Facebook’s Teachable Moment: What Higher Education Knows about Improving User Behavior

changed my privacy settings. Did you? Who among us did not review our Facebook privacy settings this past March? Were you spurred to do so by the Cambridge Analytica news? By Facebook’s full-page apology in the New York Times? Perhaps you are naturally cautious and just happen to always review your social media privacy settings on the second-to-last Sunday in March?

The fact that Facebook was sharing more data than it stated really shouldn’t come as much of a surprise. The fact that another organization didn’t delete data when it promised to do so and used it for other purposes shouldn’t be a surprise either. Yet it continues to be a bitter pill to swallow that the best defense against these vendor “oversharing” violations is a fundamental change in user behavior—especially for people who just want to share photos of their latest family celebration or what they ate for dinner at the fancy restaurant last night or to circulate the social and political views closest to their heart.

Higher education information security and privacy professionals have long recognized that changing user behavior is at the core of any successful information security awareness strategy. When the higher education information security community first started to organize in the early 2000s, it recognized the importance of convening people to develop and share effective cybersecurity practices and of promoting cybersecurity awareness to the wider higher education community. Cybersecurity awareness is just as important today. In fact, the opening keynote by Dr. Jessica Barker at the 2018 EDUCAUSE Security Professionals Conference stressed the importance of cybersecurity awareness and suggested that approaching this type of awareness training from a positive viewpoint (emphasizing good cybersecurity hygiene practices instead of highlighting the poor practices one must avoid) might lead to a more informed and security-savvy user. Thus, higher education practitioners continue to evolve and refine their approaches to information security awareness education.

Effective awareness and education activities are crucial to the success of information security program. We share practices and awareness tips in an environment that says that information security is the number one issue facing higher education IT organizations today. We promote user awareness in an environment where the complexity of security threats continues to grow and influence institutional IT strategies. And, we advance data security and privacy literacy in an environment where resource constraints may mean that the most exciting up-and-coming security technologies are beyond the reach of even the best-funded IT organizations.

So, what does higher education do that might scale for other industry sectors?

- **Community.** First, we have an identifiable community whose members work together to share tips and techniques for changing user behavior. We create awareness campaigns that any higher education institution can use to supplement its own information security awareness program. Higher education understands that changing one user’s behavior may be all that is needed to provide a good security outcome for our entire higher education community. Building a global network of practitioners that understands this is crucial.

- **Collaboration.** While there are certain subject areas in which institutions may want to be self-sufficient and even competitive, information security awareness is not one of those areas. There are opportunities for mutual and sector improvement only when those in the higher education information security and privacy community collaborate to create and share tips, techniques, practices, policies, procedures, technologies, and tools related to information security activities.

- **Conviction.** Finally, higher education leaders and information security and privacy practitioners have a true passion for protecting the data that community members entrust to their institutions. Students, faculty, staff, vendors, and other third parties entrust many different types of data (e.g., business, financial, and research data, as well as personnel information) to institutions every day. Failing to protect this data may not necessarily impact an earnings report, but it can negatively affect an institution in many other ways (e.g., data breaches or inadvertent disclosures that result in remediation costs, regulatory fines, and reputational loss). While there is no silver bullet to prevent data breaches, a sense of conviction in protecting institutional data persists in the higher education community.
Many users may have been caught off-guard earlier this year with the news about Facebook and Cambridge Analytica. Teaching users how to protect themselves is an essential step toward protecting the data of a larger enterprise, from ongoing business concerns to higher education institutions. And the results are reflexive: any security hygiene practices learned and employed at work to secure organizational resources can be used to help secure a user’s personal data as well. Higher education information security and privacy professionals offer some quick tips to help users protect data both at work and at home:

- Use different passwords for every single account, and use a good password manager tool to help keep track of all the different passwords. In most applications, passwords are coupled with an email address to grant you access to the application. When you reuse an email/password combination, you run the risk of having multiple resources compromised if a single password is exposed. At the very least, make sure that sensitive accounts (e.g., bank accounts, credit card accounts, work accounts) all have different passwords.

- Be very suspicious of unsolicited requests received via electronic communications. Sometimes these types of communications are used to steal data or spread malware. Today’s phishing scams are far more sophisticated than the “prince in a far-off land” schemes of ten years ago. Any unsolicited request that asks you to follow an embedded link, open an attachment, share your user credentials, enter banking information, or provide additional personal information should be reviewed with a critical eye. Wherever you can, use another communication mechanism to verify that the first communication was authentic before navigating to a website, providing data, or opening an attachment.

- Limit the types of personal data that you share via apps and other online services whenever possible. Often organizations and applications ask to use or access far more data than they need in order to offer you goods and services. They do this so that they can build a profile of you as a user and offer you even more goods and services. Be a discerning service user and read the user agreements before you download a new game or use a new service. You may decide that using the new service is more important to you than sharing your Facebook friends list, or you may decide to forgo the new service because it asks for too much data. In order to make an informed decision, you must know and understand what you are sharing.

Improving data security and privacy literacy is something that transcends and can unite every industry sector. The higher education approach to creating effective awareness and education programs—focusing on community, collaboration, and conviction—is something that any industry sector can emulate to improve user behavior.

Notes
A condensed version of this article was published in EdSurge, June 3, 2018.

Joanna Lyn Grama [Joanna.Grama@vantageteg.com] is Senior Consultant, Vantage Technology Consulting Group.

© 2018 Joanna Lyn Grama. The text of this article is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.