BCNET

Shared IT Services for Higher Education & Research

Conference 2017

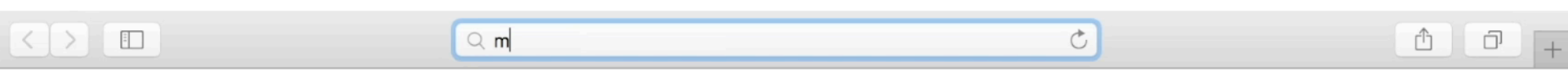
Keeping the “single” in single sign-on

Sean Feil

University of Calgary

Video

"The dream"


m

Sean Feil

Identity, Messaging, and Middleware

UNIVERSITY OF CALGARY
Information Technologies

- Why is usability so important for security?
- Does Single Sign-on help with usability? security?
- What challenges are there with building a truly Single Sign-on environment?

Usability

Nielsen Norman Group

Learnability

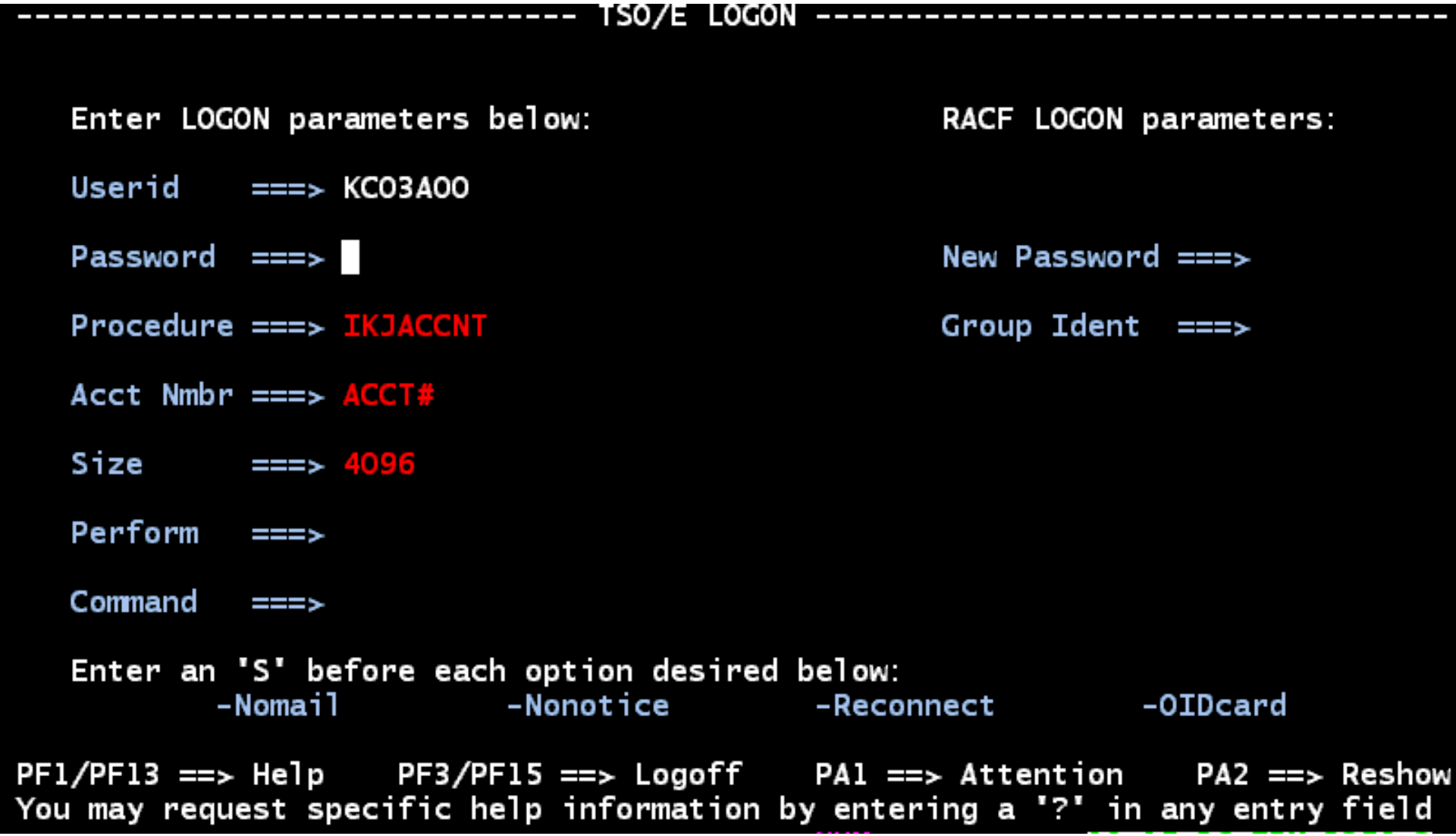
Efficiency

Memorability

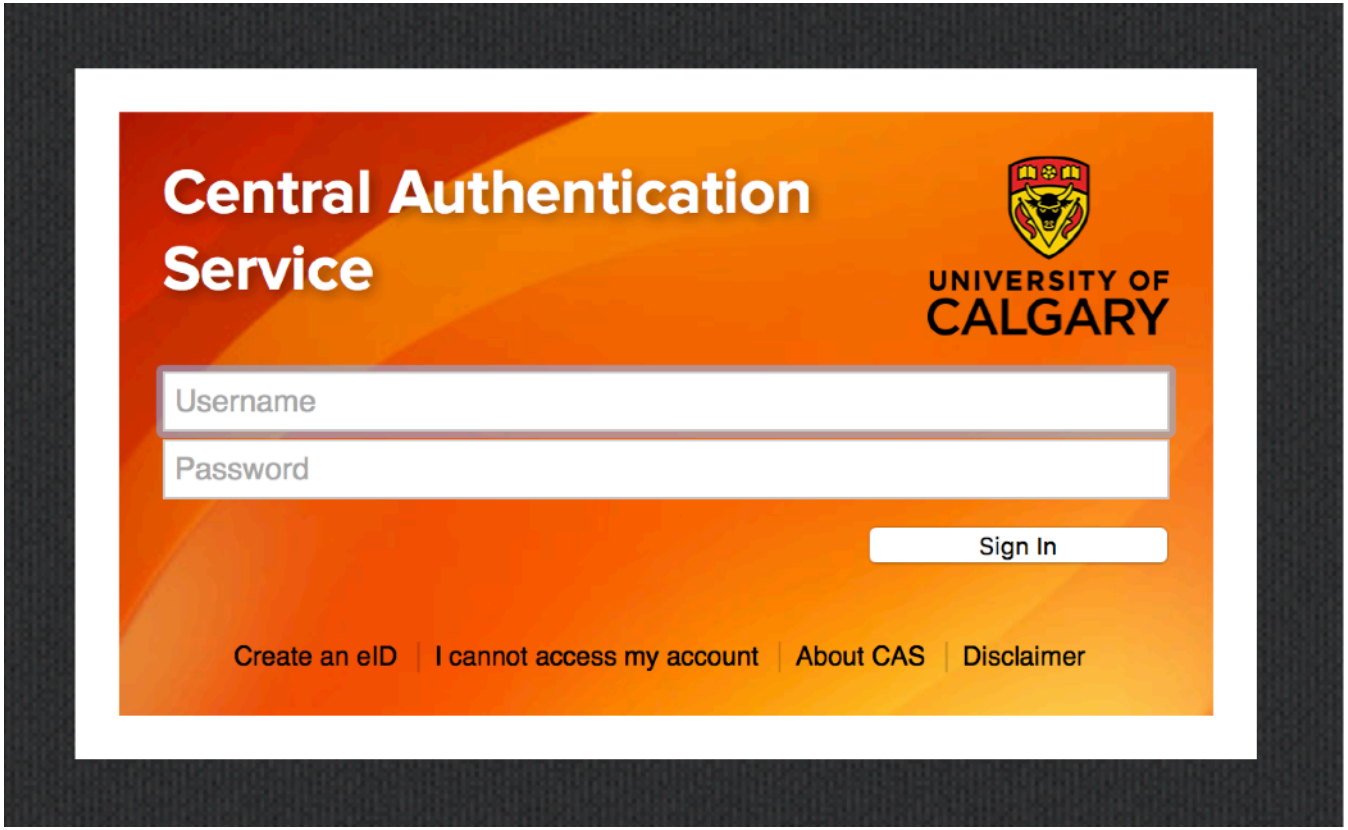
Errors

Satisfaction

Nielsen Norman Group


TSO/E LOGON
Enter LOGON parameters below:
RACF LOGON parameters:
Userid ===> KC03A00
Password ===>
New Password ===>
Procedure ===> IKJACCNT
Group Ident ===>
Acct Nmbr ===> ACCT#
Size ===> 4096
Perform ===>
Command ===>
Enter an 'S' before each option desired below:
-Nomail
-Nonotice
-Reconnect
-OIDcard
PF1/PF13 ==> Help
PF3/PF15 ==> Logoff
PA1 ==> Attention
PA2 ==> Reshow
You may request specific help information by entering a '?' in any entry field

softsmith


Central Authentication Service
UNIVERSITY OF CALGARY
Username
Password
Sign In
Create an eID
I cannot access my account
About CAS
Disclaimer

Usability

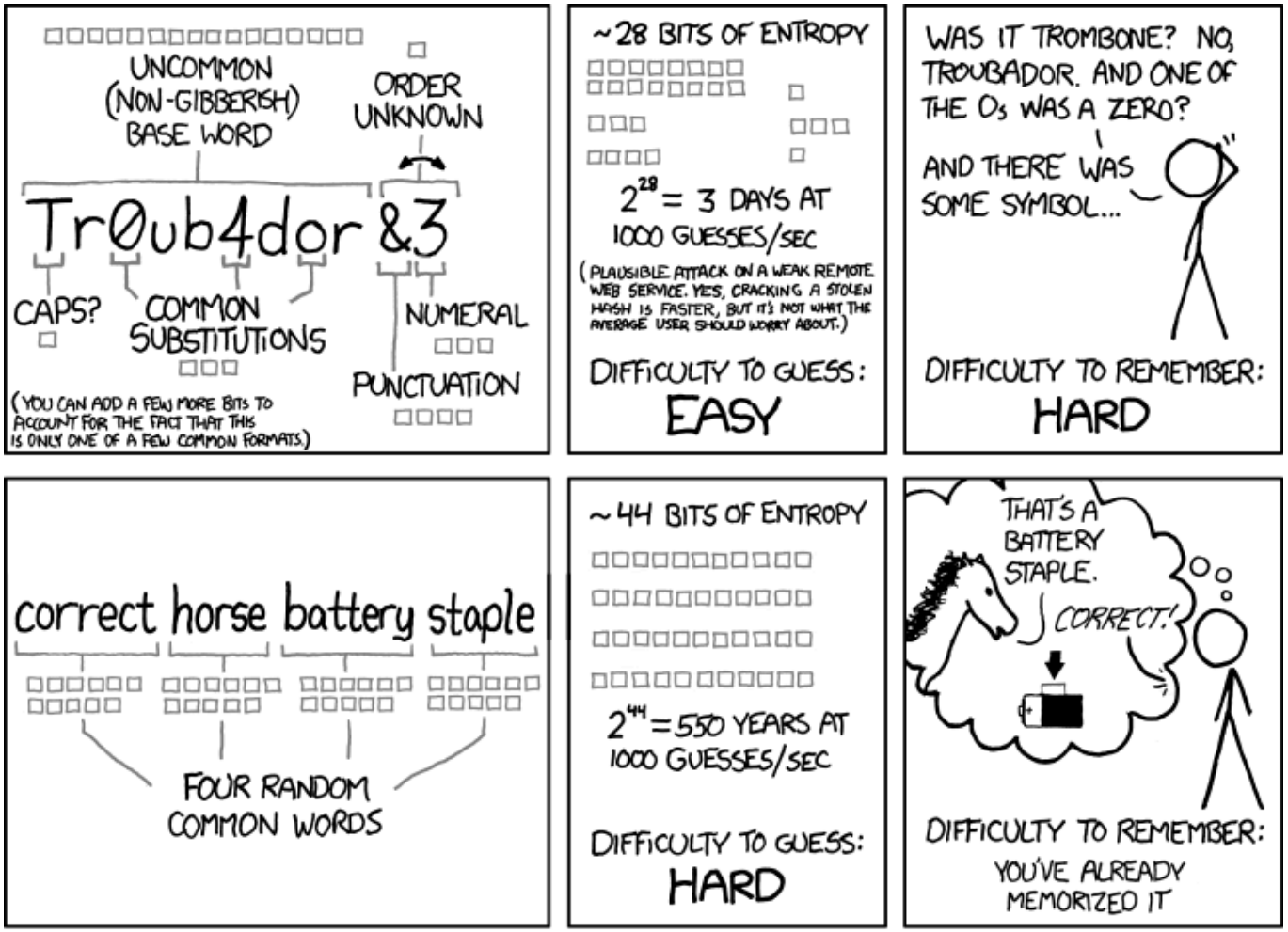
Accessibility

Security

AviD's Rule of Usability:

Security at the expense of usability comes at the expense of security.

