WELCOME

Student Orientation
2019
I. PowerPoint Presentations (MSB 1.006)
II. Laptop Configuration (MSB 1.006)
Power Point Presentations

* **Power Point Presentations in 1.006**
  * **Presentation I**
    * Speaker: Nermin Suljic
    * Duration: 10 Minutes
    * Subject: Orientation Process, Policies, Procedures
  * **Presentation II**
    * Speaker: Dr. William Weems
    * Duration: 20 Minutes
    * Subject: Trusted Identities in Cyberspace, UTH-Share
  * **Presentation III**
    * Speaker: Salman Khan
    * Duration: 10 Minutes
    * Subject: Protecting Your Computer and its Data
  * **Wrap-up**
    * Speaker: Nermin Suljic
  * **Q/A** (5 minutes)
Secure Flash Drive

* Students will be given an Kingston encrypted flash drive in LRC at a later date
* Required to use for all UT Health related activities
* Password Requirements
  * 6 – 16 characters in length
  * Password must contain Upper case, lower case, numeric and/or special characters(!, $, Etc.)
After the presentation

* Following configuration/setup will be made:
  * Configure Wireless
  * Install VPN and Setup Two Factor Authentication
    * To access UT resources from outside the network
  * Install Examplify – Exam software
  * Setup 15 minutes lockout policy
  * Setup UTH-Share account
  * Signup Mobile Device Acknowledge form for Email access on cellphone
  * Uninstall Dell Data Protection if needed (conflict with exam software)
Laptop Policies

* You will be required to use your MSIT approved laptop for computer-based exams
* Your laptop must be encrypted using BitLocker full-disk encryption
* We will record your computer’s Service Tag number
* If you replace your laptop, please bring it to LRC to be checked
* Students must store protected information only on UTHealth-approved and encrypted systems.

* Students should not store protected data on non-University owned devices or media.

MSIT will verify that all student laptops meet the full disk encryption requirements. Once encryption is verified, MSIT will place orange stickers on the laptops indicating that the laptops are encrypted and that they have been verified by MSIT. The sticker is tamper-evident and should not be removed from the laptops without MSIT approval. Removing or disabling encryption from your laptop while enrolled as a student at University of Texas Medical School at Houston is strictly prohibited. Failure to adhere to this policy will result in disciplinary action.
During the BitLocker encryption process, an encryption key is generated and required to save on Microsoft account, USB drive or printed.

Student Laptops are covered by Dell 4-year ProSupport warranty. In case of any hardware replacement, BitLocker Key will be required to unlock your Hard Drive.

Without BitLocker Key, All data will be lost
Operating System Updates

- **Windows Security updates** – ok to install

- **Windows 10 Feature Updates** – do not install until Educational Programs certifies compatibility with exam software. Typically features updates are released in May and October

- **Current version:** Windows 10, version 1903
Laptop Warranty

- Student Dell laptops come with “4-Year ProSupport with next Business Day Onsite Service”
- Does not cover accidental damage (caused by drops, spills and electrical surges...)
- Students can call Dell customer service directly or come to Learning Resource Center for help
Students may request an increase to cost of attendance (COA) for the purchase of a laptop:

- Students must complete the revision request form:
- Students must attach a copy of final purchase receipt
- This is a one-time COA increase allowance
- Complete instructions may be found on the form
Computing Resources in the Medical School

* Equipment
  * 171 All-in-One computers available 24/7 in Learning Resource Center (LRC), MSB G.200
  * 16 All-in-One computers available at the LBJ Hospital Satellite LRC
  * Black & White and Color Printers (Purchase Print Cards in the LRC)
  * Network scanner scans directly to UTHealth email account

* Software
  * Microsoft Office Suite
  * Educational Programs in support of Medical School Curriculum
LRC Computer Policy

* Do not save any data on the LRC computers
  * School issued **encrypted** Kingston USB flash drive is the only external USB storage device allowed to save files.
  * User profiles on the LRC computers are deleted every last Saturday of the month as part of regular maintenance
  * Do not disconnect any cables from the LRC computers
  * Please remember to **Log Out** when you are finished using the computer
Microsoft Office 365

- Students are provided with free Microsoft Office 365
- visit: https://office365.uth.edu to download the software
- Sign in with UTHealth email address and password
Discounted Software

* Students are eligible to purchase discounted software through https://uthealth.onthehub.com

* Sign in with UTHHealth UserID and password

7/29/2019
Webmail

- Convenient way to check your e-mail
- Please visit https://webmail.uth.tmc.edu
- Sign in with UTHealth UserID and password
- Required UTH Two Factor Authentication after sign in
- Both Webmail and Microsoft Outlook can check and send encrypted e-mail
- Start the e-mail subject with [encrypt] to send encrypted e-mail to external recipients
If you require help with your laptop, please submit a ticket to schedule a convenient time to meet with one of our student helpdesk representatives.

