



# **2-FACTOR AUTHENTICATION TOWN HALL**

**DECEMBER 17, 2015**

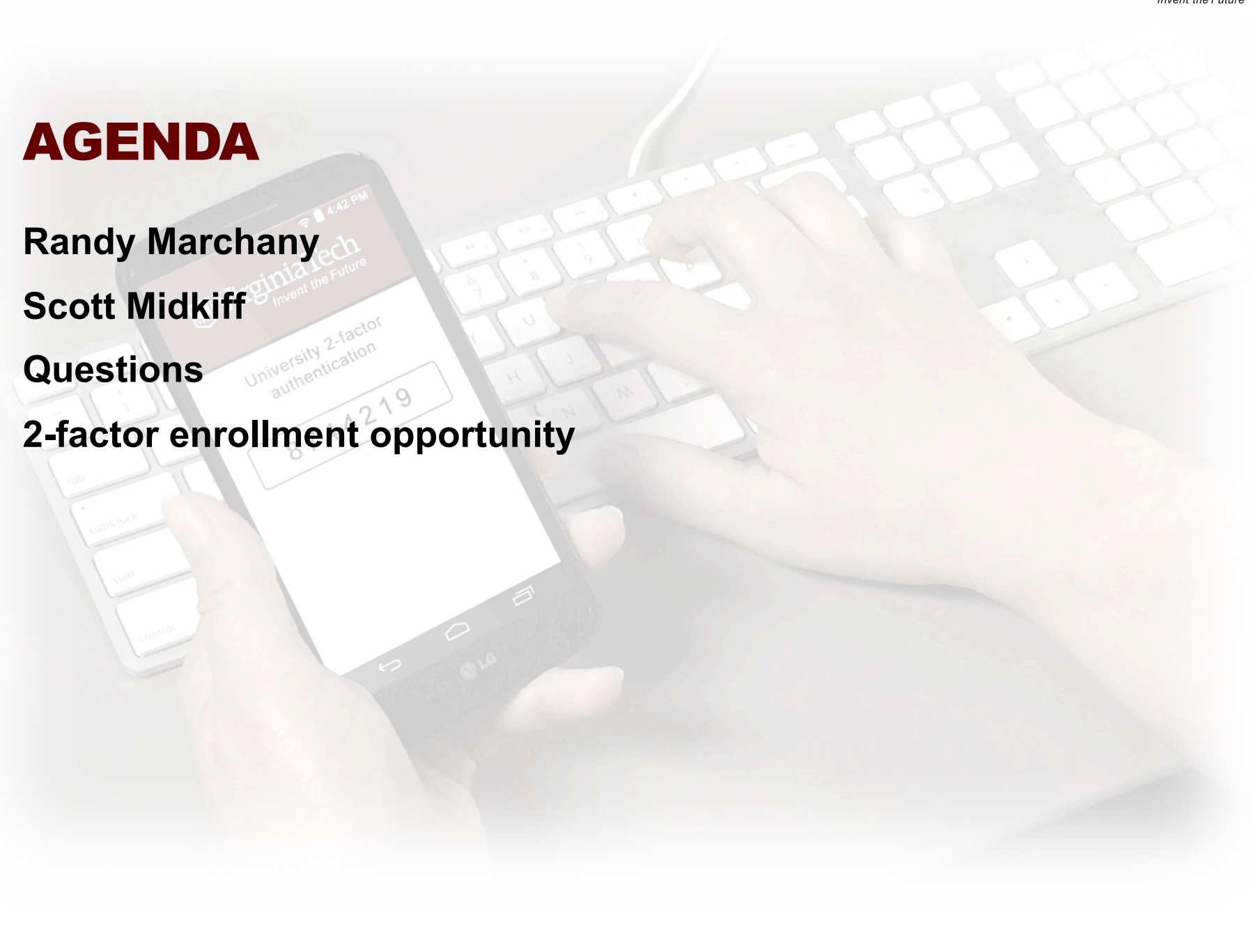
# **AGENDA**

**Randy Marchany**

**Scott Midkiff**

**Questions**

**2-factor enrollment opportunity**







# YOU ARE A TARGET

## Username & Passwords

Once hacked, cyber criminals can install programs on your computer that capture all your keystrokes, including your username and password. That information is used to log into your online accounts, such as:

- Your bank or financial accounts, where they can steal or transfer your money.
- Your iCloud, Google Drive, or Dropbox account where they can access all your sensitive data.
- Your Amazon, Walmart or other online shopping accounts where they can purchase goods in your name.
- Your UPS or FedEx accounts, where they ship stolen goods in your name.