https://security.stackexchange.com/a/6116



https://xkcd.com/936/

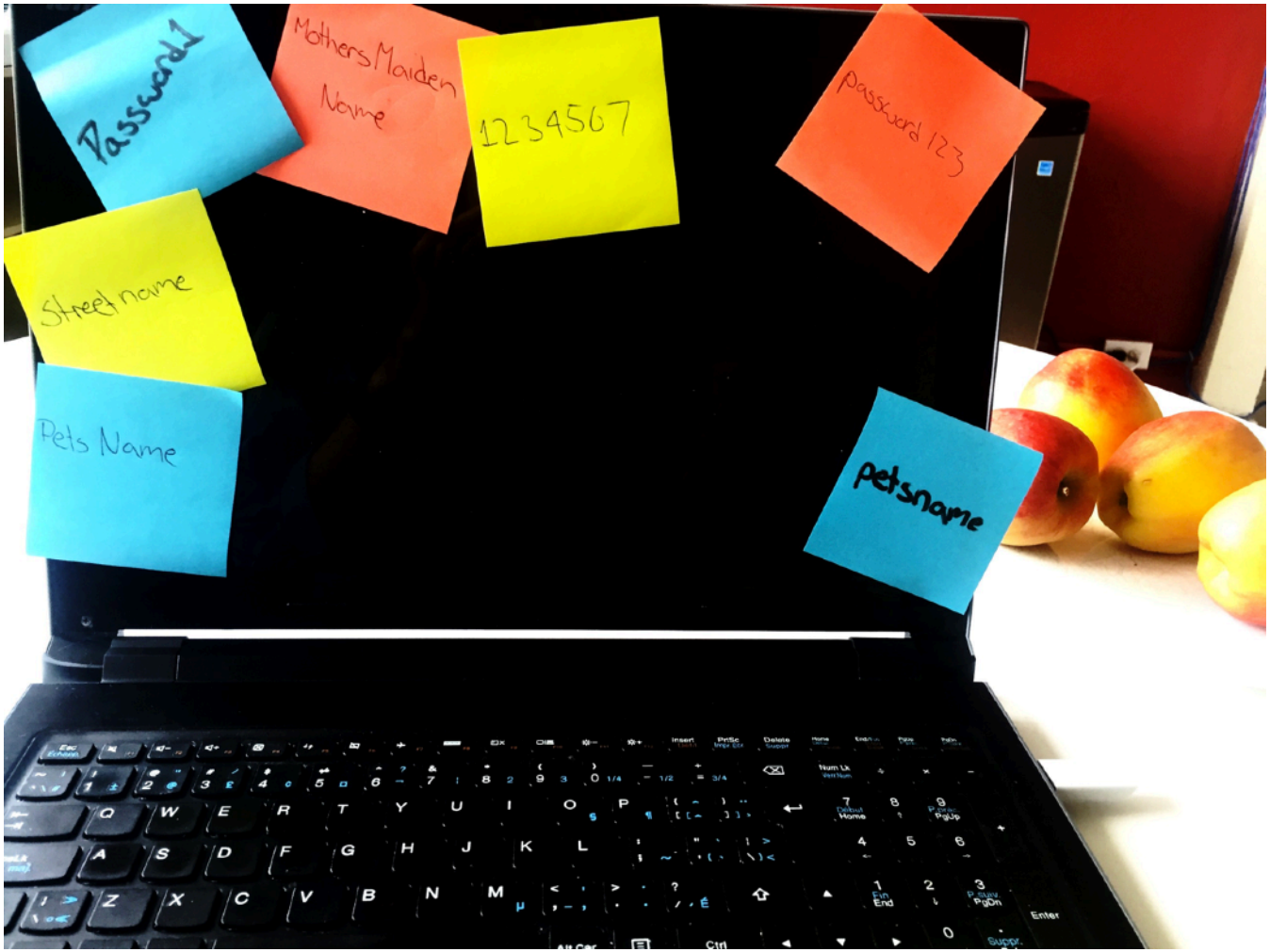
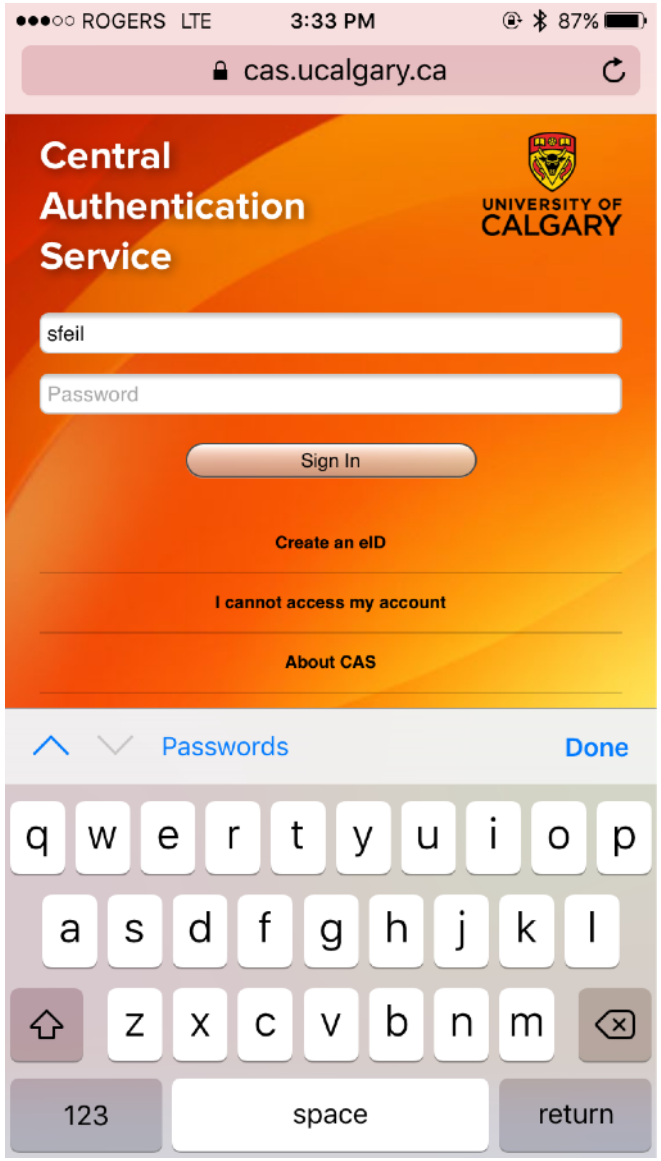


Image from https://www.vendasta.com/


●●●○○ ROGERS LTE
3:33 PM
87%
cas.ucalgary.ca
Central Authentication Service
UNIVERSITY OF CALGARY
sfeil
Password
Sign In
Create an eID
I cannot access my account
About CAS
Passwords
Done
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
123
space
return

Upgrade Form

* Email Address

* Password

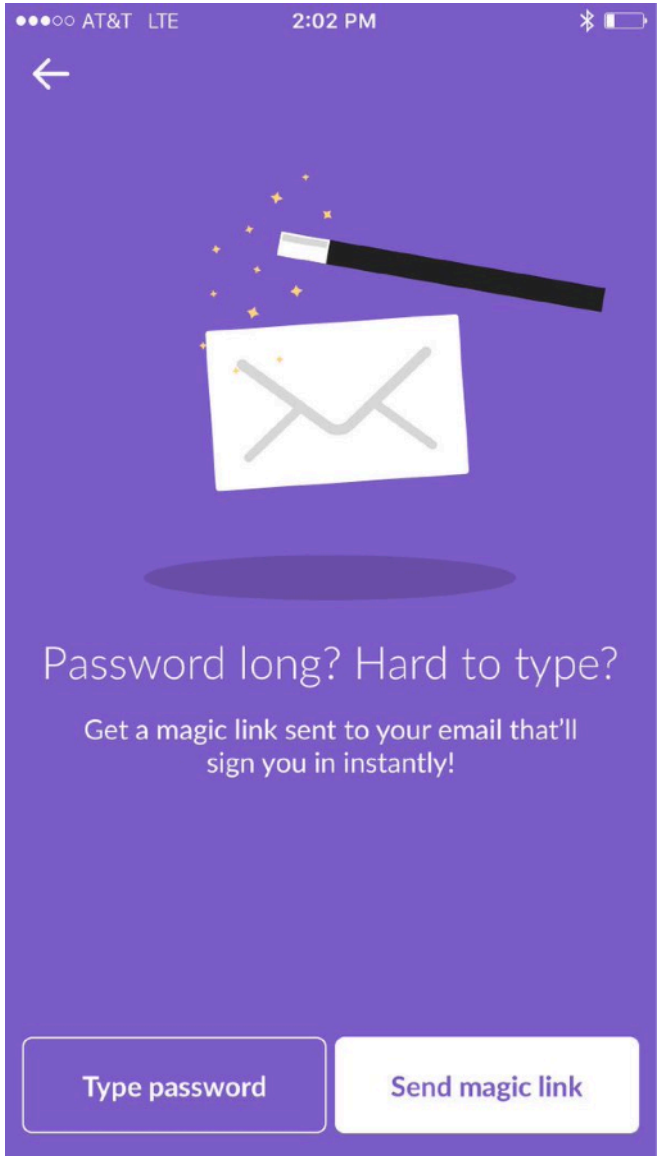
* Verify Password

* Country

* First name/Last name

Submit

Compose your survey with www.my4m.com


●●●○○ AT&T LTE
2:02 PM
Password long? Hard to type?
Get a magic link sent to your email that'll sign you in instantly!
Type password
Send magic link

Slack

Apple

…making something as important as security so effortless, so simple. We believe that technology is at its very best, at its most empowering, when it simply disappears.

- Jonathan Ive, 2013

09 Aug 2011

67 Percent of Consumers Don't Have Password Protection on Their Mobile Phones

IT security and data protection firm Sophos today published findings of independently commissioned research by TNS, which reveals consumer attitudes toward mobile security and data loss prevention. Although almost a quarter of consumers (22%) have lost a mobile phone in the past, and a further 12% have had a phone stolen, 67% don't have passwords set up on their mobile phones to protect stored data.

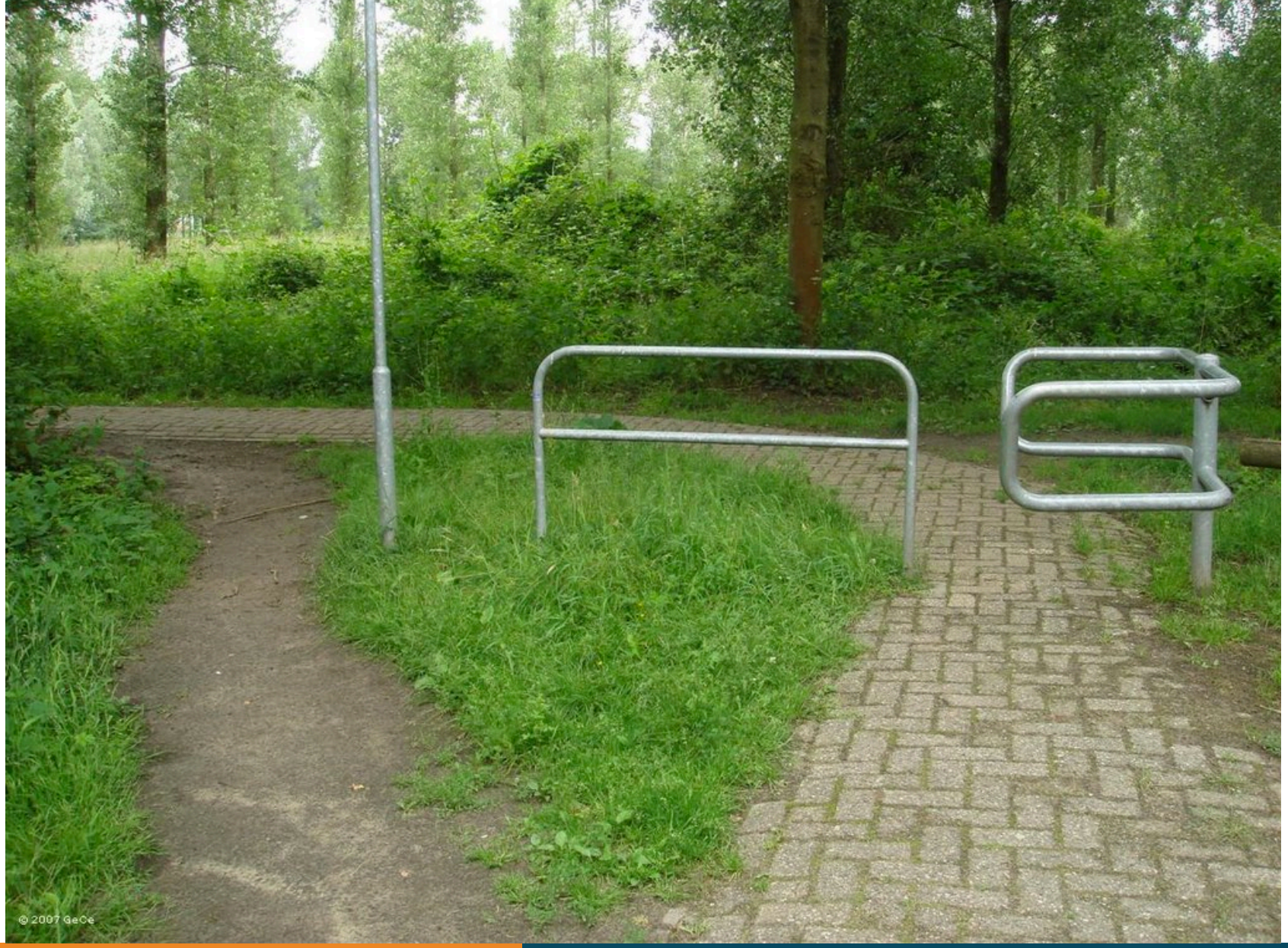
60% of those surveyed acknowledged that device theft or loss was the biggest security threat to mobile devices; however, only 57% have password protection enabled even on their laptops, with 18% admitting to using the same password for everything.

