Protecting data assets with two-factor authentication

February 3 2016

To better protect the Institute's data – including employee data – from future cyber risks, the Office of Information Technology (OIT) will begin deploying two-factor authentication to early adopters across campus in 2016. The Office of Development and the Office of the President are among the first offices to adopt this technology department-wide. Offices in the Division of Administration and Finance are scheduled to follow this year. Here's what you need to know.

What is two-factor authentication?

Two-factor authentication uses two pieces, or factors, of information to verify the identity of a user trying to access a service. The first factor, your password, has been deployed at Tech for many years. Other factors commonly used for identity include fingerprints, retina scans, numeric codes, and portable tokens. Using these two factors together gives a much stronger identity verification process than just a password alone.

Use of two-factor authentication is quite common. In fact, you may already be familiar with two-factor authentication as it is often used in banking, cloud solutions such as Dropbox, email such as Gmail, or social/productivity sites such as Google+ or Facebook.

How does two-factor authentication work?

Two-factor authentication keeps information safe by requiring the user to enter a second layer of security, usually in the form of a generated number, before accessing a protected application. Because the second authentication is independent from your username and password, if your password is stolen, the web application using two-factor authentication is safe from attempted hackers.

What is Duo?

Georgia Tech has partnered with Duo Security to provide this service to our campus. Once a Georgia Tech IT support team has enabled two-factor authentication on your Georgia Tech account, in addition to using your usual username and password to log in, you will need to authenticate your identity before accessing protected sites including TechWorks and Office365 as well as the virtual private network (VPN) via Cisco.

When you log in to these protected systems, you will need access to your device(s) with the Duo app, or a telephone that you have configured for this purpose. Additional details regarding how to authenticate your identity will be provided once your system is enabled.

Provided by Georgia Institute of Technology

Citation: Protecting data assets with two-factor authentication (2016, February 3) retrieved 18 April 2024 from https://phys.org/news/2016-02-assets-two-factor-authentication.html