YOUR ROLE IN DATA STEWARDSHIP

THE WHY AND HOW OF DATA SECURITY
DEPARTMENT OF MEDICINE IT SERVICES

UW Medicine
DEPARTMENT OF MEDICINE

Workshop Goals

- Education on data security.
- Information on how to bring your computing devices into compliance.
  - Which devices are included.
- Where to find assistance with becoming compliant.

What is Data Stewardship?

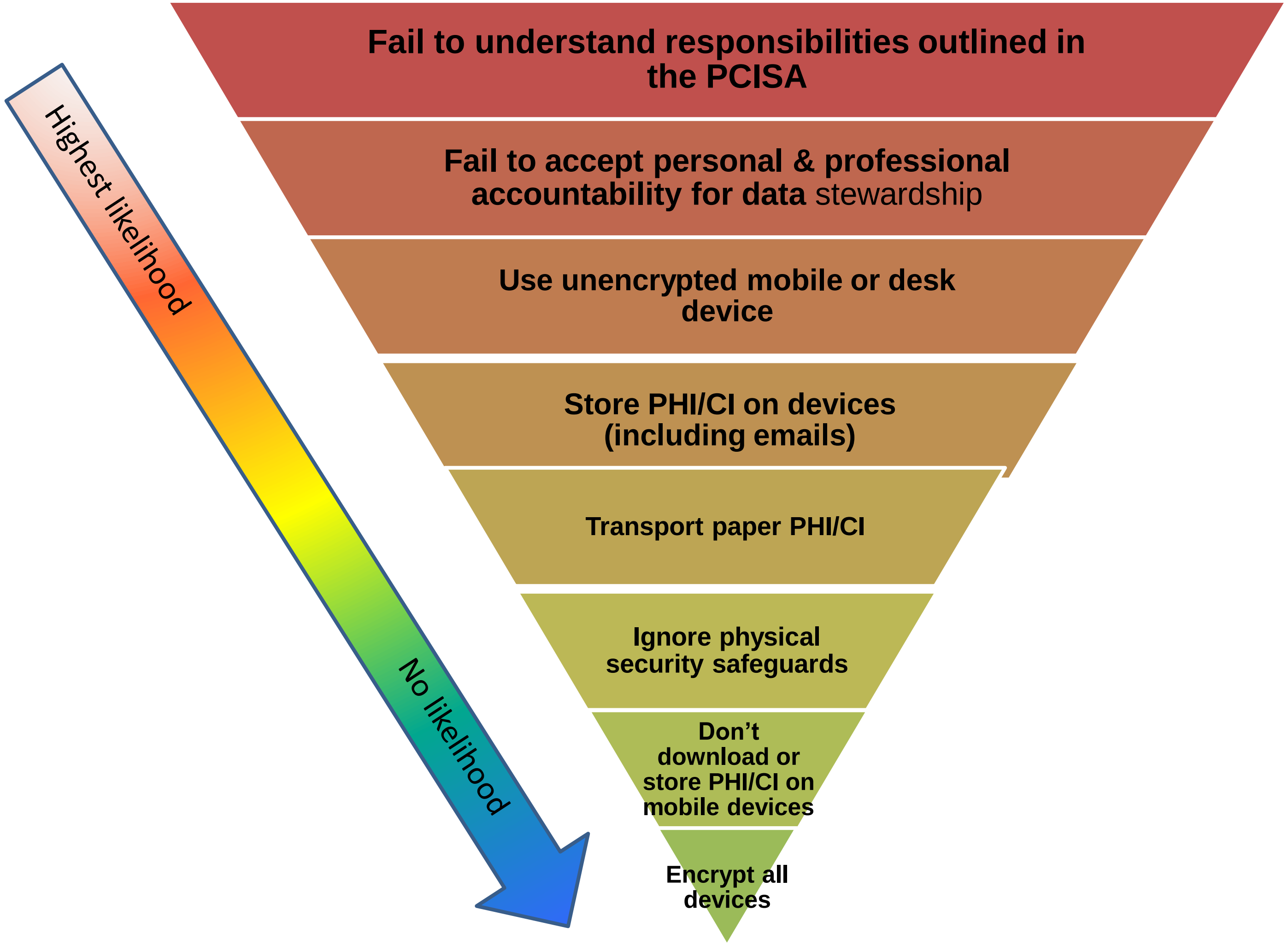
- Being personally and professionally responsible and accountable for the safeguarding of confidential and/or patient information to minimize the risk of a breach.
- Included information types (electronic or paper):
  - **Confidential** – Protection of data required by law
    - ***PHI*** - Protected by HIPAA
    - ***Individual Student Records*** - Protected by FERPA
    - ***Individual Financial Information*** (e.g., credit card, bank) and ***Personal Information*** (e.g., social security #, driver's license #) – Protected by Washington state's Personal Information law
    - ***Other Personal Information*** (e.g., home address, personal contact information, performance reviews) – Protected by Washington state's public records law
    - ***Proprietary*** - Intellectual property or trade secrets – Protected by Washington state's public records law
  - **Restricted** - Data that is not regulated, but for business purposes, is considered protected either by contract or best practice.
  - **Public** – Information that is published for public use or has been approved for general access by the appropriate University authority.