Please visit: http://go.uth.edu/MSITHelp

Following services will be available:

* Installing, troubleshooting and supporting Windows operating systems
* Installing licensed software applications
* Contact Dell warranty for Hardware replacement
Submitting a Ticket to Student Helpdesk

Authentication Service

Sign in to:
MSIT Help Desk

User ID
Password
Sign In

change password | password help

WARNING: You are currently accessing a protected information resource. Unauthorized use is PROHIBITED! Usage of this system may be subject to security testing and monitoring. Misuse is subject to criminal prosecution. There is no expectation of privacy except as otherwise provided by applicable privacy laws.

Privacy & Security | Contact | Inside UTHealth

MSIT Help Desk

Please enter your request. You may change users or select from a list of departments. If you do not receive an email confirming submission of your request within 15 minutes, please contact your LAN Manager by phone.

Request Ticket

Name: [Name]
Department: MS - VisualIT Services
Room: MSB-409
Phone: [Phone]
Call Back Number: [Call Back Number]
Email: [Email]
Computer Name: [Computer Name]
Request: [Request]

Characters remaining: [Remaining]

Submit Request
Reset Form
Trusted Identities in Cyberspace:
A Critical Component In Healthcare Information Technology & Collaborative Systems

William A. Weems, Ph.D.
Associate Dean Information Technology
Medical School
U. Texas Health Science Center at Houston
Today’s Cyberspace Realities

* 7,587,311,245 people on earth!
* Over 4 billion people have Internet access!
* Facebook alone has over 2.38 billion users!
* U.S. Population 328,202,756

* Collaboration is no longer just among persons, but also between people and increasingly intelligent digital assistants, and among the digital assistants!

* *Interactions are sometime anonymous, but increasingly must be among identified entities that have a high degree of trust.*

* E-Learning skills are indispensable!*

Estimates U.S. & World Population Clocks
13:52:45 UTC (EST+5) July 25, 2019
Identity, Trust, Privacy, Accountability: Being a Responsible Citizen in Cyberspace
**Trust Issues in Cyberspace**

- How do you prove you are who you say you are to a relying party?
- What is identity?
- How do you know that you can trust a person or a specific digital system in cyberspace?
- If your identity is stolen and used fraudulently, or personal records are altered without your knowledge or permission, how do you prove that it was not you?
Two aspects of a person’s identity

- Physical Identity - *absolutely unique to one person and can be certified by a credential provider using various physical characteristics of that person.*
- Personal attributes – *constant and time varying characteristics associated with an identified person and verified by trusted attribute providers.*
An authentication credential when presented to a relying party:

1. can only be activated by you,
2. positively verifies your physical identity.
3. positively identifies the certifying authority (CA) that is attesting it is “you”.
4. provides a certified unique identifier issued to you and registered with the CA, and
5. asserts a defined level of assurance (LOA) that the credential is presentable only by you – i.e. the person it authenticates.
Certified Authentication Credential Can Be Presented to & Trusted by Any Relying Party
Ideally, individuals would each like a minimal number of authentication credentials that can be securely used to authenticate his or her identity anytime authentication of identity is required to secure any transaction between relying parties.
Select an Identity Provider

The Internet2 Wiki Service requires that you identity yourself. Please select a trusted identity provider from the list below, or simply begin typing in the edit box.

Enter institution name:

Choose from a list:

**Federation**

- US Higher Education
- UK Federation
- Australian Access Federation
- SWAMID Test Federation
- Austria - AConet
- France - CRU
- Servicio de Identidad de RedIRIS (SIR)

**Organization**

- AAF Virtual Home
- Aberdeen College (Test)
- Aberdeen College Staff
- Aberdeen College Student
- Aberystwyth University
- Abingdon and Witney College
- Academy of Fine Arts Vienna
- Accrington & Rossendale College
- AConet
- Adam Smith College

Need assistance? Send mail to spaces-admin@internet2.edu with description.
WARNING! You are currently accessing a protected information resource. Unauthorized use is PROHIBITED! Usage of this system may be subject to security testing and monitoring. Misuse is subject to criminal prosecution. There is no expectation of privacy except as otherwise provided by applicable privacy laws.
Three types of authentication credentials.

