

Considering and Deploying Two-Factor Authentication

IAM Online

Wednesday, April 8, 2020

Presenters:

Lorrie Burroughs, Georgia Institute of Technology

Hank Foss, Sacred Heart University

Moeen Taj, Montgomery College

Moderator:

Tom Barton, University of Chicago and Internet2

2FA – Getting There From Here

It's a good thing, sure, and we know how to do it, technically. But making it happen is another matter.

- Where all should we add its protection? Initially; later on.
- What's the encompassing rationale, more meaningful than “security is good”?
- Who must be in scope?
- Who decides these things?

Marketing & Communications

- How do we sell the rationale?
- What opportunities can be leveraged to make the case?
- Can a top-down approach work? Must we find a way to explain it so that most people will actually agree to go along?
- How do we reach the various segments of our campus population, and do they need to hear different rationales?
- Who can we enlist to help with that?
- What does the campaign cost?

On-Going Support

- Do we need to engineer support differently for different segments?
- How long will it take?
- What service delivery problems should we anticipate?
- What additional support costs should we plan for?
- What data can be gathered to show that it is worth it?
- Who gets an exemption, and why?



INFORMATION
SECURITY

Sacred Heart University

MFA Implementation at Sacred Heart University

Hank Foss, CISSP, GPEN, MSCS

IT Security Manager

fossh@sacredheart.edu

Who is at risk of compromise? No one is excluded. And no \$\$\$ amount is a substitute for MFA.



Who is at risk? MFA implemented in your environment prevents unnecessary compromise.



BRIDGEPORT PUBLIC SCHOOLS

Aresta L. Johnson, Ed.D.,
Superintendent of Schools
(203) 275-1000



Cornell University
Virginia Tech

University of the Cumberlands
Oregon College of Oriental Medicine

University of Maryland, B



State University

University of Pitt

Greensboro

New York University



re

Rice University

M

ty

University of California, Los Angeles

Roch

iology



Eden Theological Seminary

University of Tennessee

Arizona State University



University of Arizona

NC State University

Purdue University

University at Buffalo

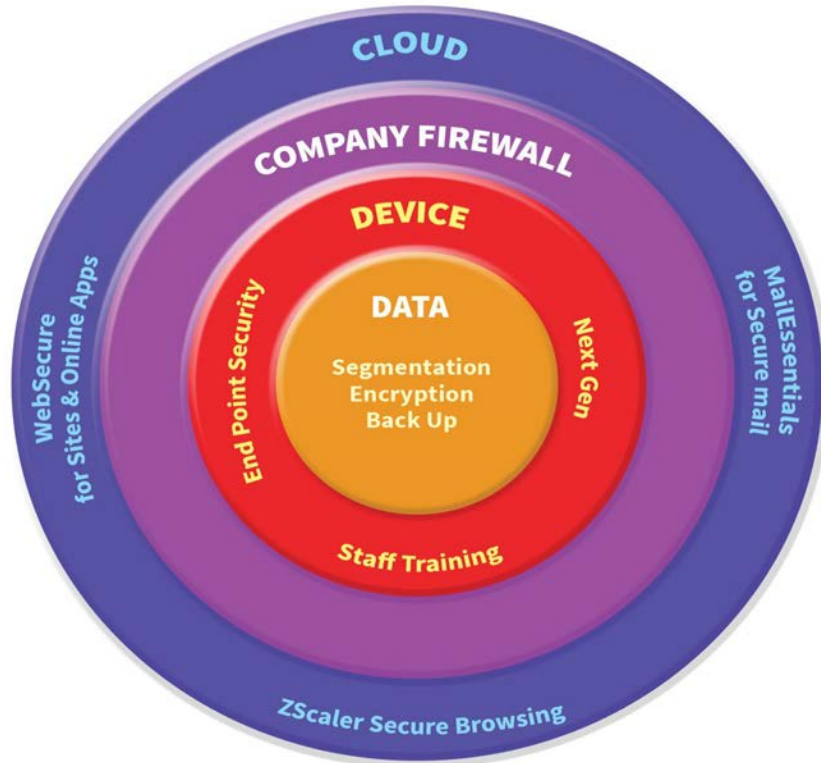
Atlantic Cape Community College

University of Washington



How is SHU ITSec Protecting You? A layered security model is good provided MFA and Security Awareness Training are part of it.