## Email Harvesting

Once hacked, cyber criminals can read your email for information they can sell to others, such as:

- All the names, email addresses and phone numbers from your contact list.
- All of your personal or work email.

## Virtual Goods

Once hacked, cyber criminals can copy and steal any virtual goods you have and sell them to others, such as:

- Your online gaming characters, gaming goods or gaming currencies.
- Any software licenses, operating system license keys, or gaming licenses.

## Botnet

Once hacked, your computer can be connected to an entire network of hacked computers controlled by the cyber criminal. This network, called a botnet, can then be used for activities such as:

- Sending out spam to millions of people.
- Launching Denial of Service attacks.

You may not realize it, but you are a target for cyber criminals. Your computer, your mobile devices, your accounts and your information all have tremendous value. This poster demonstrates the many different ways cyber criminals can make money by hacking you. Fortunately, by taking some simple steps, you can help protect yourself and your family. To learn more, subscribe to OUCH!: a security newsletter designed to help people just like you.

[www.securingthehuman.org/ouch](http://www.securingthehuman.org/ouch)



## Identity Hijacking

Once hacked, cyber criminals can steal your online identity to commit fraud or sell your identity to others, such as:

- Your Facebook, Twitter or LinkedIn account.
- Your email accounts.
- Your Skype or other IM accounts.

## Web Server

Once hacked, cyber criminals can turn your computer into a web server, which they can use for the following:

- Hosting phishing websites to steal other people's usernames and passwords.
- Hosting attacking tools that will hack people's computers.
- Distributing child pornography, pirated videos or stolen music.

## Financial

Once hacked, cyber criminals can scan your system looking for valuable information, such as:

- Your credit card information.
- Your tax records and past filings.
- Your financial investments and retirement plans.

## Extortion

Once hacked, cyber criminals can take over your computer and demand money. They do this by:

- Taking pictures of you with your computer camera and demanding payment to destroy or not release the pictures.
- Encrypting all the data on your computer and demanding payment to decrypt it.
- Tracking all websites you visit and threatening to publish them.

This poster is based on the original work of Brian Krebs. You can learn more about cyber criminals at his blog at <http://krebsonsecurity.com>

## Login to Scholar Course Management System

If you want to log in with an account other than your Virginia Tech PID, please click the following link to log in with your [Guest Account](#).

Username

Password

[Forgot username or password?](#)

☐ Warn before logging into other sites.

Login

Clear

Switch to high security [PDC login](#).

## Security Notice

For security reasons, please **close** your web browser when you have finished accessing services that require authentication.

Virginia Tech Central Authentication Service - Google Chrome

Virginia Tech Central / x

dannytice.com/wp-admin/css/sch/vt.edu/vt.htm

Apps New Tab Nessus / Login App passwords - / SR Tool Home Report a Phishing

VirginiaTech Central Authentication Service

Help Terms of Use About CAS

### Login to Scholar Course Management System

If you want to log in with an account other than your Virginia Tech PID, please click the following link to log in with your [Guest Account](#).

Username

Password

[Forgot username or password?](#)

☐ Warn before logging into other sites.

Login Clear

Switch to high security [PDC login](#).

### Security Notice

For security reasons, please **close** your web browser when you have finished accessing services that require authentication.

© 2008-2014 Virginia Polytechnic Institute and State University  
The VT CAS logo is a derivative of [Night Sale](#) by brassmax, licensed under [BY-NC-SA](#).



22

The average number of online passwords that each UK citizen has.

# How passwords are discovered...

Attackers use a variety of password discovery techniques, including the use of powerful tools that are freely available on the Internet.



## Social Engineering

Attackers can use social engineering skills to coerce users into revealing their passwords.



## Shoulder Surfing

Observing someone typing in their password.



## Manual Guessing

Attackers use personal information 'cribs' (such as name, date of birth, etc.) to guess common passwords.



## Key Logging

An installed keylogger intercepts passwords when they are typed into a device.



## Interception

Passwords can be intercepted as they are transmitted over a network.