What is a Breach?

- Unauthorized acquisition, access, use, or disclosure of sensitive information that compromises the security or privacy of the information.
- Breaches can lead to investigations, bad will from the public, penalties, and/or fines.
- The US Department of Health and Human Services (DHHS) identifies two methods of securing PHI:
  - Destruction
  - Encryption
- No breach occurs if a compromised device is encrypted and password protected.
- If a device is compromised and is not encrypted and password protected, the burden of proof is on you to show there was no confidential data stored on it.

Likelihood of Information Security Breach

DECISION PYRAMID: LIKELIHOOD OF INFORMATION SECURITY BREACH



Fail to understand responsibilities outlined in the PCISA

Fail to accept personal & professional accountability for data stewardship

Use unencrypted mobile or desk device

Store PHI/CI on devices (including emails)

Transport paper PHI/CI

Ignore physical security safeguards

Don’t download or store PHI/CI on mobile devices

Encrypt all devices

UW Medicine
DEPARTMENT OF MEDICINE

What Happens if a Breach Occurs?

- Personal consequences.
- Institutional consequences.
- HIPAA reporting cascade.
  - Notification to OCR (Office for Civil Rights investigation).
  - Notification to UW Medicine Compliance.
  - All affected individuals must be notified. If more than ten lack addresses a public notification must be placed on our website.
  - If more than 500 individuals are affected local media must be informed.
- Contact Jennifer Dickey and Walt Morrison if a breach occurs.
  - Jennifer Dickey: jennd@medicine.washington.edu; 221-5947
  - Walt Morrison: wmorrison@medicine.washington.edu; 616-4726

Case Studies

- Case Study 1 – Resident Loses Physical Logbook with patient data.
  - 487 patients affected.
  - A breach occurred.
  - Notifications required.
- Case Study 2 – Laptop stolen from car while shopping.
  - Laptop was encrypted and password protected.
  - Laptop stored no PHI.
  - No breach occurred.
  - No notifications necessary.

Responsibilities

- Everyone who is using or viewing confidential or patient information must be personally and professionally accountable for safeguarding that information.
- Users (YOU) are responsible for the safekeeping of data under your care.
- Minimize your responsibility by limiting the data under your care.
  - The safest data is that which is never removed from institutional systems/servers.
    - Copied to mobile devices, flash drives, laptops, local desktops, etc.
- Policies per UW Medicine:
  - Must use strong passwords.
  - Passwords must be changed at least once every 120 days.
  - Internet access must be for business purposes or limited personal use.
  - All UW Medicine workforce members must report any suspected or known information security incident to UW Medicine Compliance.

Policy Versus Best Practices

Policy	Best Practice
Devices that move and contain Restricted or Confidential data must be encrypted.	Anything that can be encrypted should be. All desktop and laptop computers, mobile devices (phones, tablets, and otherwise), flash drives, network storage devices, etc.
Strong password usage for any account or device used to do business. This includes institutionally and personally owned devices that are used for UW work.	Computer/device lockouts after 15 minutes. Wiping of devices after 10 failed password attempts.
Use of cloud services for University business or intellectual property is prohibited without an appropriate contract. BAA, DSA, etc. https://security.uwmedicine.org/guidance/technical/legal_agreements/default.asp	Restrict storage of restricted and confidential data to institutional servers unless absolutely necessary.
	Using remote location and wipe features for mobile devices. iPhone: Find My iPhone (built-in) Android: Cerberus (https://www.cerberusapp.com) Windows Phone: Find My Phone (built-in)

Password Complexity – Strong Passwords

- Use the full keyboard.
  - Variety in character types and length makes passwords exponentially stronger.
- Don’t use single words or names.
- String multiple random words together to form a long password.
  - Don’t use common phrases.
  - Random sentences are a good example.
- A strong password (required by policy) must:
  - Be at least 8 characters long.
  - Mix upper and lower case letters.
  - Include numbers and symbols.