LAYERED SECURITY



- **Multifactor Authentication (MFA):** For applications, Microsoft email, and portal applications (Outlook, Word, Excel, PowerPoint, Teams, et al.)
- **Security Awareness Education**
 - **Antivirus:** Symantec Endpoint Protection and Trend Micro Deep Security
 - **Firewall:** Palo Alto Next-Generation
 - **Email Firewall:** Spoofing Detections
 - **Microsoft Office 365 Security alert policies**

Implementation Strategy for MFA?

- IT Security already had a strategy in mind. We knew, and we were on the same page.
 - **Duo for applications:** Citrix NetScaler, Palo Alto GlobalProtect VPN, Thycotic Secret Server, SSO portal.
 - **From External and internal, or just external?** We chose to protect both connection methods
- **Getting buy-in from the masses, which meant buy-in from upper management**
 - SHU Security Awareness Day !!
 - Public Safety Department and IT Security Department tag teamed the community and provided in-depth presentations to Faculty and Staff and took questions.



Duo Implementation Steps

- **Duo to Protect Cisco NetScaler connections**

- IT Department as UAT for 3 – 6 months COMPLAINTS? Of course the IT Department has complaints!! The best audience you'll ever get for feedback is your IT audience. Carried lessons learned into next step.
- Documented lessons learned and brought IT HelpDesk into fold and made them “Experts”!
- Then critical departments: Business Office, Finance
- Then all other departments

- **How did we do this department by Department?**

- Created departmental security groups in AD and added them one by one into the “Duo MFA All Users” MFA group only the “ALL” group was required to be MFA protected.
- So as department by department was dropped into the ALL group, they then had the MFA requirement

- **Other Apps Protected?**

- Yes, Palo Alto GlobalProtect VPN and Thycotic Secret Server

- **Work In Progress:** SSO for Portal access to LMS, Dayforce and others



Office365 MFA Implementation Steps

- **Office365 MFA for Email and Office App Protection**
 - IT Department as UAT for 6 – 12 months COMPLAINTS? Of course.
 - Documented lessons learned and brought IT HelpDesk into fold and made them Office365 experts as well.
 - Notified groups of users, department by department, and enabled them manually at first.
 - Method of notification to user community was under some scrutiny, and became a bit cleaned up by this process, helping button up our end-user PR
 - Completed all departments except for Senior Management
 - **NOTE #1:** All senior management required two IT staff per exec – serious handholding with executives
 - **NOTE #2:** We MFAed the President’s account early in the exec process, making the other execs follow suit
- Scripted enablement of MFA automatically for all new employees and students



Office365 MFA Implementation Steps (continued)

- Completing the MFA process for Office365 became a goal for our VP's Performance Review

THIS RAMPED THINGS UP A BIT

- Most of our students still had the status of **Enabled** in our MFA portal, which was unexplained by much of Microsoft's documentation
- After opening a call with MS, we confirmed MFA Enabled simply meant not using the MFA Authenticator piece and most students were using the SMS feature to authenticate
- MS Engineer also confirmed that once in **Enabled** status, changing to **Enforced** does not affect the user.
- For reporting purposes, changed all protected users (now, everyone except for Alumni, to Enforced). Mission accomplished for VP of IT !!
- Work In Progress: Alumni accounts

Technical & Institutional Feasibility

Moeen Taj

Manager, Enterprise Application Services
Montgomery College, MD

Pilot Program

- Identification
 - Identify Project Team
 - Identify set of users for focused pilot program
 - Identify tools to be used
- Discovery
 - Seek to discover issues and challenges during the pilot program;
Barriers to Adoption
 - Discover potential redundancies for MFA

Institutional Readiness

- **“Institutional Project”**
- Identify stakeholders across the board
 - Student Services, Academic Advisors, Financial Aid, Senior Leadership etc.
- Why? Who? When? What?