## Brute Force

Automated guessing of billions of passwords until the correct one is found.



## Stealing Passwords

Attackers can steal passwords that have been stored insecurely. This can include handwritten passwords hidden close to a device.



## Searching

Searching IT infrastructure for electronically stored password information.

# ...and how to improve your system security.

The following advice will reduce the workload on your users, making your system more secure as a result.

## Help users generate appropriate passwords

Put technical defences in place so that simpler passwords can be used.

Steer users away from choosing predictable passwords, and prohibit the most common ones.

Encourage users to never re-use passwords between work and home.

Train staff to help them avoid creating passwords that are easy to guess.

Be aware of the limitations of password strength meters.

## Help users cope with 'password overload'

Only use passwords where they are really needed.

Use technical solutions to reduce the burden on users.

Allow users to securely record and store their passwords.

Only ask users to change their passwords on indication or suspicion of compromise.

Allow users to reset passwords easily, quickly and cheaply.



CPNI  
Centre for the Protection  
of National Infrastructure

BLACKLIST  
THE MOST  
COMMON  
PASSWORD  
CHOICES.

MONITOR FAILED  
LOGIN ATTEMPTS,  
AND TRAIN  
USERS  
TO REPORT  
SUSPICIOUS  
ACTIVITY.

DON'T STORE  
PASSWORDS  
IN PLAIN TEXT  
FORMAT.

USE ACCOUNT  
LOCKOUT,  
THROTTLING OR  
MONITORING  
TO HELP PREVENT  
BRUTE FORCE  
ATTACKS.

PRIORITISE  
ADMINISTRATOR  
AND REMOTE  
USER  
ACCOUNTS.

CHANGE ALL  
DEFAULT  
VENDOR-  
SUPPLIED  
PASSWORDS  
BEFORE DEVICES  
OR SOFTWARE  
ARE DEPLOYED.

# PHISHING

## Be aware of unexpected email, messages, and attachments.

From: Virginia Tech Webmail Center [helpdesk0@vt.edu]  
Sent: Sunday, March 28, 2010 3:03 PM  
Subject: Response Is Urgently Needed.

Next Last

Welcome to [www.vt.edu](http://www.vt.edu) (VIRGINIA TECH)

We are currently performing service interruption.

Please you must reply to t  
(\_\_\_\_\_) and Password (\_\_\_\_)

Check out your new feature

To enable us upgrade your

Thank you for using [www.vt.edu](http://www.vt.edu)  
<http://mail.vt.edu/>

No legitimate business will ever ask for your credentials by email!

to ensure you do not experience

From: SunTrust [security@suntrust.com]  
To: Sparrow, Rich  
Cc:  
Subject: Reminder

This is a courtesy reminder that your suntrust card needs to be verified.  
In order to continue using your card, click the link below and follow the provided steps:

<http://www.suntrust-sv.com/portal/?server.pt>

Regards, Suntrust

Outlook Web App - Google Chrome

Outlook Web App x

fntlinedbcker.besaba.com

Apps New Tab Nessus / Login App passwords - SR Tool Home

Microsoft®  
Outlook® Web App

Security ( [show explanation](#) )

☒ This is a public or shared computer  
☐ This is a private computer  
☐ Use Outlook Web App Light

Domain/user name:

Password:

Email:

[Log On](#)

Connected to Microsoft Exchange  
 Secured by Microsoft Forefront Threat Management Gateway  
 © 2009 Microsoft Corporation. All rights reserved.



Gmail

tradietoolbox.com.au/vt.edu/vt.htm

Apps


New Tab

Nessus / Login

App passwords -


SR Tool Home

Report a Phishing



# One account. All of Google.

Sign in to continue to Gmail










Sign in

☐ Stay signed in
 [Need help?](#)

Please enter your full email address  
example@vt.edu

[Create an account](#)

One Google Account for everything Google










About Google

Privacy

Terms

Help



English (United States)

# **ONE USER'S EXPERIENCE**

**User account identified as compromised**

- 4HELP contacted her to change her passwords

**Working from home in the evening on personal PC**

**User changed password second time from work desktop**

**User received email of Direct Deposit change**

**As a precaution user changed password from “clean” machine**

- During the process user gets call on personal cell phone

**User had passwords saved in browser!**

**Account Recovery Options**