Physical Data Security

- Keep all physical restricted and confidential material behind lock and key.
  - Lock filing cabinets.
  - Lock offices when unattended.
  - Lock computers while unattended.
    - CTRL + ALT + DEL → Enter
    - Windows Key + L
- Maintain responsibility for mobile devices containing restricted and/or confidential material under your control.
  - Prevent portable devices from being lost or stolen.
  - Don't allow unauthorized parties potential access to restricted and/or confidential data.

UW Medicine
DEPARTMENT OF MEDICINE

Passwords and Encryption

- A password does not imply encryption, and encryption does not imply a password.
- A password is only a gatekeeper. It protects access to the device not the data stored on it.
- Different encryption methods have different means of operation.
  - BitLocker, on supported PC's, doesn't require any extra passwords.
  - FileVault for Macs requires an additional login during startup.
  - TrueCrypt always requires passwords.
- For maximum security, passwords and encryption must both be used.
- All restricted and confidential data stored in locations other than institutional servers must be encrypted and password protected.
- We recommend the following methods approved by UW Medicine:
  - Windows: BitLocker on compatible devices, TrueCrypt
  - Mac: FileVault
  - Mobile storage devices: TrueCrypt
    - Hardware-encrypted flash drives – Kingston DataTraveler 4000

Password Safety

- Don’t leave passwords on Sticky Notes (physical or digital).
  - A password safe program utilizing industry-standard encryption methods can be used to store difficult to remember passwords.
  - This makes using a unique password for each account easier.
  - The master password should be exceptionally strong. If compromised, all the accounts are at risk.
  - We recommend using a password safe.
    - KeePass - http://keepass.info
    - Password Safe - http://passwordsafe.sourceforge.net
    - 1Password - https://agilebits.com/onepassword
- Your password should be known only to you.
- Department of Medicine IT Services, UW Medicine IT Services, and UW-IT staff members will never ask you for your password.
  - We don’t want it.
- UW Medicine password policy and recommendations can be found here: https://security.uwmedicine.org/guidance/role_based/end_user

Data Storage

- Use computing in place whenever possible.
  - Terminal services, remote desktop, and/or webmail.
- Data should be stored only on institutional servers and systems unless there is a compelling reason not to.
  - User is responsible for security of removed data.
  - The device data is transferred to must be encrypted and password protected.
- Any data stored on local computers, laptops, flash drives, or mobile devices must be encrypted and removed when the need no longer persists.
- Sensitive information must never be stored with a cloud-service provider without an appropriate contract. BAA, DSA, etc. (https://security.uwmedicine.org/guidance/technical/legal_agreements/default.asp)
  - These include (but are not limited to): Dropbox, Google Drive, Box, SkyDrive, iCloud, SpiderOak, etc.
  - Data stored on these services is no longer under institutional control and can be compromised.
  - SkyDrive Pro, provided by the UW is certified for confidential data such as PHI.

Smartphone/Tablet Security

- Use a strong password to lock the device.
- Enable encryption.
  - iPhones/iPads do this automatically with an unlock password.
  - Removable SD cards should be encrypted as well.
- Set an automatic lockout timer on the device.
  - No greater than 15 minutes.
  - Shorter lock times are highly recommended.
- Don’t use cloud backup services.
  - iOS devices – Use iTunes encrypted backups (http://support.apple.com/kb/HT4946)
  - Android devices – Helium (available in the Play Store)
- Initiate a device wipe after 10 failed password attempts.
  - Most devices initiate a timed lockout after a certain number of failed password attempts.
  - Android does not have this capability.
- Don’t store data on the SIM card (contacts, SMS, etc).
  - Smartphones store data on internal storage by default. Non-smartphones sometimes store contacts and SMS messages directly on the SIM card. This must be avoided for restricted and confidential data.