- **UTHealth Username/Password: Identity Provider Service (Shibboleth)**
  - Low level of assurance (one-factor authentication)
    - UTHealth userID (UID) & Password transmitted via Internet
    - Less functionality: Only for authentication of physical identity

- **UTH-Share (Google Suite For Education Collaborative System)**
  - UTHealth userid@uth.edu e.g. wweems@uth.edu
  - Can be upgraded to two-factor authentication

- **Digital ID on eToken (two-factor authentication)**
  - High level of assurance – some thing you know and have
    - Password only goes to e-token
    - Only the e-Token owner, i.e. you, can manage password
  - More functionality (e.g. authentication as well as digital signatures)
Using Public Key digital IDs (DIDs)

• **Digital Signatures**
  – authenticates senders
  – guarantees that messages are unaltered (message integrity)
  – provides for non-repudiation
  – legal signature with the United States

• **Encryption of e-mail and electronic documents**
  – Provides confidentiality of e-mail when required

• **Digitally Signing On-line Forms**

• **Strong Authentication for Access Control**
Dr. Weems,

I have attached your portion of the orientation presentation. Please review it and send it back to us so that we can incorporate it into the full presentation slideshow.

Thanks,

Nermin Suljic
Manager, Systems & Applications (MSIT)

UTHealth | The University of Texas Health Science Center at Houston | Medical School
6431 Fannin St | MSB G.520 | Houston, TX 77030
713 500 5426 Telephone | 713 500 0708 Fax
Subject: Orientation Presentation (Dr. Weems)
From: Suljic, Nermin
Signed By: Nermin.Suljic@uth.tmc.edu

The digital signature on this message is Valid and Trusted.

For more information about the certificate used to digitally sign the message, click Details.

Warn me about errors in digitally signed e-mail before message opens.

Close
Value of Public Authentication Credentials with Public Identifiers

* A presenter’s physical identity is immediately known to any party accepting the credential!
* Risk of identity theft becomes very unlikely!
* The presenter is “in control” of his or her “trusted” actions in cyberspace.
  * Relying parties “know” it is the actual physical person initiating an action!
* The presenter has “increased control” over release of his/her personal attributes from attribute providers.
Jane E. Doe

* Email: Jane.E.Doe@uth.tmc.edu
* UTHealth UserID (UID): jdoe
* Scoped UserID: jdoe@uth.edu
* Used for your UTH-Share ID – Google Apps EDU

External Identifiers

jdoe23@gmail.com
Log in to take control of your health records today

Sign In

or, use an alternative

Facebook, Google, Microsoft, Yahoo, Cerner

How is this information used?

I need to sign up
UTH-Share

UTHealth’s Implementation of Google’s G Suite for Education
Why Implement G Suite for Education?

Users want a *Collaborative System* providing

- Document and file sharing (All files & folders have URLs)
- Shared workspaces
- Online document creation and editing of linked documents
- Automatic, instant saving with versioning
- Online, simultaneous editing by multiple individuals
- **Globally** grant secure access to credentialed individuals
- Powerful search and discovery (Intelligent Digital Assistants)
- Integrated Voice/Video Conferencing
- Unlimited storage: Individual files: <= 5 Terabytes!
- Easy & functional access via most mobile devices
Google Collaborative Cloud Services

G Suite for EDU includes many familiar Google applications and new innovations **UTH-Share**

- Text Documents
- Presentations
- Spreadsheets
- Forms
- Drawings
- Drive
- Intelligent Digital Assistants
- Sites
- Video Hangouts
- Calendar
- Groups
- Notifications
- Mobile Devices
IT SECURITY AWARENESS
for New Students

July 2018
PHISHING AND DATA BREACHES

July 19, 2018 - UMC Physicians (UMCP), a physician practice management group set up by Texas-based UMC Health System, announced July 11 that it had notified more than 18,000 patients about a healthcare data breach in which their PHI may have been compromised by the hack of an employee’s email account.

ALIVE HOSPICE’S PHISHING ATTACKS EXPOSE TREASURE TROVE OF PHI

Tennessee-based Alive Hospice said July 13 that unauthorized persons gained access to two employee email accounts through phishing attacks that exposed a treasure trove of patient PHI.

BILLINGS CLINIC HAS EMAIL BREACH EXPOSING PHI ON 8,400 PATIENTS

Montana-based Billings Clinic experienced a PHI breach that may have affected 8,400 patients, the Billings Gazette reported July 13.