Institutional Readiness

- Why
 - Gramm-Leach-Bliley Act (GLBA) Compliance
 - Performed a risk assessment that addresses the three areas noted in 16 CFR 314.4(b), which are (i) employee training and management; (ii) information systems, including network and software design, as well as information processing, storage, transmission and disposal, and (iii) detecting, **preventing** and responding to attacks, intrusions, or other systems failures; and

Institutional Readiness

<ul style="list-style-type: none">● Who<ul style="list-style-type: none">○ Staff○ Faculty○ Students	<ul style="list-style-type: none">● Why<ul style="list-style-type: none">○ GLBA
<ul style="list-style-type: none">● When<ul style="list-style-type: none">○ Project Timeline○ Possible Phased Rollout	<ul style="list-style-type: none">● What<ul style="list-style-type: none">○ Applications○ Tools

Things that Worked

- Phased Rollout
 - Applications with Personally Identifiable Information (PII)
 - Staff & Faculty
 - Opt-In MFA period
- Promoting through Senior Leadership not within IT
 - Eg., our President made a video about benefits of MFA
 - [Video Link](#)
- Post Go-Live Support - Anticipating FAQs and preparing Service Desk



Two-factor Authentication: Marketing Approach & Lessons Learned

Lorrie Burroughs, Communications
Officer

April 8, 2020

Why Two-Factor at Georgia Tech?

- Successful phishing attacks escalated need for more secure system access
- Many critical applications were secured with a single authentication method using CAS
- Early phases of Two-factor Authentication with Duo for specific applications had been successful in limited release
- Institute directive to implement a multi-factor integrated solution on a more comprehensive scale



Requirements

- Maintain the integrity of Institute data and computing resources
- Build a framework for OIT and campus unit resources to support the roll-out
- Provide two-factor authentication app to faculty, staff, and students
- Leverage familiar access methods with added multifactor capability to ease change impact

Assumptions

- Massive change required
- Need for early adoption by administration first to spur adoption
- Required communicating the need to change behaviors for students, faculty and staff
- Required communicating the process of enrolling and using 2FA to all campus constituents

The MarCom Approach



Communications and Marketing Goal

To communicate a campus-wide requirement to adopt two-factor authentication for accessing Georgia Tech data and assets

Create an Extensive Comm Plan in Phases

Communication Item(s) / Tasks	Recipient	Message Content	Delivery Method	Development Lead	Communicator (i.e. who's it coming from?)	Approval (If needed)
Sidewalk banner	All students	Glad to see you here	In person	LB	OIT	JL, EG
Signage in Dining Halls	Students	Reminder of deadline with link to enrollment instructions	Table Cards	LB	Cyber, LB	JL, EG
Signage on Tech Trolleys	Students	Reminder of deadline with link to enrollment instructions	Email	LB	Cyber, LB	JL, EG
End of Awareness Campaign						
Create Enrollment Campaign	Students	Glad to see you here and Awareness	Table on Walkway	LB	EG, LB	JL, EG
Email to students on what, when, where, etc.	Students	Message 1 of 3: As a follow-up to the previous communication on the potential for cyber attacks on GT resources, we will begin implementing multi-factor authentication...	Email	MM, LB	Cyber, LB	JL, EG
How-to videos on enrolling	faculty, staff	How to enroll	Video	GTIC, LB	Cyber, LB	JL, EG
How to videos on using the app	Students	How to use the app	Video	GTIC, LB	Cyber, LB	JL, EG
How to videos on students enrolling students	Students	How students can enroll each other	Video	GTIC, LB	Cyber, LB	JL, EG
Article in the Technique	Students	Focus on Cyber; hacking event, FBI recommendation, what's in it for students, other campuses using it	Technique			
Determine swag to purchase						
DRAWINGS during Enrollment on Skiles, other areas around campus	Students	Enrolling -names in hat for \$10 Starbucks card	Drawing	LB, Cyber	Cyber, LB	JL, EG
Digital Signage	Students	Use theme/designs from postcards	Digital Signage	LB	Cyber, LB	JL, EG
Article in Daily Digest		Article in Daily Digest on 2FA Enrollment Deadline for Students	DD			
		Message 2 of 3: As a follow-up to the previous				