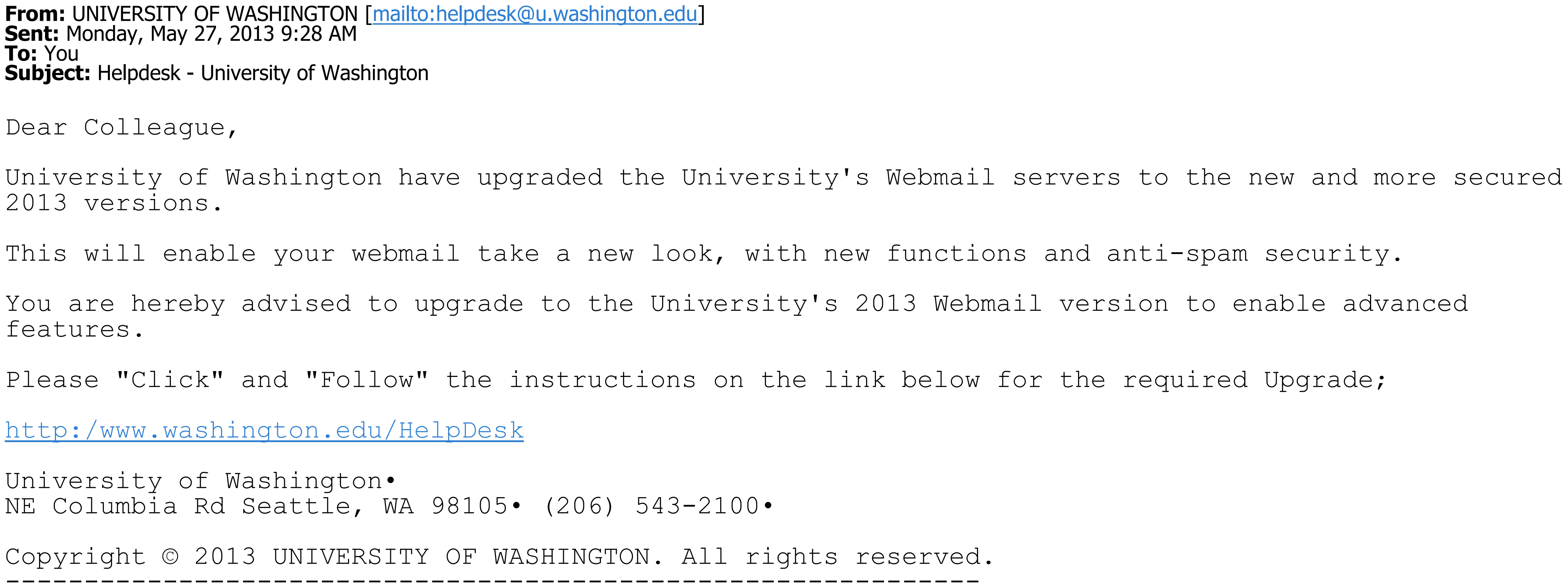
Email Security

- All email containing Restricted or Confidential data must be secured in transport.
  - Encrypted connections must be used between email servers.
- Messages between University email systems (Outpost, UW Exchange, and UW Deskmail) and some recipients are automatically encrypted.
  - This encryption only applies to message data while it moves between servers. It likely will not be encrypted once it reaches its destination mail server.
  - UW Google Apps should NOT be used for University business.
- Restricted or Confidential information sent over email must be delivered to a secure system.
  - UW Medicine maintains a list of pre-approved email systems on their site: https://security.uwmedicine.org/guidance/technical/email/approved_list.asp.
- Email in Outlook (and other email clients) is cached on the local machine, as are any attachments you open from email messages.
  - This information can be retrieved offline if the local storage of the device is not encrypted.

Email Safety – Phishing and Other Scams

- Never open email attachments if you don't know the sender.
  - If an attachment is at all suspicious (the filename ends in .exe or .zip, or it doesn't make sense), don't open it.
- Email addresses can be spoofed. Don't trust an email just because of who it shows it came from.
- Recognize bogus links in phishing emails.
  - Hover your cursor over the hyperlink. The URL (web address) it links to will be displayed somewhere on your screen.
- If the context of the message doesn't make sense to you, don't open it.
  - If you're not expecting an email from the IRS, it's most likely not a legitimate message.
- UW Medicine page on phishing emails: https://security.uwmedicine.org/guidance/technical/email/caught_phishers.asp

Phishing Email Example



From: UNIVERSITY OF WASHINGTON [mailto:helpdesk@u.washington.edu]
Sent: Monday, May 27, 2013 9:28 AM
To: You
Subject: Helpdesk - University of Washington

Dear Colleague,

University of Washington have upgraded the University's Webmail servers to the new and more secured 2013 versions.