ROCKY MOUNTAIN HEALTH CARE SAYS LAPTOP THEFT EXPOSED PHI ON 1,087 PEOPLE

Colorado-based Rocky Mountain Health Care Services (RMHCS) reported to OCR on July 13 that the theft of a laptop exposed PHI on 1,087 individuals.

UPMC COLE SAYS PHISHING ATTACKS EXPOSED PHI OF 790 PATIENTS

Pennsylvania-based UPMC Cole said July 16 that it notified 790 patients that their PHI may have been inappropriately accessed because of two phishing attacks against employees.
Indicators of a Phish

- Does the message plant a false sense of urgency?
- Is the greeting generic?
- Do you recognize the sender?
- Can you spot typos or grammatical errors?
- Does the email involve sensitive data, such as your password?
You must forward the original e-mail as an attachment for IT Security to be able to gather all the information needed to address the phish.

Pressing “Ctrl+Alt+F” simultaneously will enable you “Forward as Attachment”

You can also select “More” and then select “Forward as Attachment”

Send the new forward to: its@uth.tmc.edu
SAFEGUARD SENSITIVE INFORMATION

- Encrypt devices; email & texts
- Use encryption: Bitlocker FDE, Outlook e-mail encryption and TigerText
- Use two factor authentication
- Two-factor authentication (DUO) helps protect access
- Protect against malware
- Don’t share passwords
- Don’t store PHI on personal devices
- Store all PHI in the Electronic Health Record (EHR) system (including photos)
- Avoid public networks
- Attackers often exploit public networks
- Use firewalls and antivirus
- Anything done under your log-in is your responsibility!
E-MAIL SECURITY

1. [ENCRYPT] All e-mails containing PHI
   Type [ENCRYPT] in the Subject field of all e-mails containing PHI.

2. No PHI in Subject field of ANY e-mails
   DO NOT include PHI in the Subject field of any e-mails; the Subject field is never encrypted.

3. Report Suspicious e-mails to IT Security
   Forward “phishy” e-mails as an attachment to IT Security at its@uth.tmc.edu.
E-MAIL SECURITY

4. Use Patient Portals to communicate with Patients.

E-mail is not the method of communicating with patients.

5. If sending an email to multiple recipients; use BCC.

DO NOT show the names of other e-mail recipients.

6. Report Incidents or Misuse to IT Security.

If you see something, say something to IT Security at its@uth.tmc.edu.
WE ARE NOT IMMUNE
Password Security

A strong password is critical for keeping your private information secure, whereas a weak password invites criminals to steal your data.

Even the strongest password can be stolen if you fall for a phishing attack. Make sure when you login to an account, pay close attention to the URL to make sure it is the right site.

Follow these password security tips to help protect your accounts:

- **Use a different password for every account.** Otherwise, a single data breach can compromise several accounts. Keep track of your passwords with a password manager application.
- **Use long and complex passwords.** A strong password is long and includes uppercase letters, lowercase letters, numbers, and special characters. Use random combinations of characters and avoid easy-to-guess phrases like the name of your first pet or high school mascot.
- **Change your passwords regularly.** A data breach can compromise any account and may not be disclosed for weeks or months.
- **Set up multi-factor authentication (MFA).** Strengthen the security of your account by setting up MFA wherever it is offered.

**Remember:** Never respond to an email that asks for your password. No legitimate organization will request your password via email.
**RANSOMWARE**

Ransomware is a type of malware that locks your screen and prevents you from accessing files until you pay a ransom.

Keep these tips in mind when browsing the internet and checking your email:

**Back up your files regularly.** Secure your backup in a safe place and disconnect the device when you aren’t using it. Ransomware can infect connected network and external drives.

**Update software frequently.** Unpatched software can contain security holes that leave your system vulnerable. Only download updates from your app store or from a known, bookmarked source.

**Use caution when surfing the web and checking your inbox.** Never download attachments or click any links from unknown senders. If you see a suspicious email, report it.

