Cyberattacks are common occurrences in today’s digital world. As the internet of things, artificial intelligence, and machine learning create exponentially more valuable data, it needs to be protected and managed appropriately. This is even more important as we enter into the age of the Fourth Industrial Revolution, where the physical, digital and biological worlds intersect.

Universities face the complexity of allowing the academic community access to knowledge, while maintaining robust security around the information that needs to stay private. Educause [1] finds that information security is the No. 1 concern of higher education IT organizations for the third year in a row. Our vast amounts of sensitive personal data, financial records and intellectual property make us an enticing target for hackers.

Being good stewards of your personal data, as well as University systems, is something that we take very seriously at the University of Arizona.

Recently, all three state universities – Arizona State University, Northern Arizona University and the UA – participated in an IT Security Performance Audit, which is conducted by the Arizona Office of the Auditor General every 10 years. For the UA, this audit has been a useful tool to help us understand our level of information security maturity; it also provides recommendations to further strengthen our cybersecurity model. The final report is available on the Auditor General’s website [2].

The audit found several areas across campus where the UA needs to be more sophisticated and deliberate.

The UA is already on track to address the report’s recommendations and has made investments to improve information security. Our information security team, led by Lanita Collette, has made great progress to further secure our people and systems.

The University took a significant step forward in April by requiring NetID+ two-factor authentication for all employees, which provides an additional layer of protection beyond the use of strong passwords. With NetID+ required for logins to campus services, personal data like UAccess Employee information and UAConnect365 emails will be protected in case your password is compromised. UA students also will be required to use NetID+ beginning this fall.

The audit recommends information security awareness training for employees to further reduce social engineering attacks. The UA’s current security awareness training is in the process of being redesigned and will be released later this year. The brief online tutorial and assessment will be mandatory for all staff and faculty every year, as required by the Auditor General. New monitoring features will assist with tracking completion and compliance.

Over the next two years, we also will be implementing a variety of additional tools and
systems to help improve the level of sophistication in our IT operations and campus networks. Areas of focus will be vulnerability scanning, patching, log monitoring, configuration management, web app development, and systematic communication and collaboration within the UA's IT community.

Implementing the audit recommendations will need to be a priority for IT units across campus. We have been working with campus IT directors and the first few steps have been released and are ready for IT units to begin implementing.

All of us at the UA have a role to play in helping to keep our campus information and devices secure. As you use your computer, email and the internet, we ask you to be aware of the security requirements associated with your work and cyber risks that potentially exist. Explore the resources at the Information Security office’s new website, security.arizona.edu [3], including phishing alerts, news, security tips for work, and tips to protect you and your family's information at home.

Priorities for us will be to protect people and systems, and also to respond quickly when we see unexpected cyberactivity.

In the coming months, we will continue to communicate information security updates to campus through a series of articles in Lo Que Pasa.

If you have suggestions for topics that should be covered, please send an email to uaatwork@email.arizona.edu [4] with "information security" in the subject line.

Barry Brummund became the UA's chief information officer in April. Previously, he was assistant vice president for financial planning and analysis.

Source URL: https://uaatwork.arizona.edu/lqp/keeping-your-ua-information-secure

Links:
[3] https://www.security.arizona.edu
[4] mailto:uaatwork@email.arizona.edu?subject=Information%20security