This will enable your webmail take a new look, with new functions and anti-spam security.

You are hereby advised to upgrade to the University's 2013 Webmail version to enable advanced features.

Please "Click" and "Follow" the instructions on the link below for the required Upgrade;

http:/www.washington.edu/HelpDesk

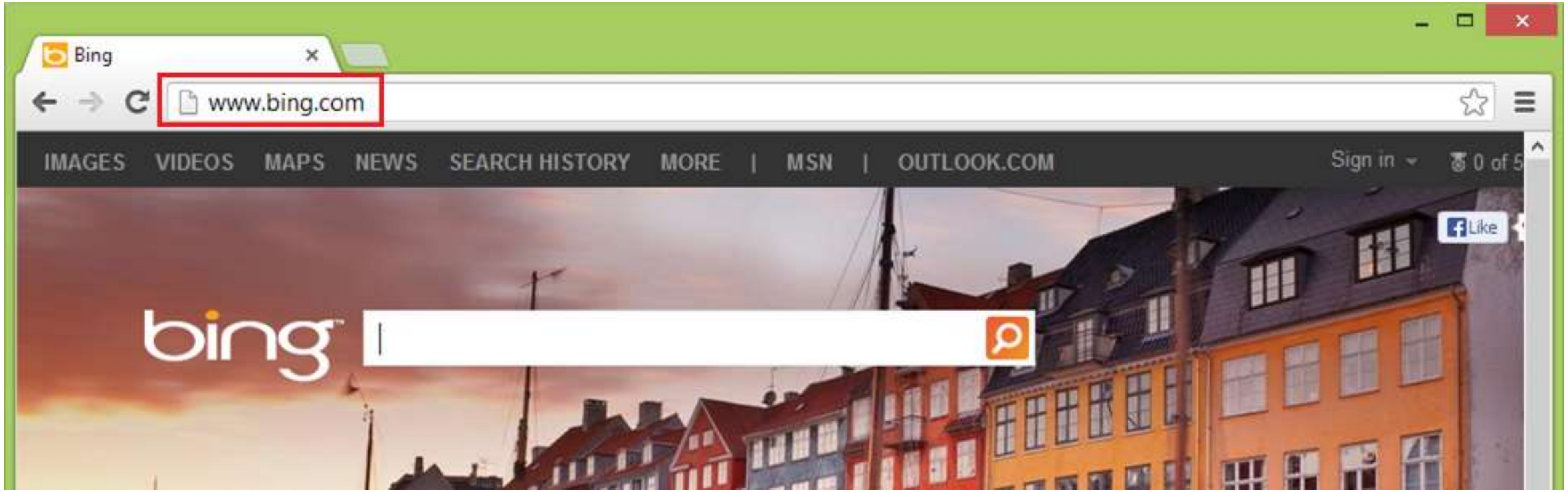
University of Washington•
NE Columbia Rd Seattle, WA 98105• (206) 543-2100•

Copyright © 2013 UNIVERSITY OF WASHINGTON. All rights reserved.

