VirginiaTech

Vice President for Information Technology and
Chief Information Officer (0169)
Burruss Hall, Suite 314
800 Drillfield Drive
Blacksburg, Virginia 24061
540/231-4227   fax: 540/231-5843

Memorandum

To: Virginia Tech Students, Staff, and Faculty

From: Scott F. Midkiff, Vice President for Information Technology and Chief Information Officer SFM

Date: November 12, 2015

Subject: Update on Two-Factor Authentication at Virginia Tech

Monday, November 9, 2015, represented an important milestone for our transition to a stronger cybersecurity posture through two-factor authentication. On November 9, general users across the university began to see the first set of web-based applications that utilize our new Virginia Tech Login service and were presented with options for two-factor authentication. The first wave of web applications are so-called “federated services” and include applications such as Cayuse 424, PeopleAdmin, Lynda.com, and off-campus sign-in for the Libraries. A user accessing one of these applications now sees a different login screen featuring the Virginia Tech Pylons. After entering their PID and password the user is offered an opportunity to enroll one or more devices to use for two-factor authentication. For now, the user can defer enrollment and proceed to the application. Once a user has enrolled one or more devices, then the next step would be to do the second step of authentication.

We, of course, want to encourage people to enroll a device and begin to have more protection for authentication as soon as possible. With time, more and more web-based applications, such as HokieSPA, Canvas, Scholar, etc. will be using the new Login service and two-factor authentication. During Spring 2016, we expect that all web-based applications now using the Central Authentication Service (CAS) and managed by the IT organization will use the new Login service and two-factor authentication. During Summer 2016, we expect that the ability to defer enrollment will end and two-factor authentication will be required.

Over time, all Virginia Tech faculty, staff, and students will be using two-factor authentication. There will, no doubt, be some authentication procedures that will continue to use only a password, but our goal is to change the mindset to where two-factor authentication is the norm and one-factor authentication (password only) is the exception. Many systems, including those managed outside of central IT, will move to two-factor authentication. Once our two-factor infrastructure is fully available, we will use the following mechanisms to encourage and, as appropriate, enforce the transition:

- Systems managed by the central IT organization will be expected to require two-factor authentication except where not practical.
- Our “rules of engagement” for distributed IT groups to connect to critical systems managed by central IT will be escalated to require two-factor authentication.
- In collaboration with data trustees, our data policies will be updated as appropriate to require two-factor authentication for protection of sensitive data and critical resources.
- We will disseminate and encourage best practices to facilitate adoption, maintain usability, understand risks, and protect data and resources.

It is worth noting that two-factor authentication places some, but we believe minimal, continuing burden on a user but with no real gain in functionality that directly benefits the user. However, two-factor authentication substantially reduces the likelihood of unauthorized access to sensitive information and important systems, thus reducing the time and money spent on remediation after a data breach as well as reputational loss. And, given the current and future cybersecurity threat environment, the single password is simply no longer sufficient as the only means for authentication. Many universities have moved or are moving to two-factor authentication. Many are taking a minimalist approach, where two-factor is the exception. Based on what I believe is a more holistic and long-term view, we are taking a bigger step now to more significantly and more comprehensively improve our cybersecurity posture and to do this as systematically as possible rather than piecemeal over time.

People in central IT are engaged in discussions with IT directors from administrative units, colleges, and institutes through the IT Council and I appreciate their engagement. We are also in discussions with various functional units across campus to plan the details of transitions including dealing with special use cases. We will be offering “showcase” events on campus and in the National Capital Region to let people see device options and to assist with enrollment. A town hall open to the university community will be held on December 17 to discuss our motivation and approach and for us to listen to how we can best support the transition. We look forward to these and other opportunities to communicate with the university community.

More information about Virginia Tech’s two-factor authentication initiative is available at http://www.it.vt.edu/2factor/.

Thank you for your help with this important transition.