- Phase VI A&F
- Phase VII Enrollment Services
- Phase VIII Faculty and Staff
- Phase VIII Students
- All campus CSRs, Faculty, Staff
- +

Create a Communications Toolkit

- PowerPoint presentations
- Website – navigated by audience
- Video
- Direct email
- Postcards
- Banners
- Dining Hall cards
- Bus and Trolley signs
- Poster
- T-shirts
- Social media

Next Steps

Create brand awareness through
easy-to-identify graphic across deliverables



Brand Identification

“Peace of Mind with 2FA”



Create a Website

- Easy to remember URL (2fa@gatech.edu)
- Overview of 2FA
- Multi-media with “how to enroll” video
- Pages for students, faculty and staff
- News updates as new technology is rolled out

Georgia Tech Two-Factor Authentication

Home About Us For Students For Faculty For IT Support Staff FAQs Employee CONTACT US

CT Home

Self-enroll in Two-factor Authentication

READ MORE

Welcome to Two-Factor Authentication

Georgia Tech considers the security and privacy of employee and student information to be of utmost importance. To keep our information safe, the Institute requires that all students, faculty, and staff use two-factor authentication when accessing campus services and systems. This is a new standard that strengthens the protection of employee and student data and will maintain compliance with University System Information Security policy.

The "Using Two-factor Authentication with Duo at Georgia Tech" video offers a quick overview of how two-factor works and how to use two-factor authentication as well as the methods you can use for authenticating your "second" factor.

Using Two-factor Authentication with Duo at Georgia Tech

Watch Video Download

Georgia Tech Office of Information Technology

To read more about this initiative, go to the full news article.

For Employees, contact your IT lead or visit the Technology Support Center (TSC) located in Clough Commons, Room 215.

Students

Learn more about two-factor authentication including how to use Duo's self-enroll video series.

Learn More

Employees

Learn more about how to enroll in two-factor authentication using Duo.

Learn More

Resources and Training

Discover guides and videos on using two-factor authentication in procedures areas.

Learn More

Work with a Project Manager

- The PM identified stakeholders and created standing meetings every week for 18 months
- Ran meetings
- Met with individual stakeholders
- Used the Communications Toolkit
- Provided stakeholders with what they needed to bring success to their unit's enrollment

Work with Stakeholders

COLLABORATION



Use Different Assets for Specific Audiences

- In-person presentations to President, VP, Provost, etc.
- Direct emails to faculty and staff (counting down the deadline to comply)
- Campus news outlets for overall campus outreach
- Numerous platforms to reach students

Reaching 2nd Tier – Faculty and Staff

As deadline to move to 2FA approached, more faculty/staff enrolled

Effect of Targeted Emails to Non-Enrolled Employees on Two-Factor Enrollment Rates

DELIVERABLES - Over 15 announcements, articles and emails to campus since 4/16 and website was created

COLLABORATIONS - Tech communicators & IT leads, Project Managers, Two-Factor Steering Committee, Tech Institute Communications



Reaching Students – Start with Early Adopters – Incoming First-years at Orientation

ENHANCED SECURITY PEACE OF MIND

TWO-FACTOR AUTHENTICATION WITH DUO SECURITY

Using two factors of identification creates a much **stronger protection** than a pass word alone.

Hesitant? Once enrolled, your password remains the same for the entire year!

STUDENT DEADLINE:
Oct. 16, 2017

Visit TSC (Clough Commons) Or
Wreck Techs to get started!



Georgia Tech Office of Information Technology



Step 1 - Log In
(What you know)

Step 2 - Validate
(What you have)

SUCCESS!

Choose your authentication method

PUSH

PHONE CALL

PASSCODE



Georgia Tech considers the security and privacy of our students' information to be of utmost importance. Using two factor identification will create a much stronger protection than a password alone.