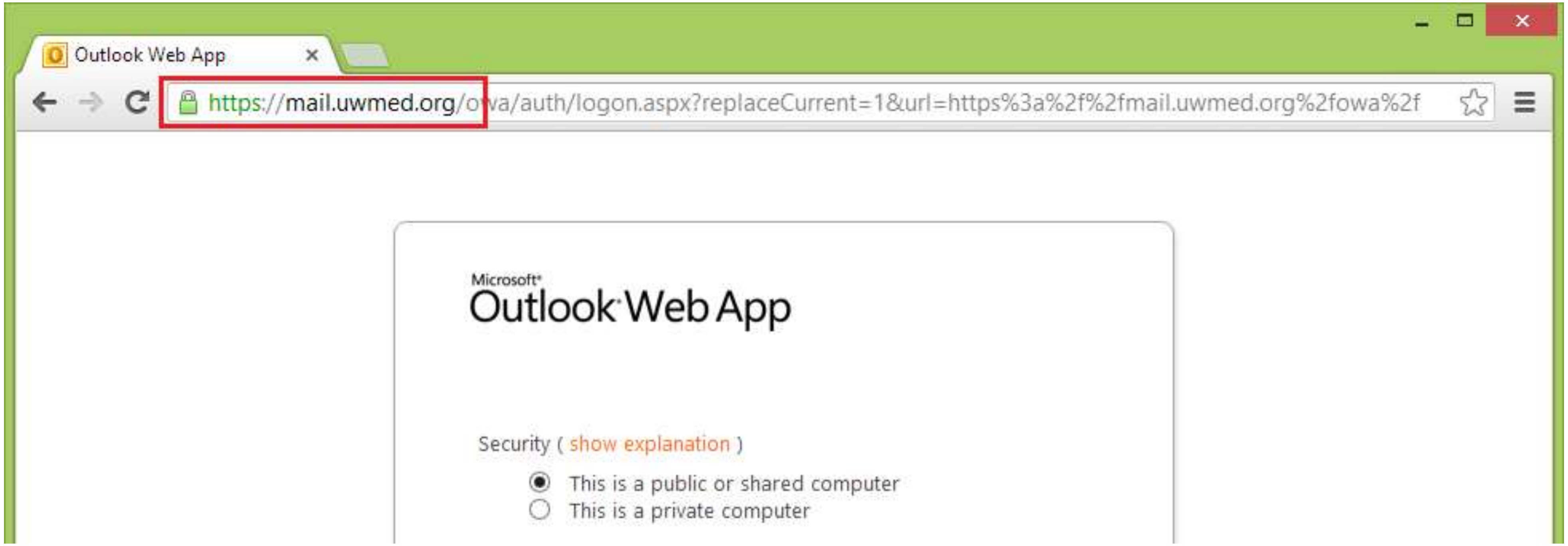
Personal Computer Safety

- Install software updates as available.
  - Modern browsers greatly improve browsing safety.
- If entering sensitive information into a form on a web page make sure that the connection to the site is encrypted.
  - Chrome, Firefox, and Internet Explorer all show grey lock icons next to the address bar.
  - Web addresses begin with 'https://' instead of 'http://'
- Don't run questionable programs.
  - "Youtube Video Downloader" is one example.
- Don't click on questionable links.
  - There's no such thing as a '1 millionth visitor' prize.
- Be wary of your activities on "open" Wi-Fi networks.
  - If you don't have to enter a password to connect, it is not secure.
    - Network passwords that have been entered once and are automatically stored are an exception.
  - The UW wireless network is an open network.
- More Information: https://www.washington.edu/itconnect/security/