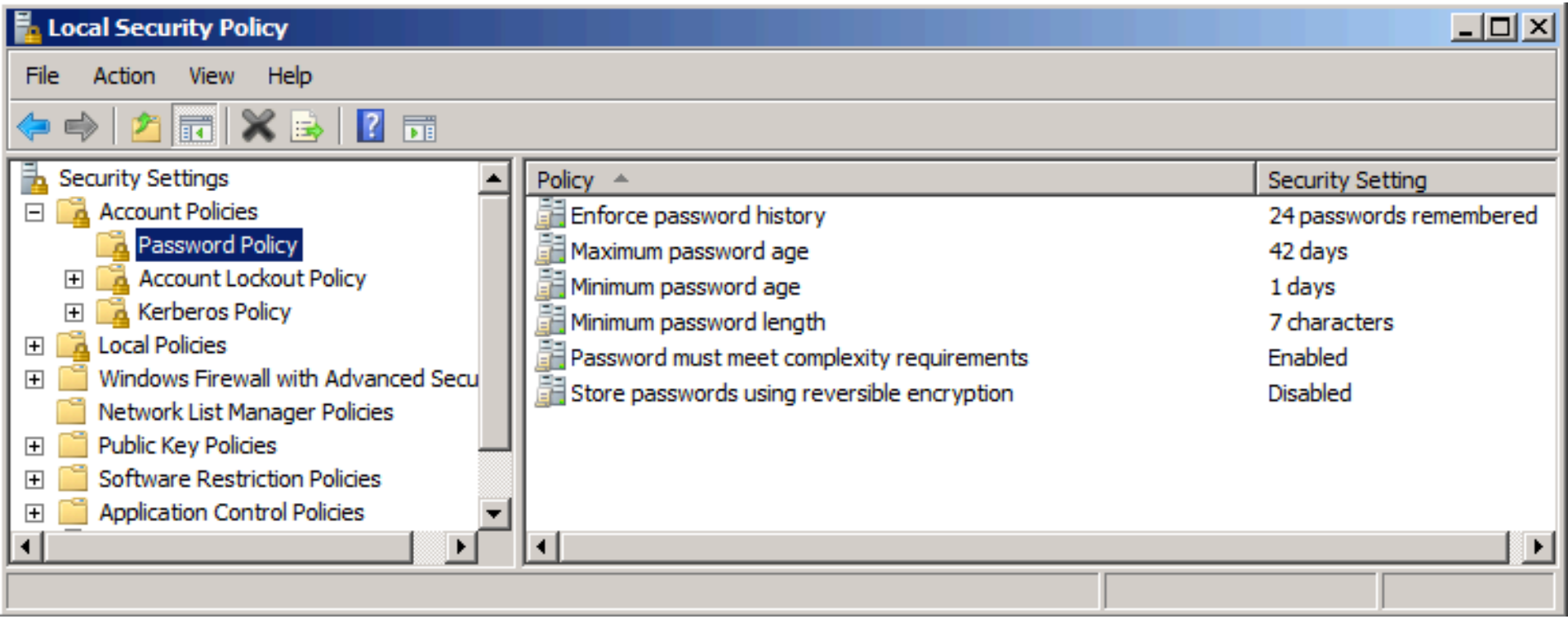
Sophos

Macworld

Please enter your phone number:

(216) 409-9989 + Submit


© 2007 GeCe


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
Policy
Security Setting
Enforce password history
24 passwords remembered
Maximum password age
42 days
Minimum password age
1 days
Minimum password length
7 characters
Password must meet complexity requirements
Enabled
Store passwords using reversible encryption
Disabled

Problem?

CAS

Azure Active Directory

Shibboleth

Microsoft
Active Directory
Federation Services

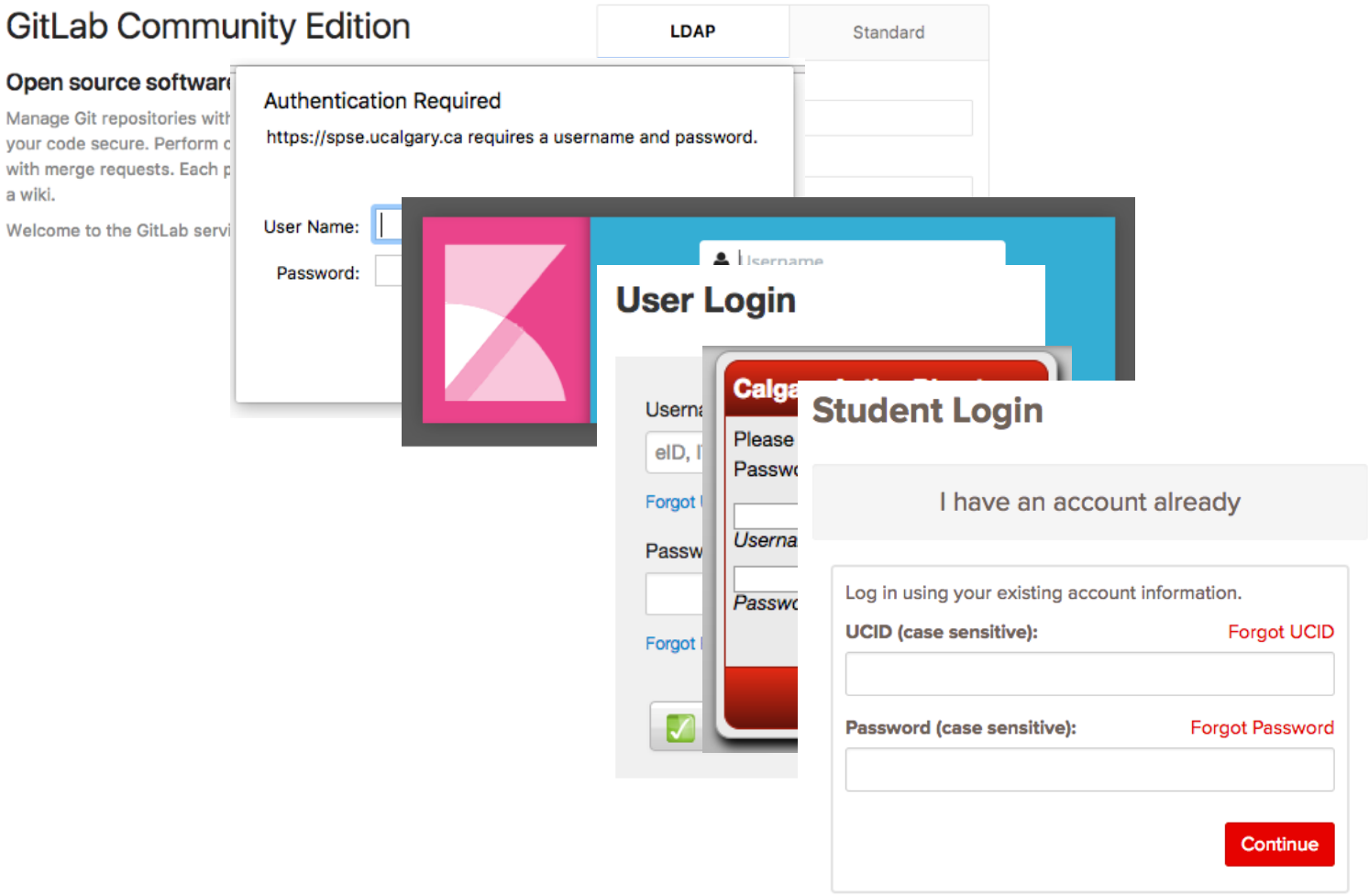
OpenLDAP

Microsoft
Active Directory

Passwords stored in internal databases somewhere??

(I really hope not but probably)

Central Authentication Service
UNIVERSITY OF CALGARY
Username
Password
Create an eID | I cannot access my a
Login Service
UNIVERSITY OF CALGARY
Please enter your UCalgary email address and password:
Example: username@ucalgary.ca
Ucalgary email address
Password:
Password
I cannot access my account | IT
Outlook
UNIVERSITY OF CALGARY
Security (show explanation)
This is a public or shared computer
This is a private computer
Use the light version of Outlook Web App
User name:
Password:
Sign in
Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.

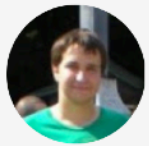

GitLab Community Edition
LDAP
Standard
Open source softwar
Manage Git repositories with
your code secure. Perform c
with merge requests. Each p
a wiki.
Welcome to the GitLab servi
Authentication Required
https://spse.ucalgary.ca requires a username and password.
User Name:
Password:
User Login
Student Login
I have an account already
Log in using your existing account information.
UCID (case sensitive):
Forgot UCID
Password (case sensitive):
Forgot Password
Continue

Who does this well?

Google

One account. All of Google.

Sign in to continue to Gmail



Sean Feil

Password

Sign in

Stay signed in Forgot password?