Reaching Incoming Students: Results of “How to” Video URL on Postcard

Web Traffic & Number of Page Views from
Students (June-October)

OVERALL: 51,194 PAGE VIEWS

2,500 VIEWS



Other Marketing Efforts to Students Coming Back to School – Walkway Sign

Enrollment table with T-shirt giveaways to students who enroll on the spot

**GLAD TO SEE
YOU HERE!**

Ready to enroll?
Got questions?
Need to know more?

[2FA.GATECH.EDU](https://2fa.gatech.edu)



Results

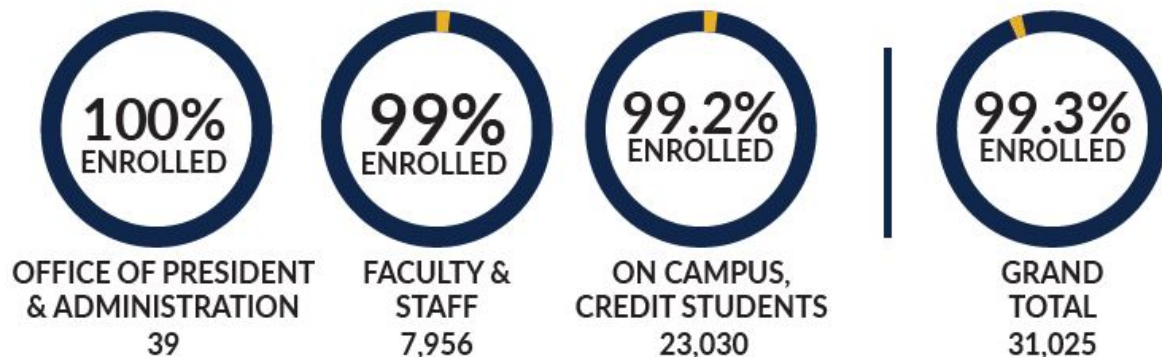
OBJECTIVES

Implement a communications tool

Engage campus stakeholder

Leverage teamwork through collaboration

The implementation of Two-factor Authentication was/is being implemented in the following order:



Lessons Learned



What We Could Have Done Better

- Take more time to reach students in channels where they go for information
- Work with student organizations
- Be mindful of students who don't live on campus (may not see marketing collateral or articles)
- When you think you've communicated enough, communicate more

Expand Student Enrollment Deadline

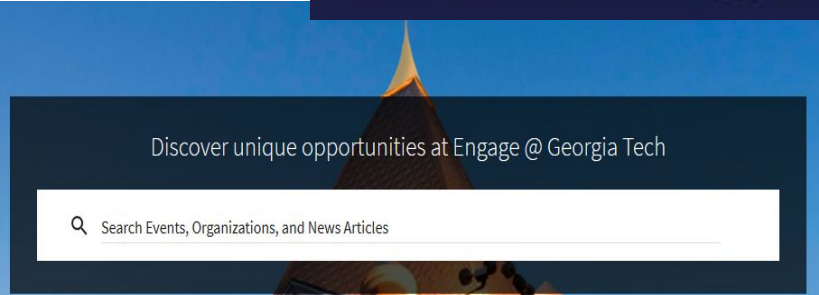
We only had 8 weeks to enroll over 23k students.....

We had over a year to enroll faculty and staff



Remember Student Commuters

Take more time to reach students in channels where they go for information

The logo features a large, white, serif letter 'T' on a dark blue rectangular background. To the right of the 'T', the word 'technique' is written in a white, lowercase, sans-serif font.A screenshot of a search bar interface. The background is a photograph of a building with a sign that says 'TECH'. Overlaid on this is a dark blue rectangular box containing the text 'Discover unique opportunities at Engage @ Georgia Tech' in white. Below this text is a white search input field with a magnifying glass icon on the left and the placeholder text 'Search Events, Organizations, and News Articles'.

