics were featured in February and April. Now, as we start another fall semester, is a great time to reacquaint ourselves with the resources available and to consider new actions to respond to the growing, evolving threat. These days, taking the bait involves one simple click. That's all that is needed to imperil your privacy—and that of your higher education institution as well.

Notes

1. Anti-Phishing Working Group, "Phishing Activity Trends Report: 4th Quarter 2016," February 23, 2017.
2. Joanna Grama and Valerie Vogel, "Information Security: Risky Business," *EDUCAUSE Review*, January 17, 2017.
3. Joanna Grama, *Just in Time Research: Data Breaches in Higher Education* (Louisville, CO: ECAR, May 2014): 30 percent of breaches studied were caused by unintended disclosure (e.g., posting sensitive information on a public website or sending e-mail to the wrong person); the other 17 percent of breaches were caused by lost, discarded, or stolen portable devices.
4. Joanna L. Grama and Leah Lang, *CDS Spotlight: Information Security*, ECAR Research Bulletin (Louisville, CO: EDUCAUSE, August 15, 2016).
5. "2017 EDUCAUSE Information Security Almanac," May 2017.
6. Joanna L. Grama and Eden Dahlstrom, *Higher Education Information Security Awareness Programs*, ECAR Research Bulletin (Louisville, CO: EDUCAUSE, August 8, 2016).

John O'Brien (jobrien@educause.edu) is President and CEO of EDUCAUSE.