Sign in with a different account

One Google Account for everything Google

Log in as Sean Feil

****@****.com · Not You?

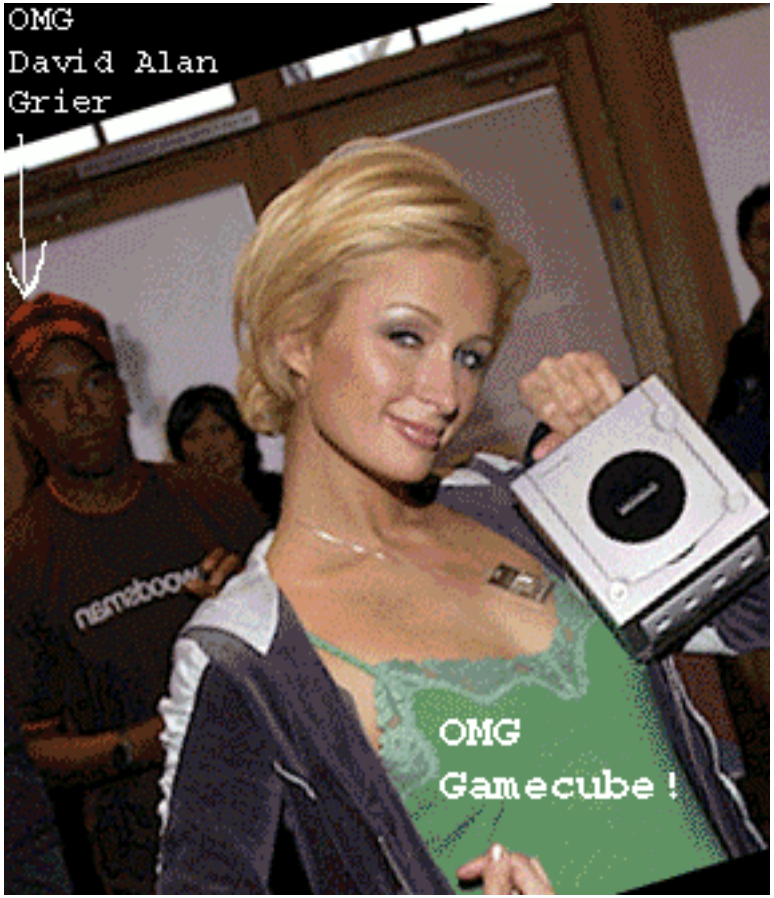
Email or Phone Number

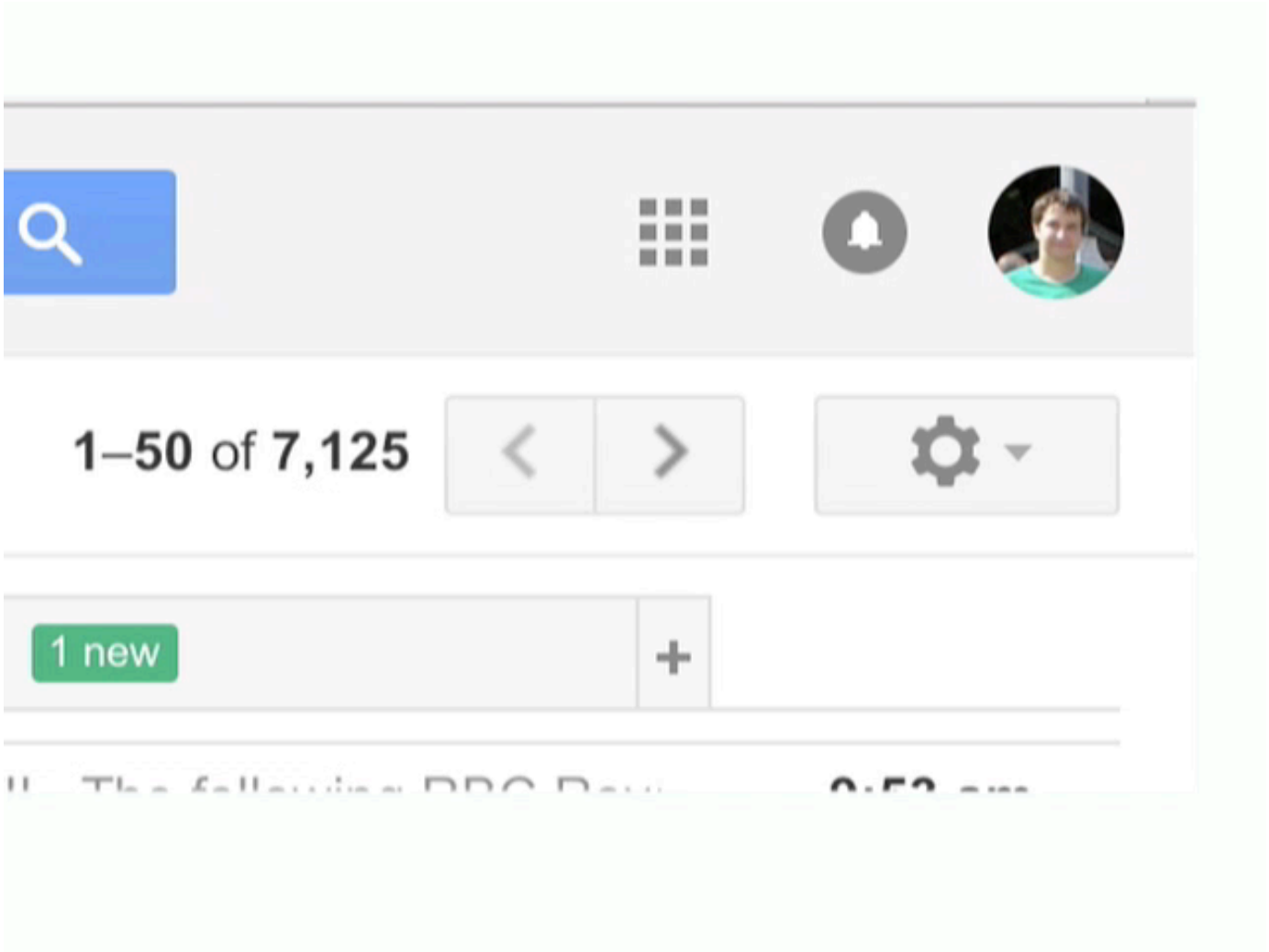
Password

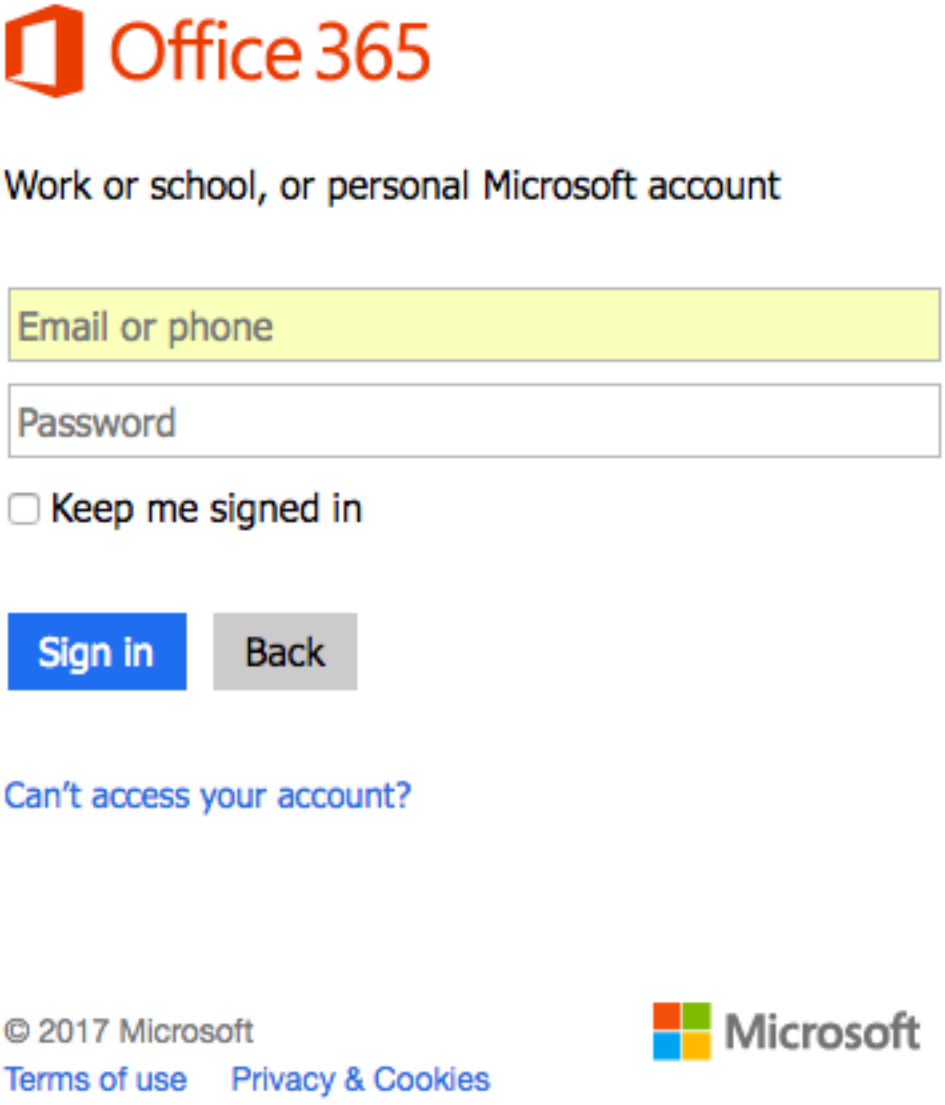
Log In

Recover Your Account

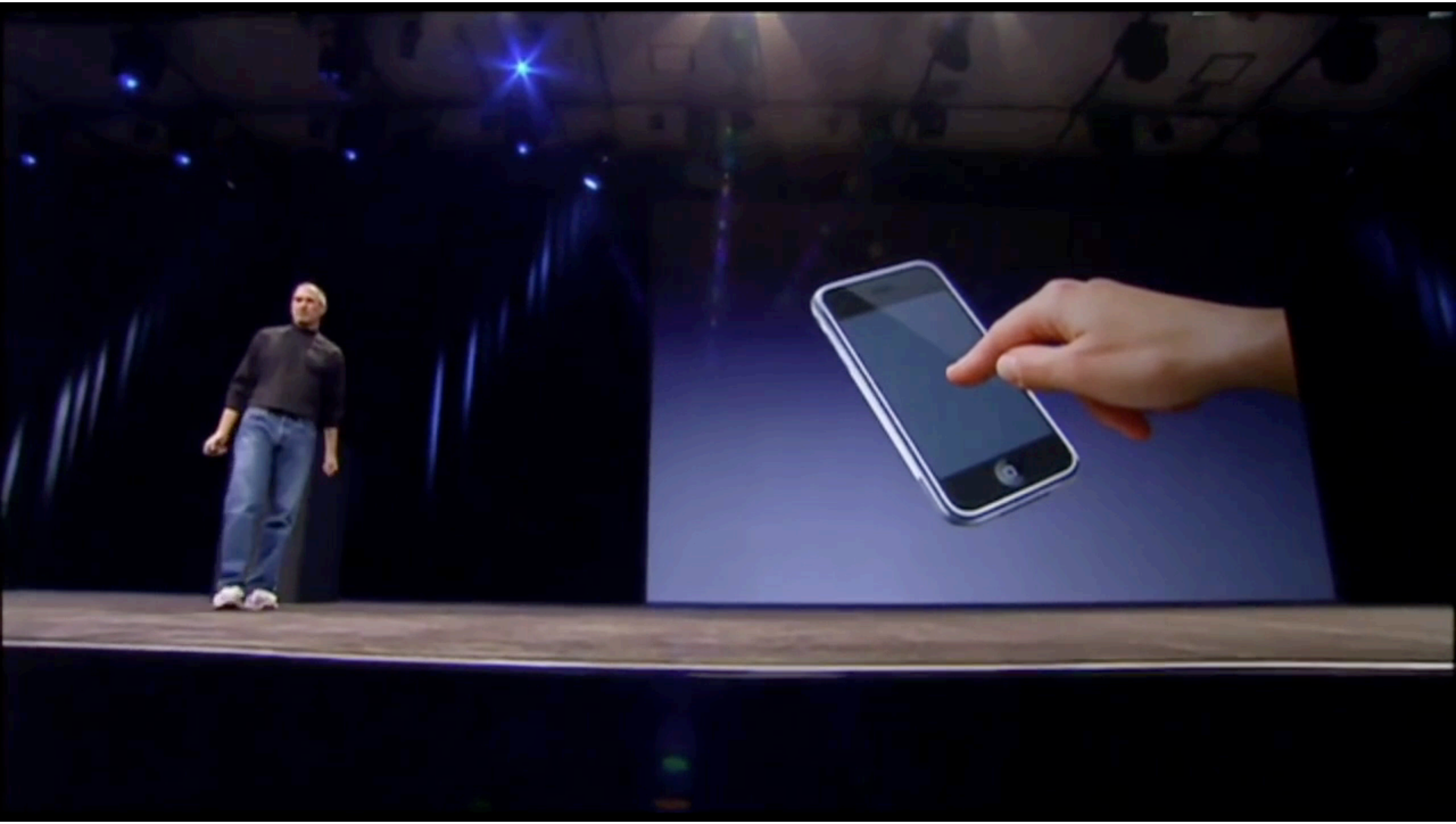
Sign up for Facebook


OMG
David Alan
Grier
OMG
Gamecube!


1–50 of 7,125
1 new


Office 365
Work or school, or personal Microsoft account
Email or phone
Password
Keep me signed in
Sign in
Back
Can't access your account?
© 2017 Microsoft
Terms of use
Privacy & Cookies
Microsoft

NORTH
AMERICA
EUROPE
CAS

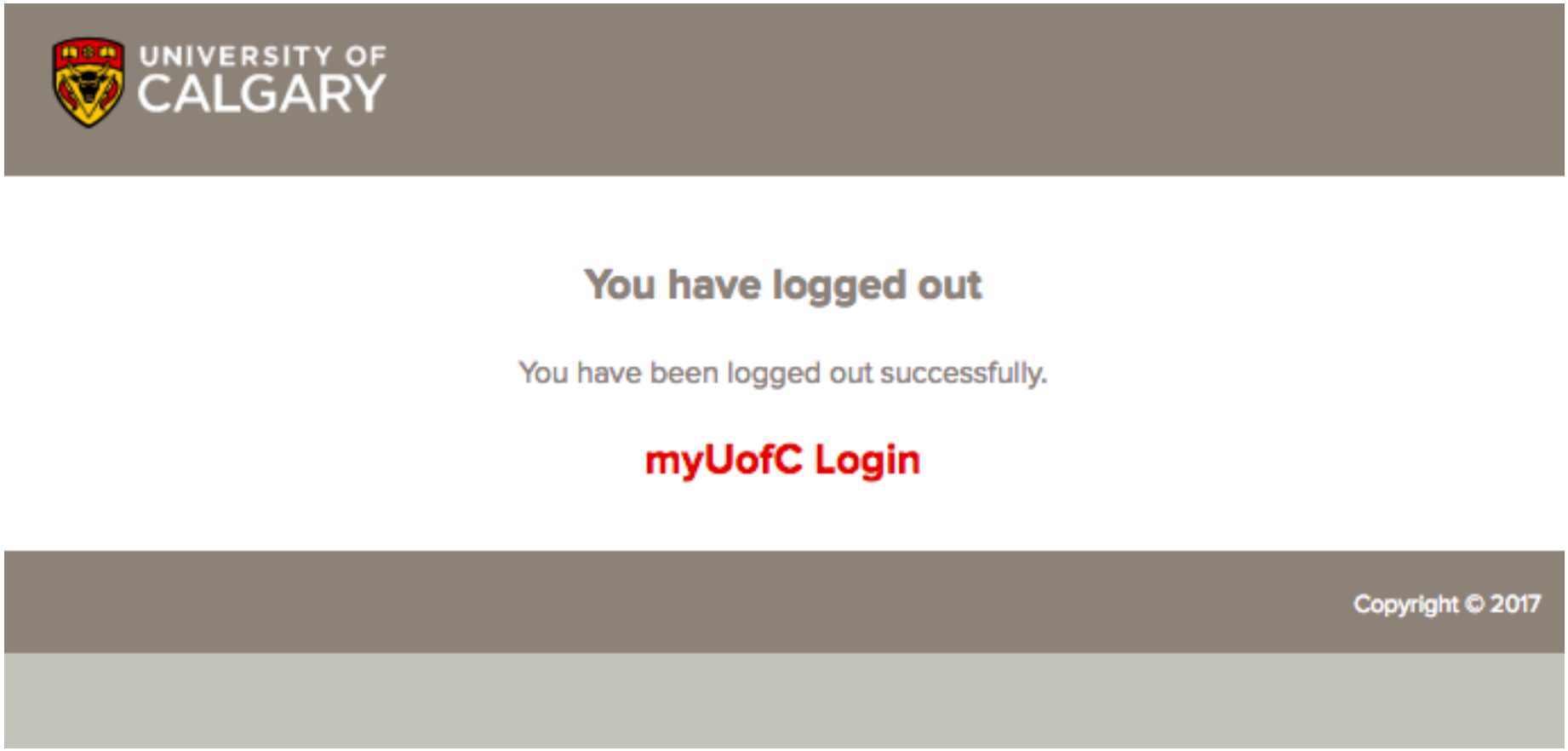


Apple

eduGAIN
PIMS
CareerLink
Shibboleth.
Central Authentication Service
UNIVERSITY OF CALGARY
Username
Password
Sign in
Create an eID | I cannot access my account | About CAS | Disclaimer
CAS
servicenow
COGNOS
Azure Active Directory
ORACLE
PEOPLESOFT
Office 365