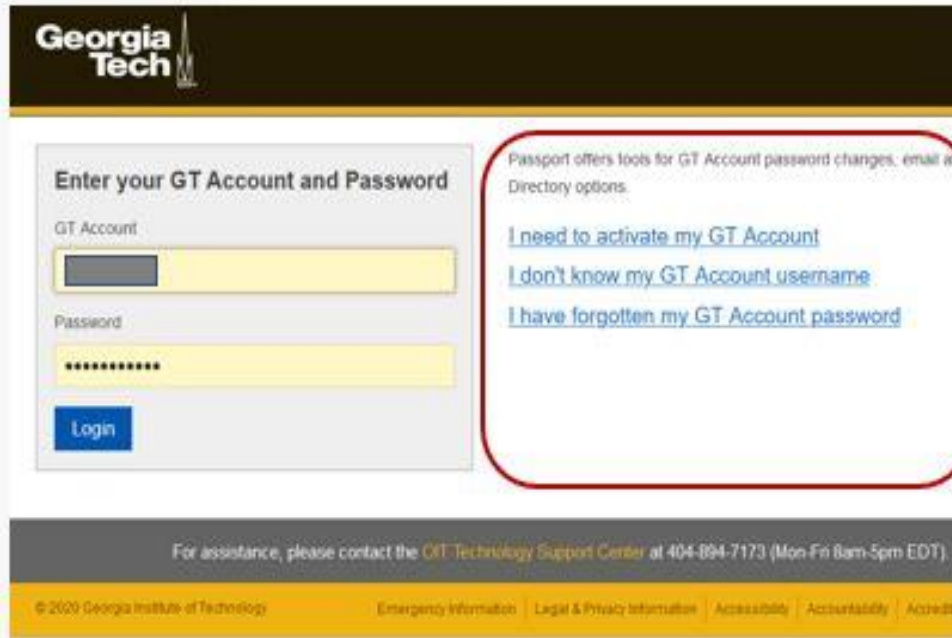
canvas

Push Out New Features Quickly

- Create a two-page “how to” guide that can be downloaded and printed
- As OIT and IT staff developed new ways to enroll (self-enrollment, enroll a friend, etc.) push out this information in direct emails, tables, word of mouth and other distribution channels
- Use IT staff in campus housing to help students enroll using the latest technologies
- Remind all users to print back-up codes!!!!

Use CAS for Immediate Messaging

Utilize login page for broad announcement of deadline and link to resources



The image shows a screenshot of the Georgia Tech login page. At the top left is the Georgia Tech logo. Below it is a section titled "Enter your GT Account and Password" with input fields for "GT Account" and "Password", and a "Login" button. To the right of the login form is a red-bordered box containing the text: "Passport offers tools for GT Account password changes, email at Directory options." followed by three blue hyperlinks: "[I need to activate my GT Account](#)", "[I don't know my GT Account username](#)", and "[I have forgotten my GT Account password](#)". At the bottom of the page, there is a footer with contact information for the GT Technology Support Center and a copyright notice for Georgia Institute of Technology.

Work with OIT Stakeholders Throughout the Campaign

- There was no “official” project sponsor of our roll-out
- Cyber Security took over the role so work with a team who has the most authority in the eyes of administration.

Communicate, communicate, and communicate!

Lorrie Burroughs
Georgia Institute of Technology
lorrie.burroughs@gatech.edu

May IAM Online

May 13, 2020 - 2 pm ET | 1 pm CT | Noon MT | 11 am PT

Seamless Access to Scholarly Resources

Seamless Access was developed by a group of stakeholders from identity providers and service providers, libraries, and publishers to provide a convenient way for researchers to access digital scholarly content and services.

InCommon Trusted Access Platform Training

<https://incommon.org/academy/software-training/>

Software Component	Virtual Training Dates	Early-Bird Rate Deadline
COmanage	May 19-20, 2020	April 17, 2020
Grouper	June 2-3, 2020	May 8, 2020
midPoint	June 16-18, 2020	May 15, 2020

IAM Online Evaluation

<https://www.surveymonkey.com/r/IAMOnline-April-2020>