**Never enable macros on Microsoft Office documents.** Enabling macros can allow a malicious program to download and run malware.
KEY POINTS TO REMEMBER

Be cautious of e-mails

Phishing

Pause
Before you click on Links or attachments in e-mails

Think
Before you reply with your UserID and password or any personal information

Ask
IT Security if you’re not sure

Email
its@uth.tmc.edu

Be cautious with confidential and sensitive information

Login

Username
Password

Unencrypted file information

Your account no. is 01234

Encrypted file information

7b64bkk0k4/kk8xkyKq7K7IPVg

HIPAA
Health Insurance Portability and Accountability Act

UTHealth | McGovern
The University of Texas Health Science Center at Houston Medical School
CONNECT WITH IT SECURITY

Contact

713.486.4848
[HelpDesk]

its@uth.tmc.edu

inside.uthouston.edu/itsecurity/

Follow

facebook.com/uthealthsec

twitter.com/uthealthsec

Phishing Blog
itsecurity/sac/phish/index.htm
Connectivity to the UTHealth Exchange e-mail system with an approved mobile device is available to students.

Students are allowed to connect supported device through Intelligent Hub MDM Agent.

Jailbroken or Rooted devices are not supported.
Upon joining a supported mobile device to the UTHealth e-mail system, pre-defined policies will be enforced. These policies include but are not limited to 

*minimum password length*, *inactivity timeout period* & *number of failed unlock attempts allowed*. For more detailed information on what policies are being applied, see [https://inside.uth.edu/dcos/services/mobile-device-management/policies.htm](https://inside.uth.edu/dcos/services/mobile-device-management/policies.htm). This URL is accessible while connected to the UTHealth network.

Notify the LRC immediately if your device is lost or stolen. UTHealth has the ability to remote wipe your device in this instance but can only do so while the cellular account is still active.
Two-factor authentication adds an additional layer of assurance onto your normal login process.

- UTHealth is using **Duo Security** which uses your phone as the second factor in addition to the login method.

- Smartphone users can install DUO Mobile app for more authentication option.

- This service is mandatory for VPN and Webmail access.
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Pass</th>
<th>Fail</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSIT approved Laptop: Latitude 3490 / 3400 / 5490 / 7390 (Windows 10 Pro, Intel i5, 8 GB RAM or more, 4 year warranty)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>BitLocker Encryption (Full Disk Encryption)</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**SETUP**

<table>
<thead>
<tr>
<th>Setup</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTHSC Wireless</td>
<td>Yes / No</td>
</tr>
<tr>
<td>FS BIG-IP VPN</td>
<td>Yes / No</td>
</tr>
<tr>
<td>Examplify – Exam software</td>
<td>Yes / No</td>
</tr>
<tr>
<td>15 minutes lockout policy</td>
<td>Yes / No</td>
</tr>
<tr>
<td>Two Factor Authentication – Duo Mobile Setup</td>
<td>Yes / No</td>
</tr>
<tr>
<td>UTH-Share Account Setup</td>
<td>Yes / No</td>
</tr>
<tr>
<td>Mobile Device Policy Acknowledgement Signup - [ ] iOS [ ] Android [ ] Other</td>
<td>Yes / No</td>
</tr>
<tr>
<td>Uninstall Dell Data Protection suite (if needed)</td>
<td>Yes / No (if needed)</td>
</tr>
</tbody>
</table>

**PASS / FAIL**

Student Signature: ____________ Date: ____________

*If you failed the computer orientation you must correct the problem and submit an MSIT ticket to have your computer re-checked at the Learning Resource Center (MSG 2.200) within two weeks. Failure to do so will result in a "Hold" being placed on your record.

LAN Manager Name ____________ Signature: ____________ Date: ____________

Mon(7/29) Tue(7/30)

PASS OR FAIL, THIS FORM MUST BE SUBMITTED IN THE FRONT OF THE CLASSROOM!
Student Name: __________________

Failed Computer Orientation

Important: You have two weeks from today to correct the issue(s) below. Failure to do so will result in a “Hold” being placed on your record! PLEASE BRING THIS FORM WITH YOU WHEN YOU COME TO HAVE YOUR COMPUTER RE-CHECKED!

* PLEASE BACKUP YOUR DATA BEFORE YOU START ENCRYPTING YOUR LAPTOP OR SEEKING ANY MSIT ASSISTANCE.

<table>
<thead>
<tr>
<th>Reason</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No MSIT Approved Laptop</td>
<td></td>
</tr>
<tr>
<td>Failed BitLocker Encryption</td>
<td></td>
</tr>
</tbody>
</table>

MSIT Signature: ____________________ Date: ____________________
Important Reminders

* Keep your BitLocker key saved in a secure location, without it, you may not be able to access your data!

* Do not install new Windows 10 Feature updates until approved by Educational Programs. Security updates are okay to install.
Thank you!

Questions?

Ticket# 7/29/2019