Single Sign-on Rules

- Sign in once
- Sign out once
- Prompt the user only for new information

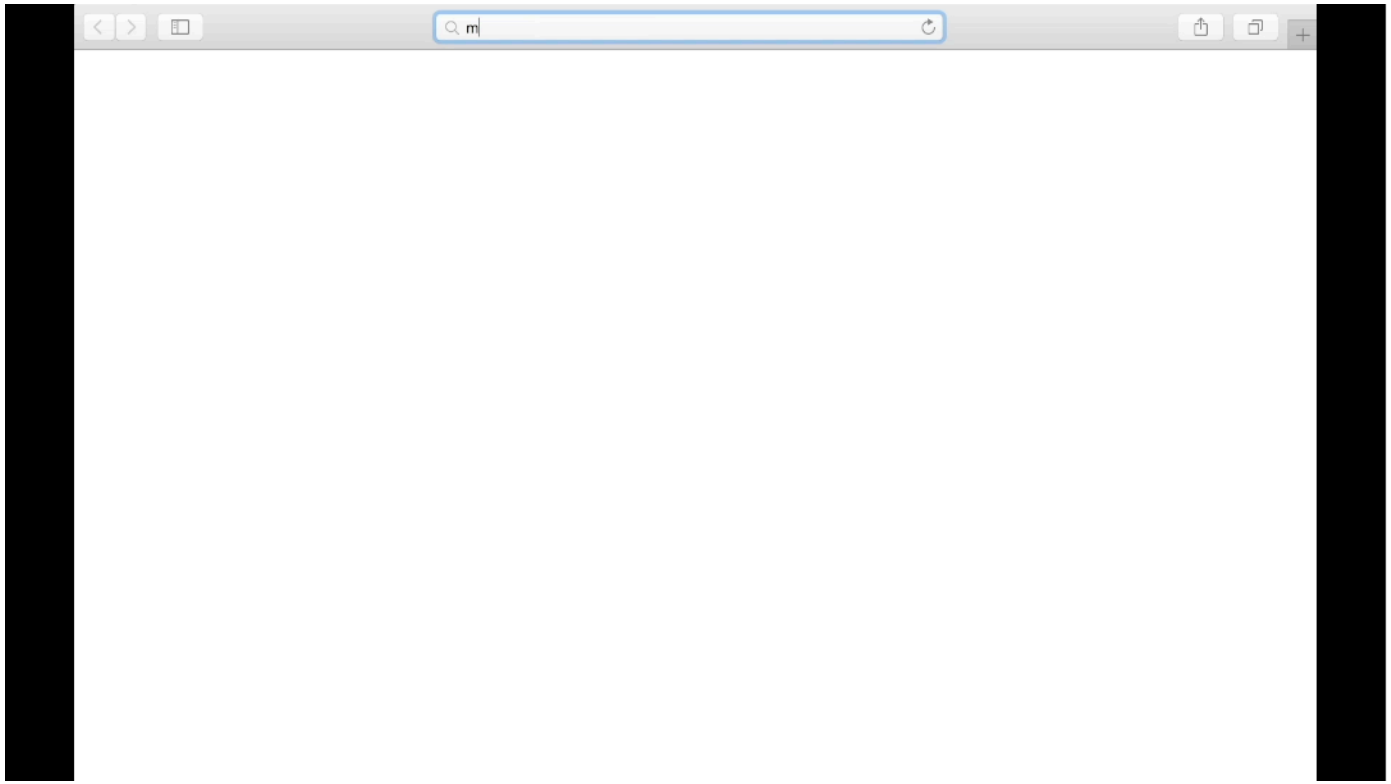

UNIVERSITY OF CALGARY
You have logged out
You have been logged out successfully.
myUofC Login
Copyright © 2017

Video review

“The dream”

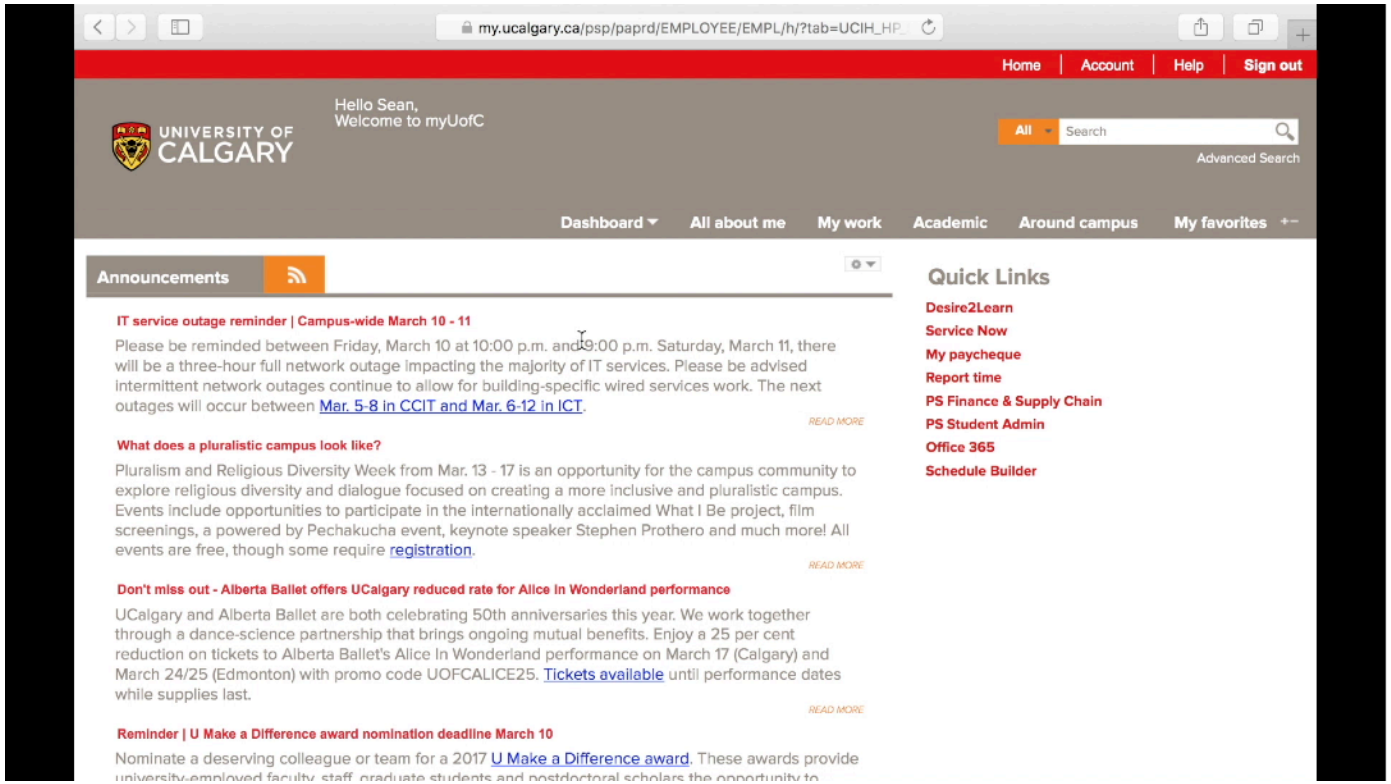
PeopleSoft Portal

CAS



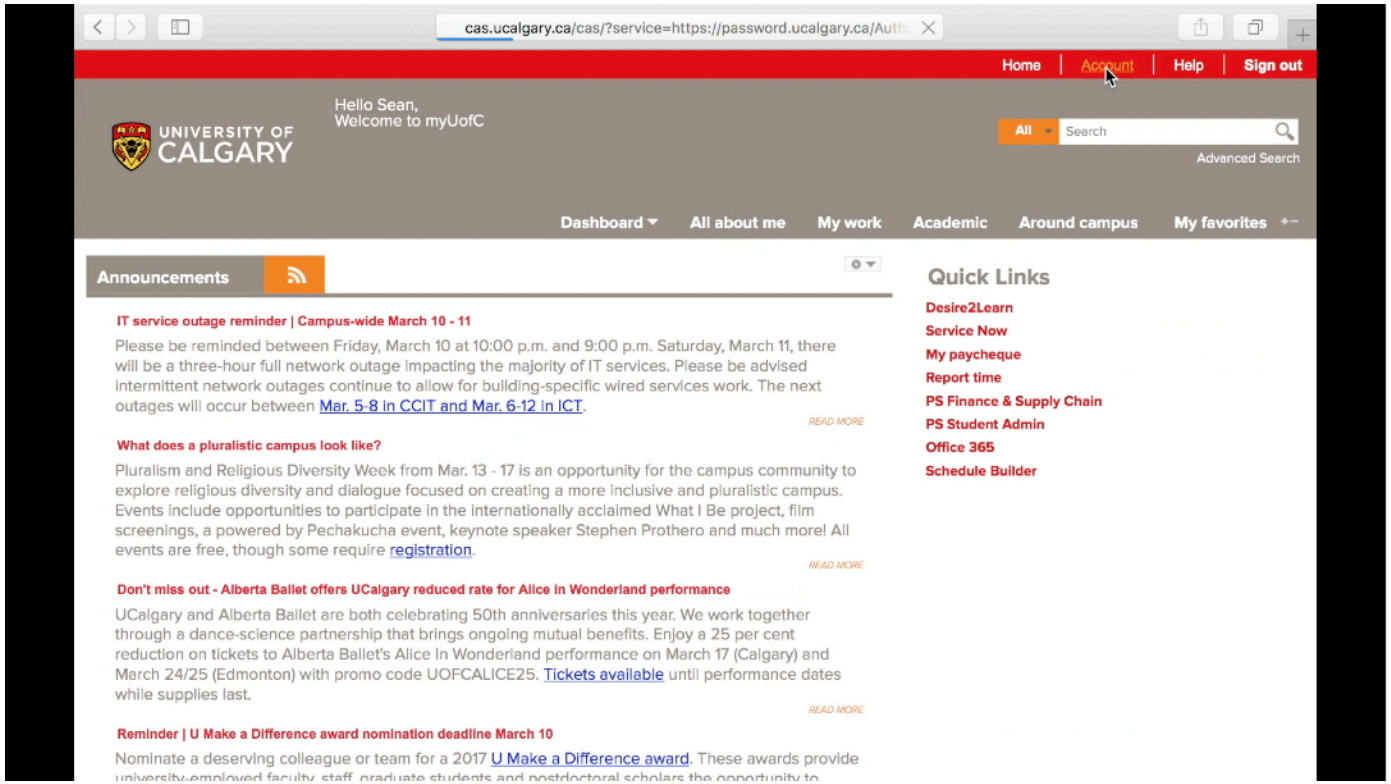
PeopleSoft Finance

PeopleSoft SSO



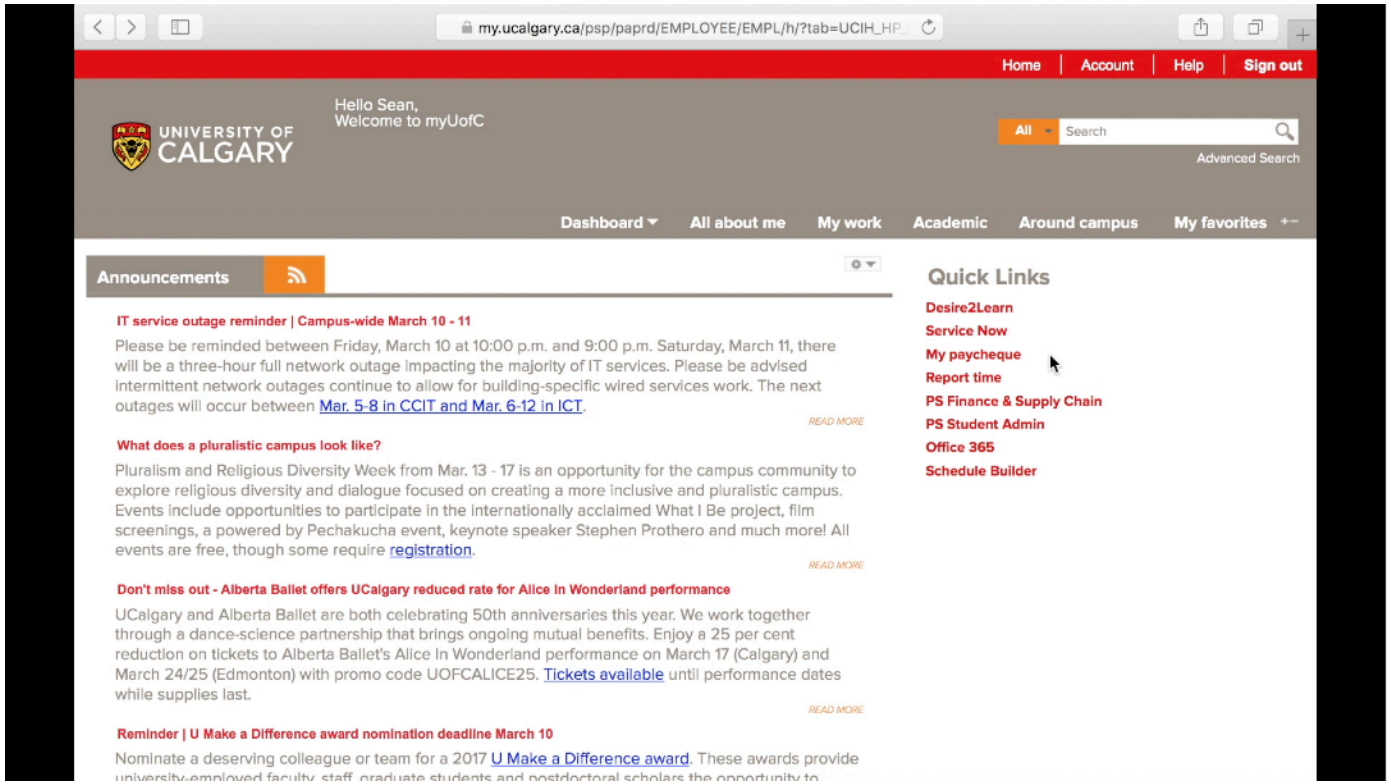
Password Management

CAS



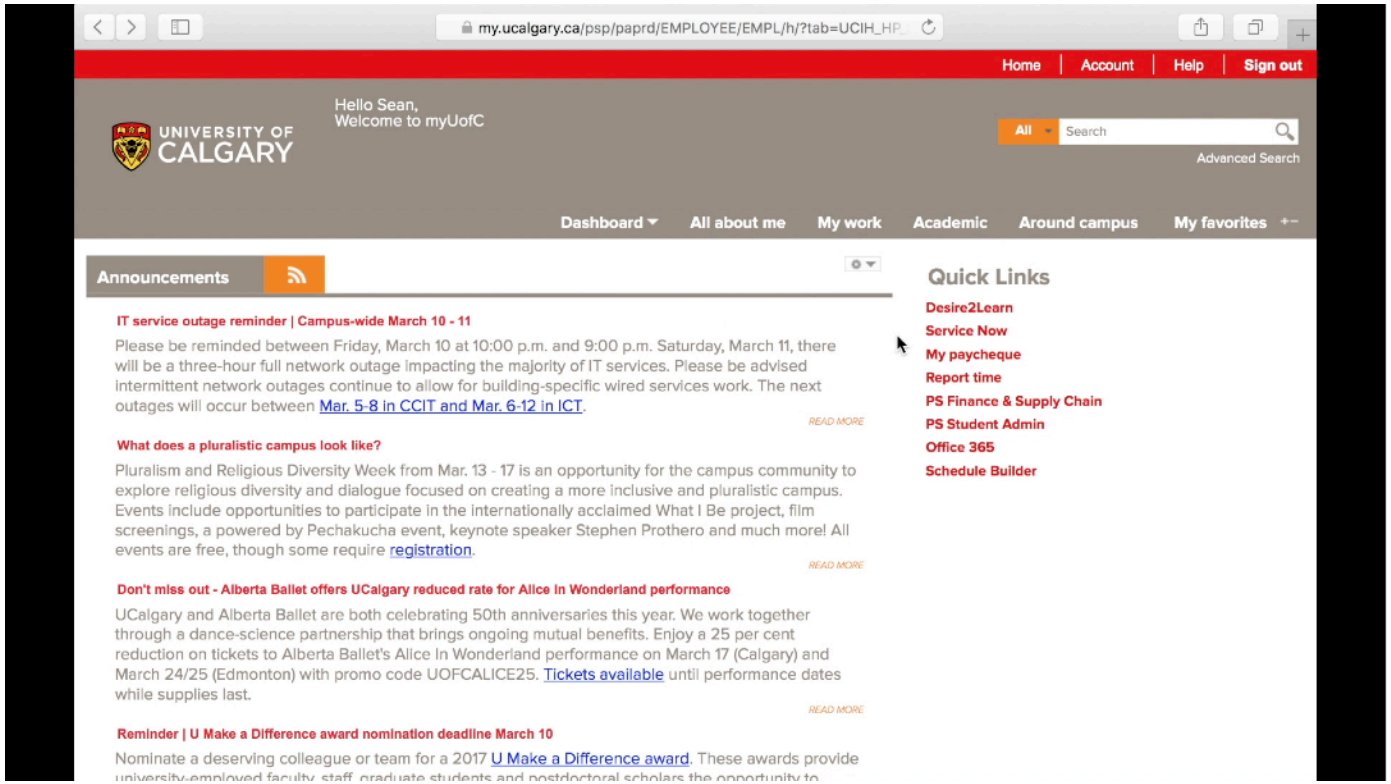
Desire2Learn

CAS



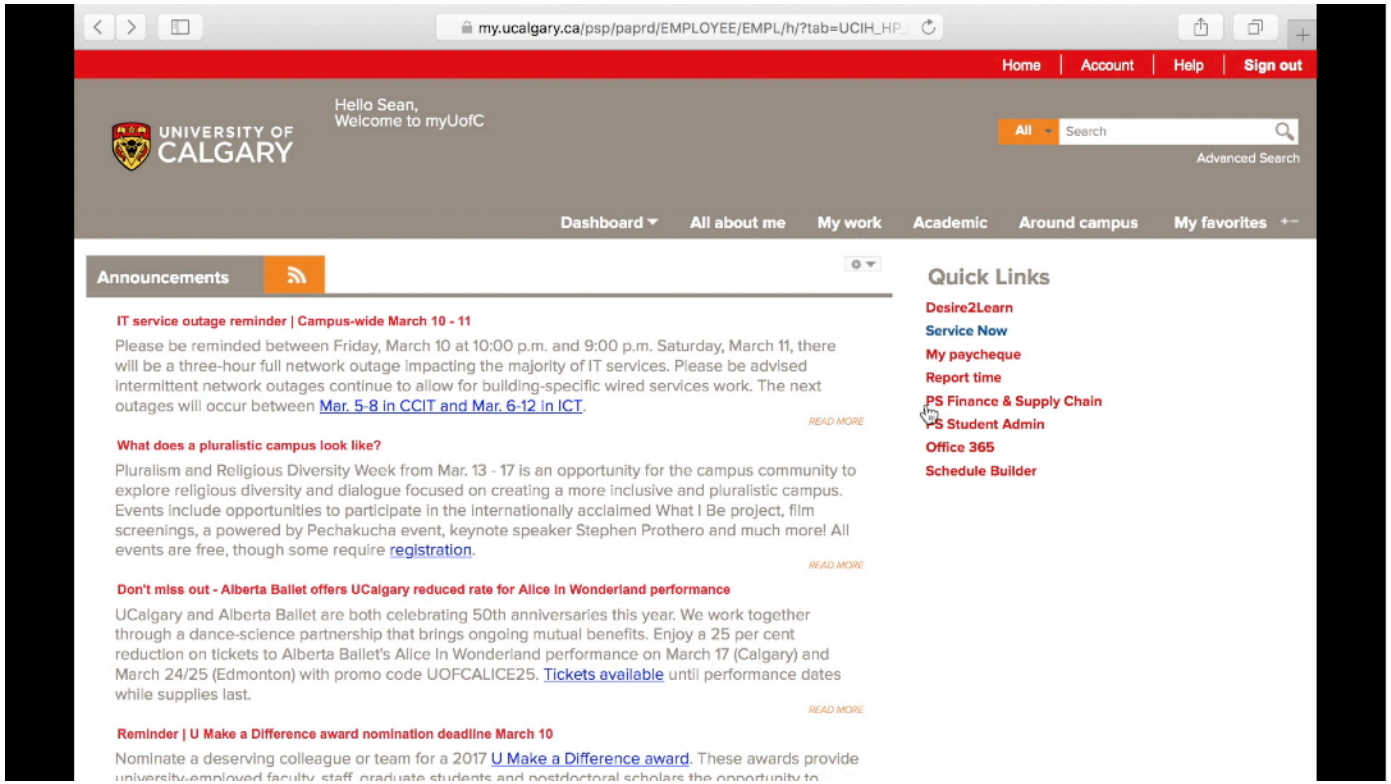
Service Now

Shibboleth



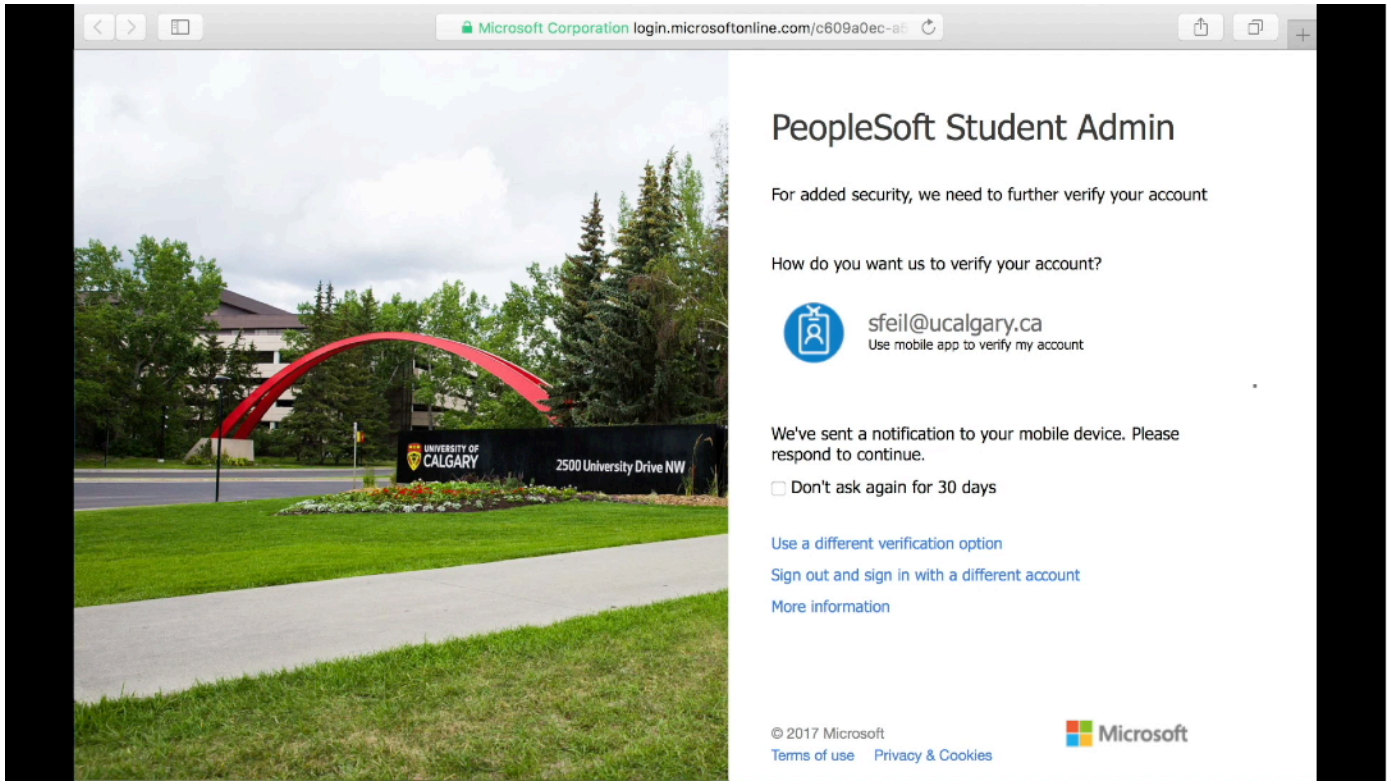
PeopleSoft Student Admin

Azure AD (MFA)



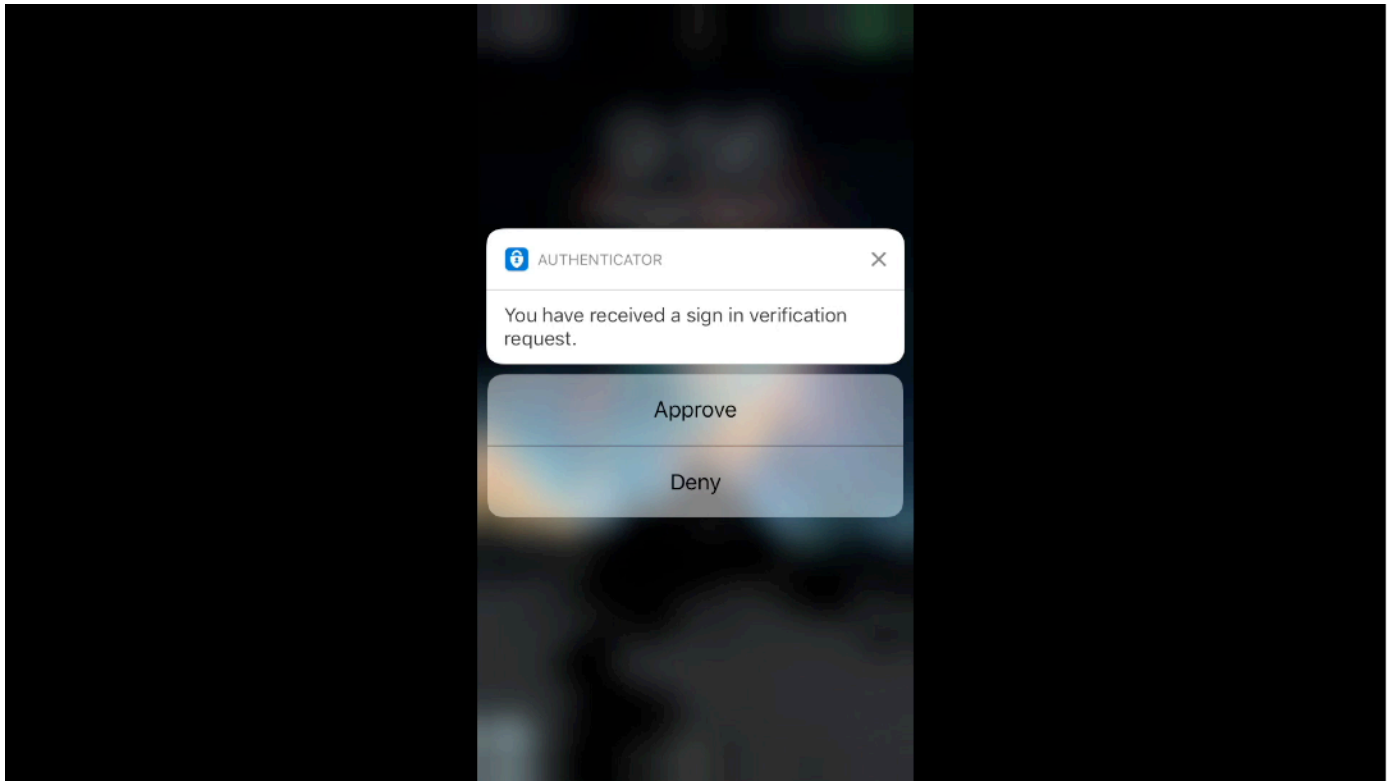
PeopleSoft Student Admin

Azure AD (MFA)



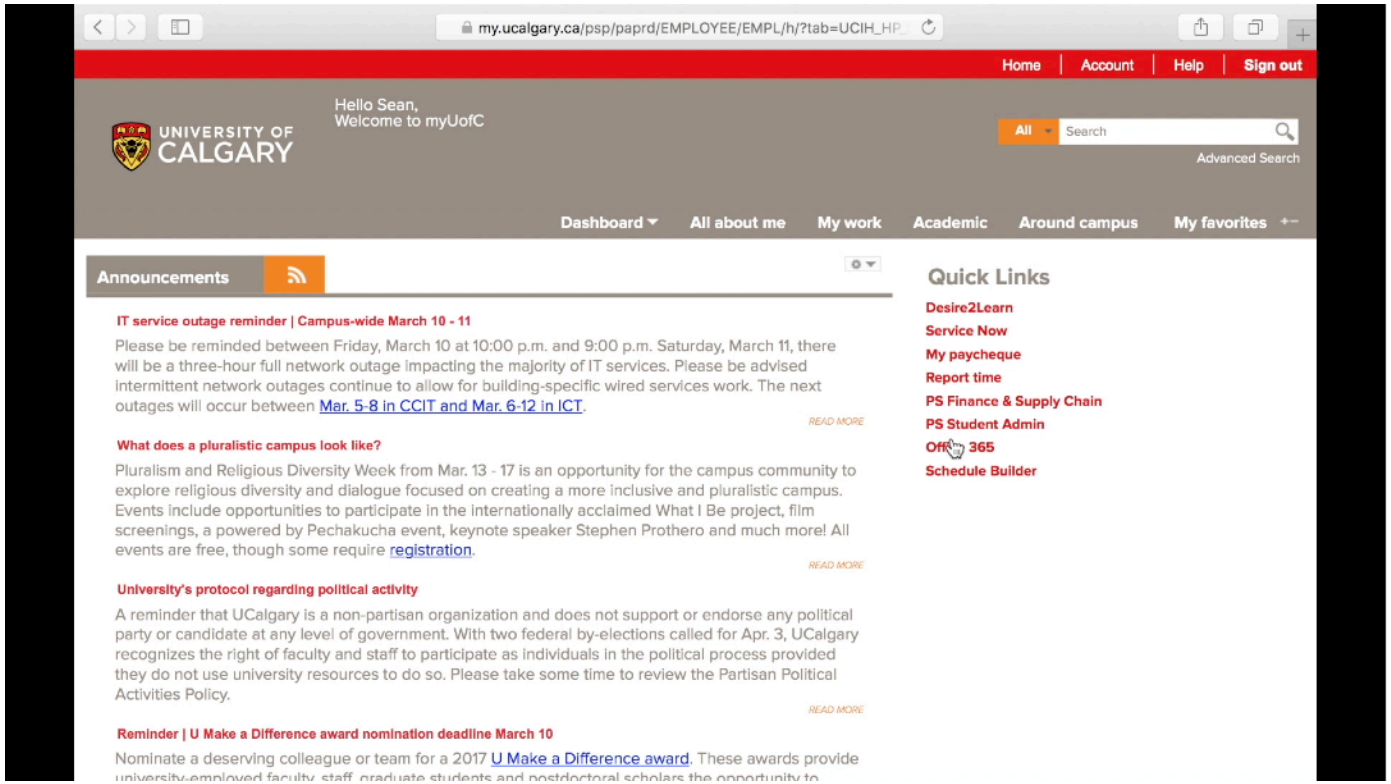
PeopleSoft Student Admin

Azure AD (MFA)



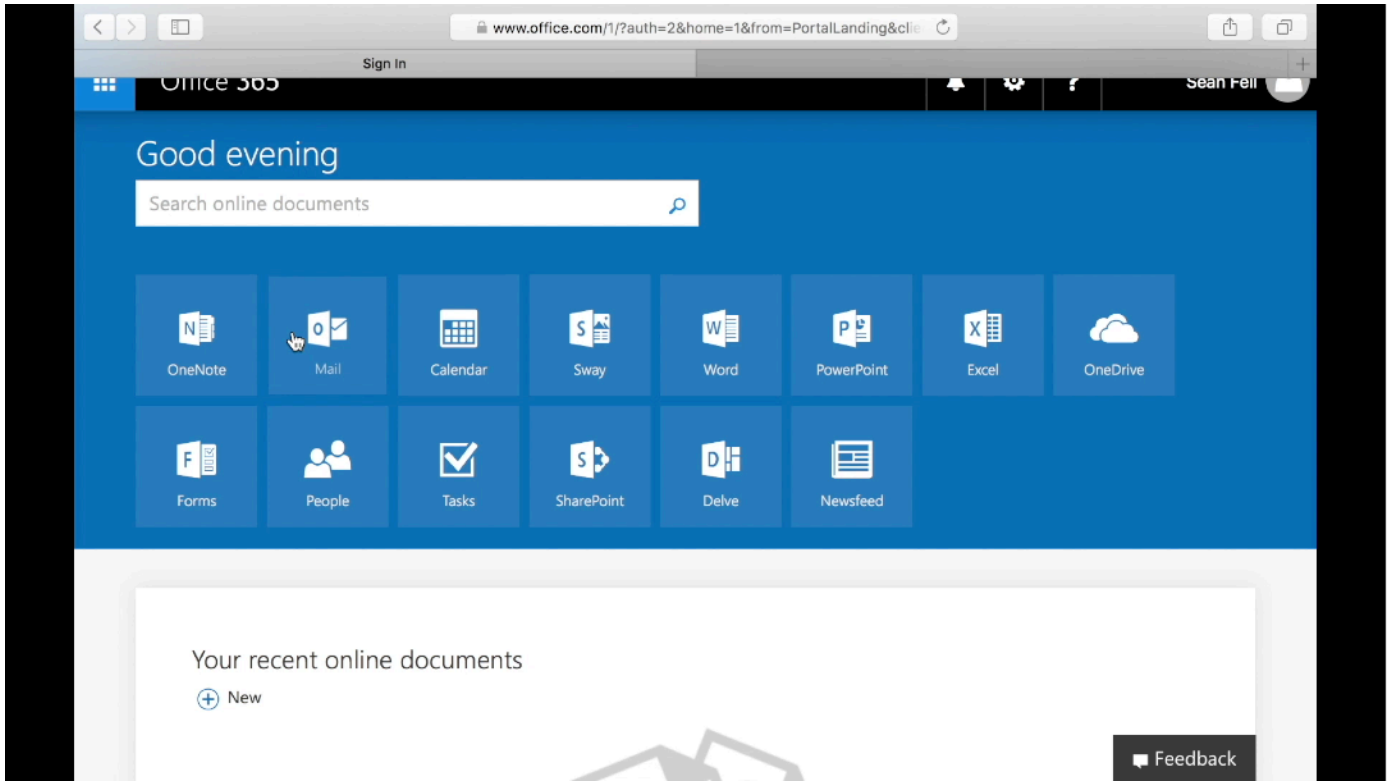
Office 365

Azure AD



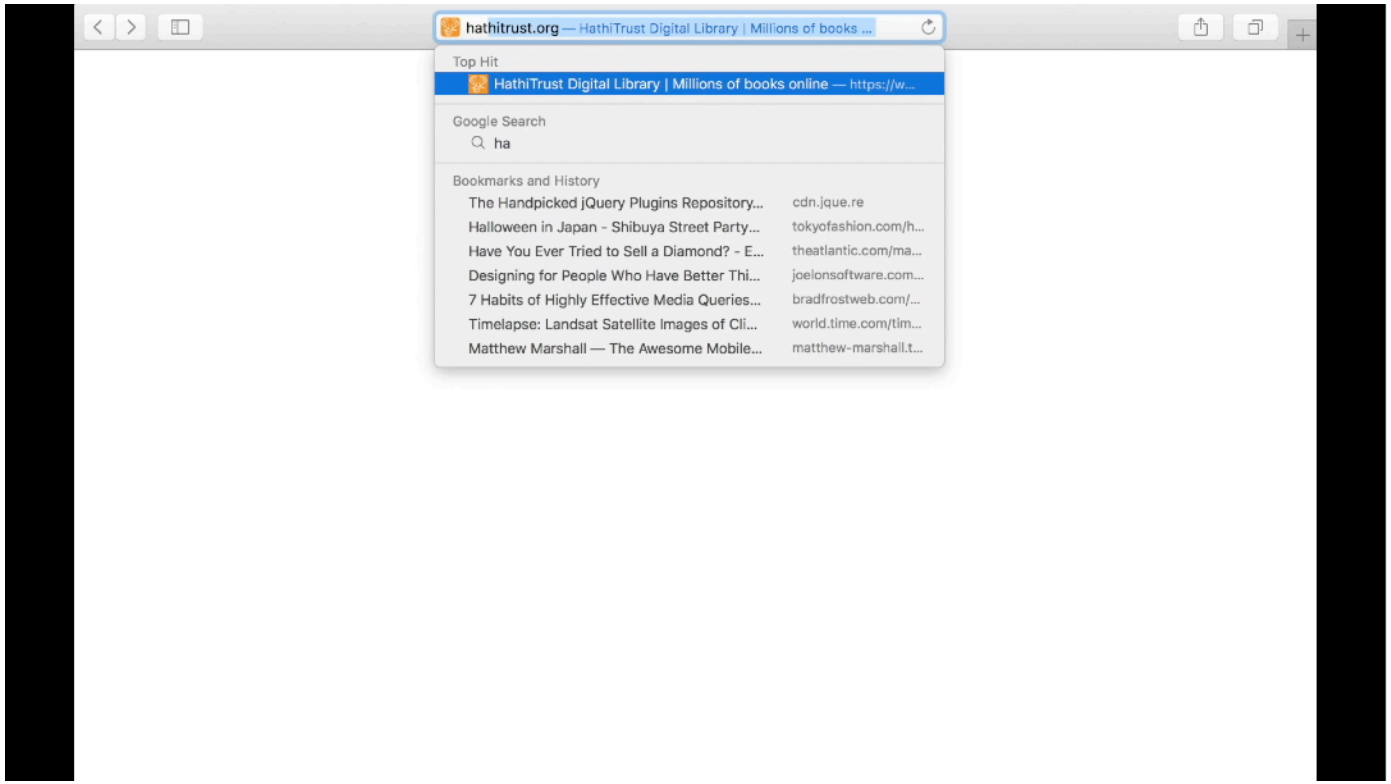
Exchange Online

Azure AD



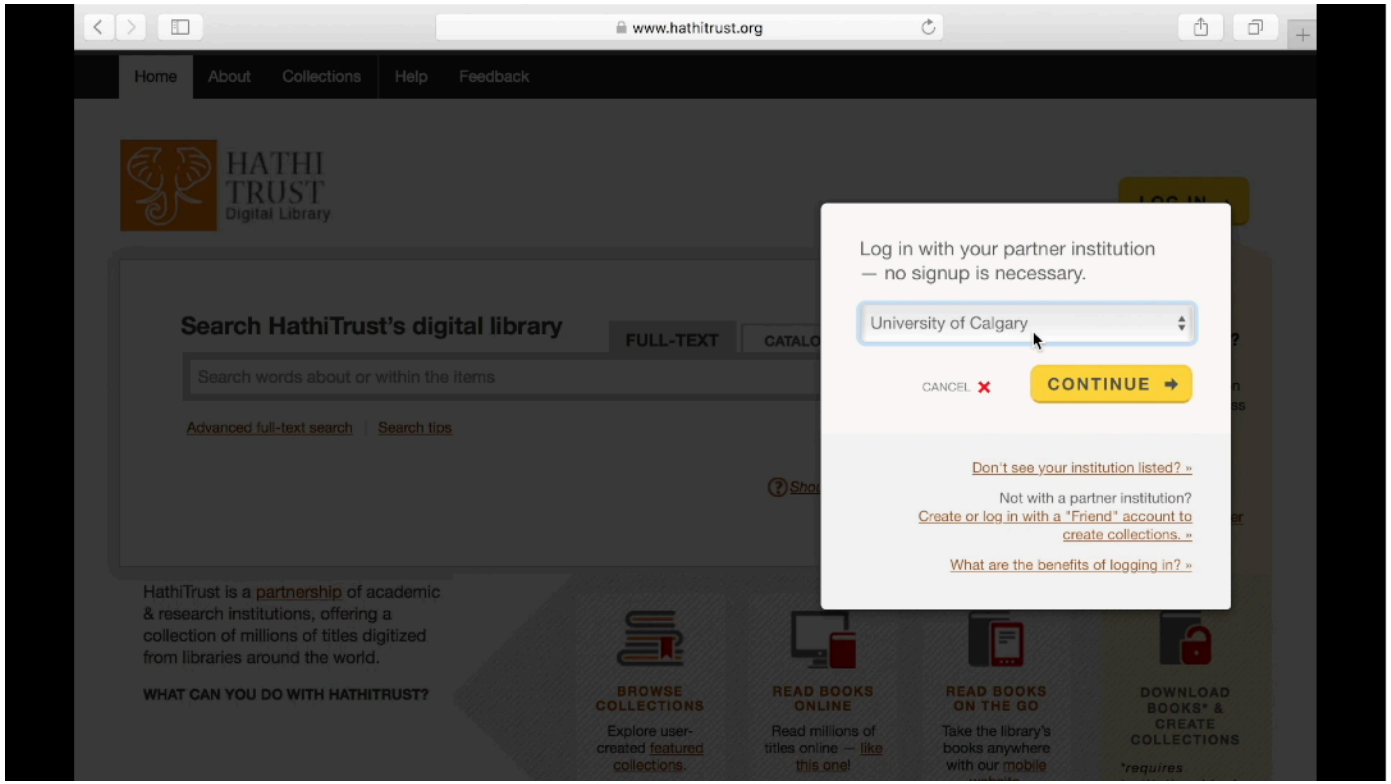
HathiTrust

Shibboleth (via eduGAIN)



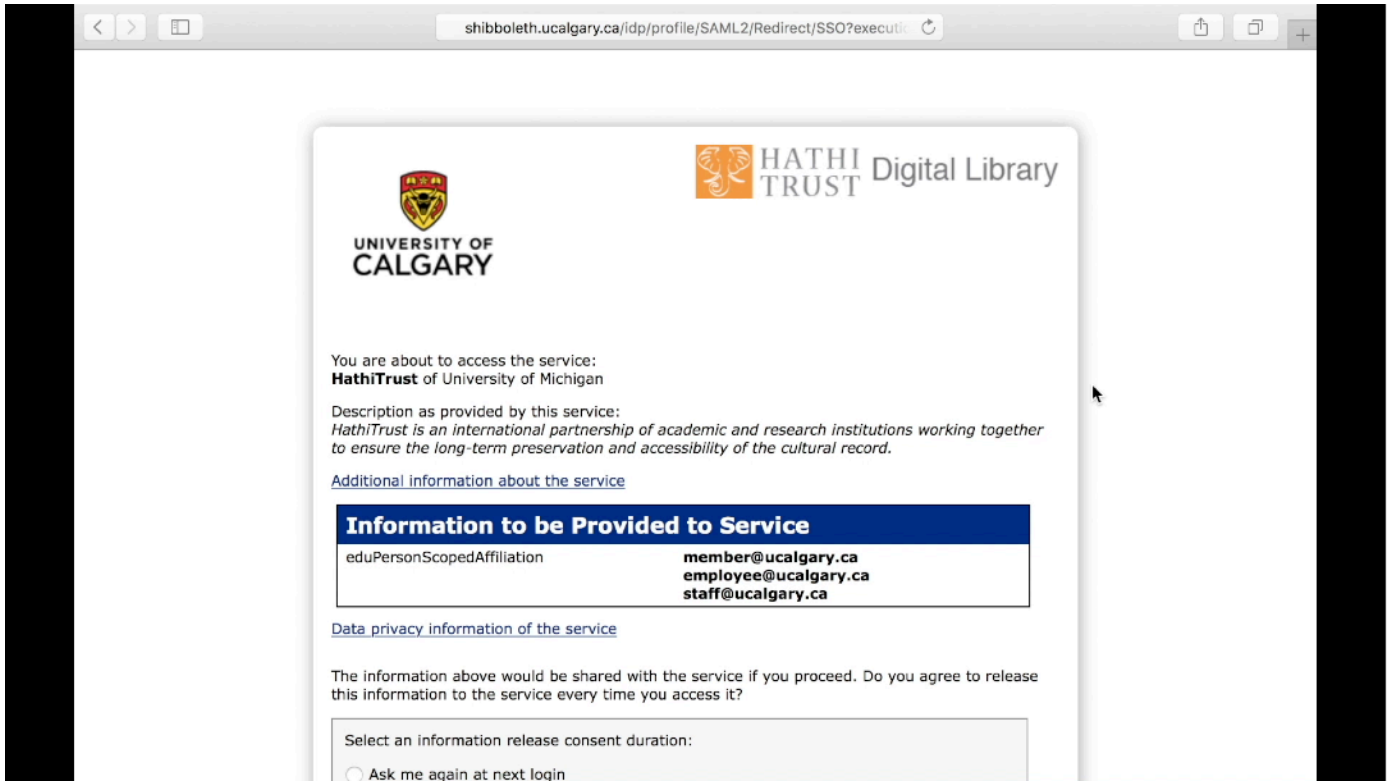
HathiTrust

Shibboleth (via eduGAIN)

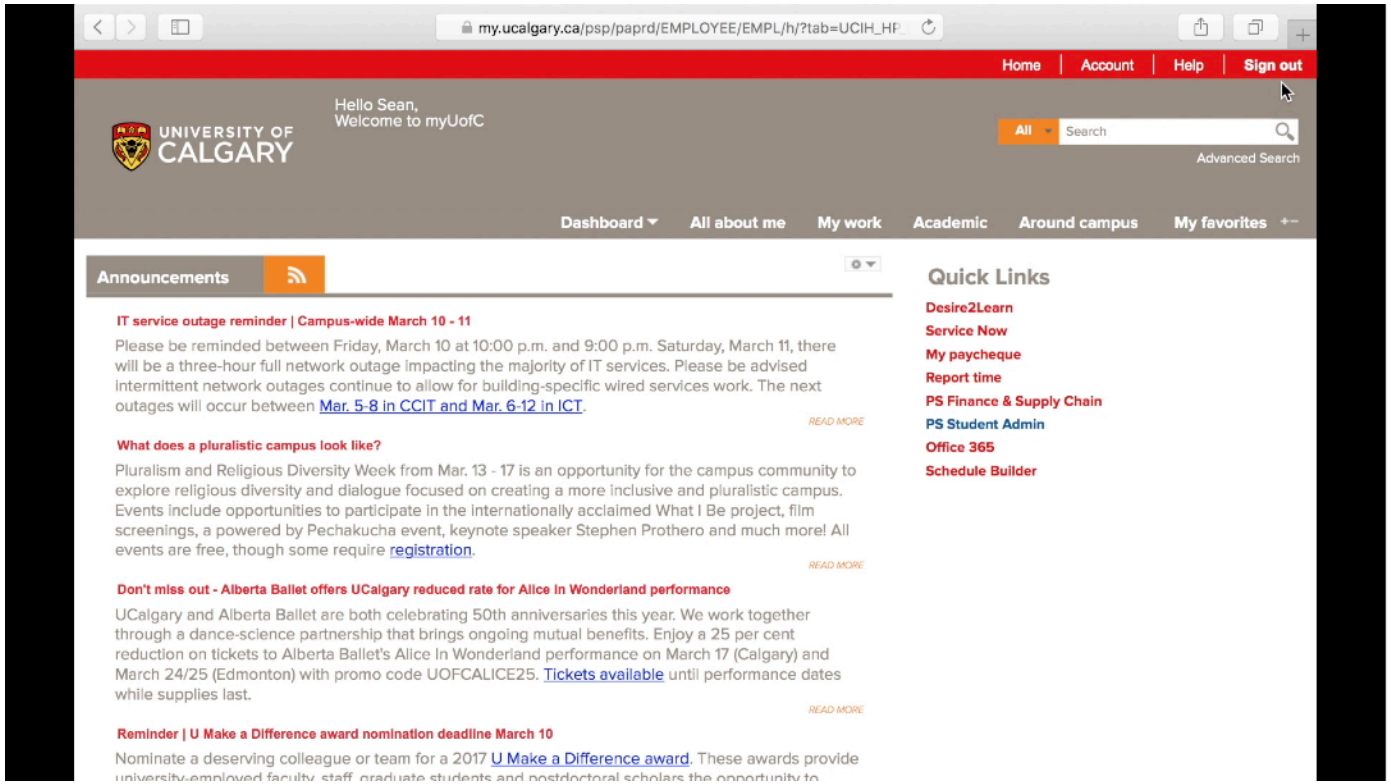


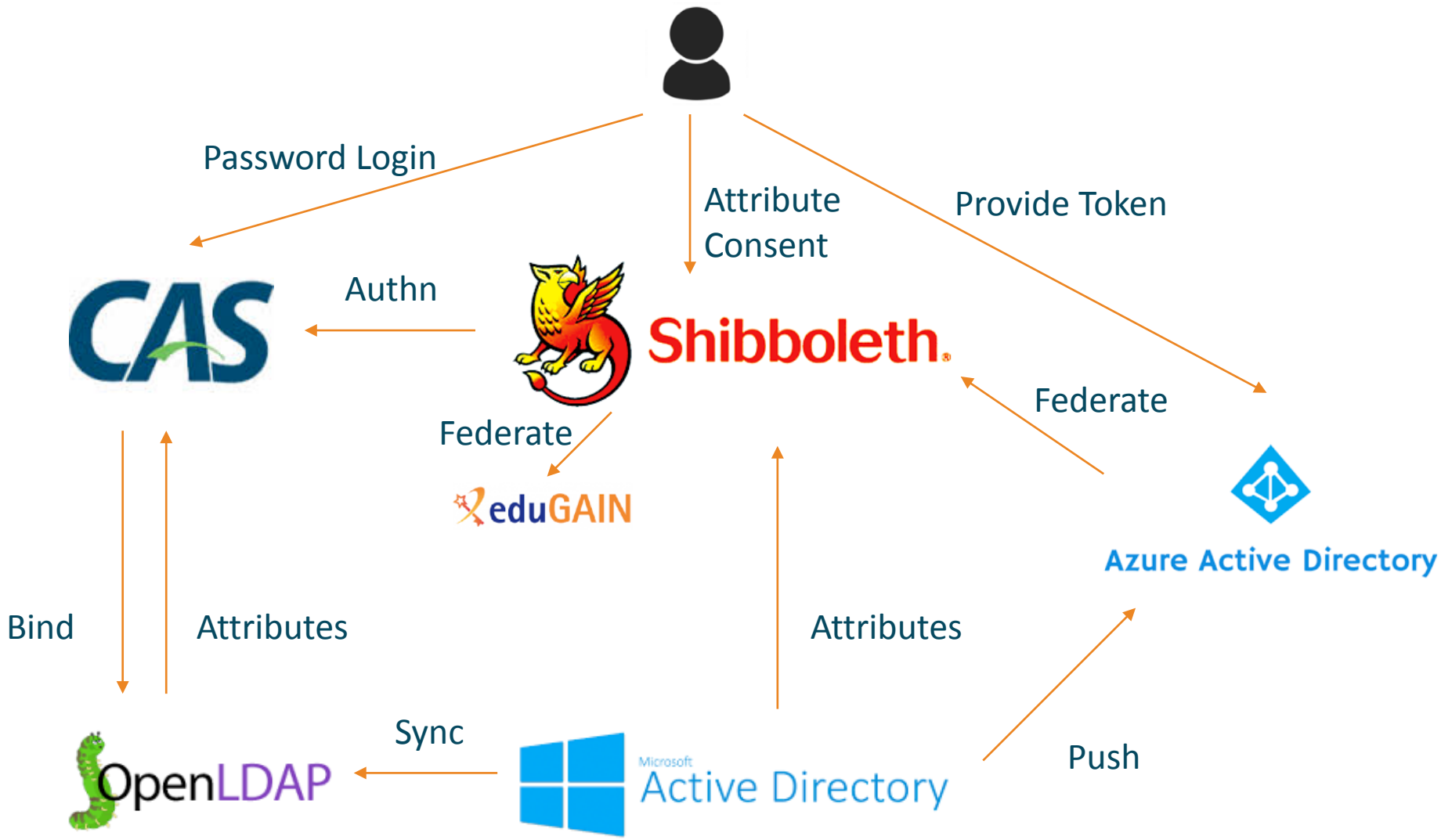
HathiTrust

Shibboleth (via eduGAIN)

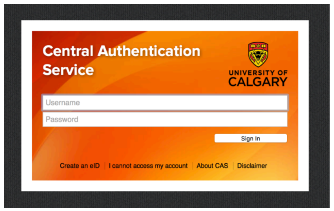


Single Logout



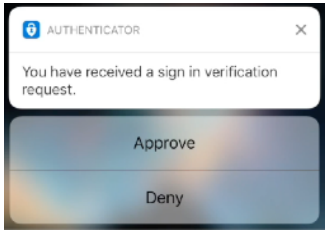

Password Login
Attribute
Consent
Provide Token
CAS
Authn
Shibboleth
Federate
Federate
eduGAIN
Azure Active Directory
Bind
Attributes
Attributes
Sync
OpenLDAP
Microsoft
Active Directory
Push

Password Login



Attribute Consent

Provide Token



CAS 1.0
CAS 2.0
Legacy apps

SAML1
SAML2
eduGAIN

SAML2
OpenID
WSFed
Azure App Store
Multi-Factor Auth

Information Technologies

Service Providers

Users

Complexity

Eyes High Strategy Statement

The University of Calgary will be a global intellectual hub located in Canada's most enterprising city. In this spirited, high-quality learning environment, students will thrive in programs made rich by research and hands-on experiences. By our 50th anniversary in 2016, we will be one of Canada's top five research universities, fully engaging the communities we both serve and lead.

Your turn

- What are your big challenges on sign on?
- How important is single sign on in your organization?
- Do you apply usability to any of your practices?
- Do you analyze your user behaviour?
- What security improvements could you make by applying usability?