Unencrypted Site



Encrypted Site

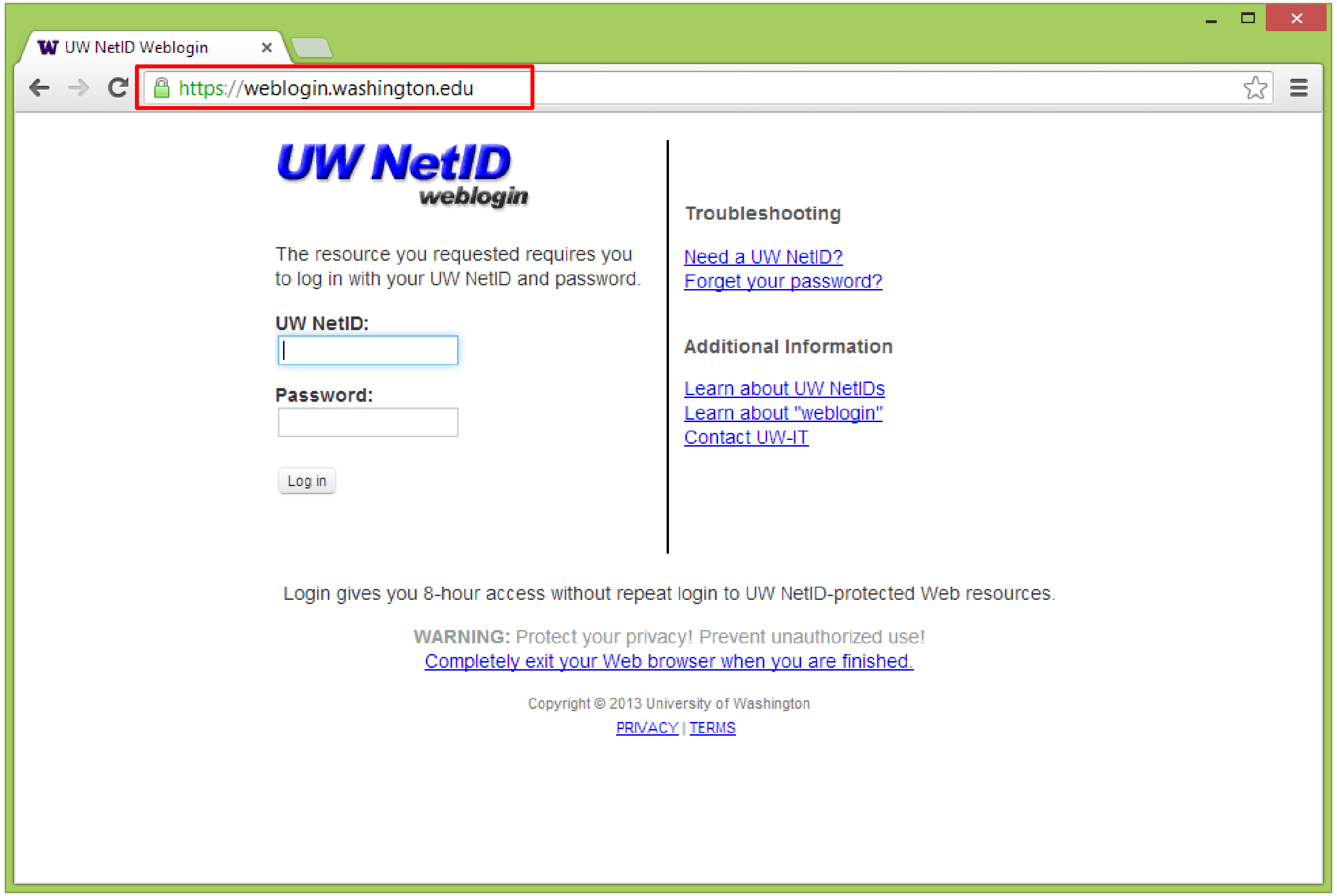


https://mail.uwmed.org/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fmail.uwmed.org%2fowa%2f

Security (show explanation)

● This is a public or shared computer
○ This is a private computer

UW NetID Login Page



The resource you requested requires you to log in with your UW NetID and password.

UW NetID:

Password:

Troubleshooting

Need a UW NetID?
Forget your password?

Additional Information

Learn about UW NetIDs
Learn about "weblogin"
Contact UW-IT

Login gives you 8-hour access without repeat login to UW NetID-protected Web resources.

WARNING: Protect your privacy! Prevent unauthorized use!
Completely exit your Web browser when you are finished.

Copyright © 2013 University of Washington
PRIVACY | TERMS

Secure Remote Access of Resources

- Utilize the Department of Medicine's NetExtender SSL VPN or AMC's Juniper SSL VPN service for remotely accessing UW resources.
  - Use a terminal server or remote desktop access to your workstation.
- Avoid using computers you are not personally responsible for to access University resources.
- Only store sensitive material on mobile devices if it is absolutely necessary.
  - Make sure that the storage of the mobile device is properly encrypted.

Informational Resources

- Department of Medicine Intranet Site: http://depts.washington.edu/domweb/
- UW Medicine Security: https://security.uwmedicine.org/
- The Office of the Chief Information Security Officer for the UW provides resources on their site regarding safe computing - https://ciso.washington.edu/
  - Risk Advisories and Best Practices - https://ciso.washington.edu/resources/risk-advisories/
  - Online Training - https://ciso.washington.edu/resources/online-training/
- A copy of this presentation, as well as technical documentation for securing computers and mobile devices, will be emailed to you.

Laptop Encryption Prerequisites

- Mac
  - FileVault 2 - Mac OS X 10.6 “Snow Leopard”
    - Older version of OS X will not encrypt the entire disk.
- Windows
  - BitLocker – Windows Vista or 7 Ultimate or Enterprise, or Windows 8 Pro or Enterprise.
    - TPM chip or dedicated USB flash drive.
  - TrueCrypt – No special requirements; requires a password during computer startup.
    - Blank CD for recovery disk.

Where to Get Help

- UW IT
  - 206.221.5000
  - help@uw.edu
- Department of Medicine IT Services
  - 206.616.8805
  - ishelp@medicine.washington.edu

END OF PRESENTATION

APPENDIX A – IOS DEVICE SECURITY

APPENDIX B – ANDROID DEVICE SECURITY

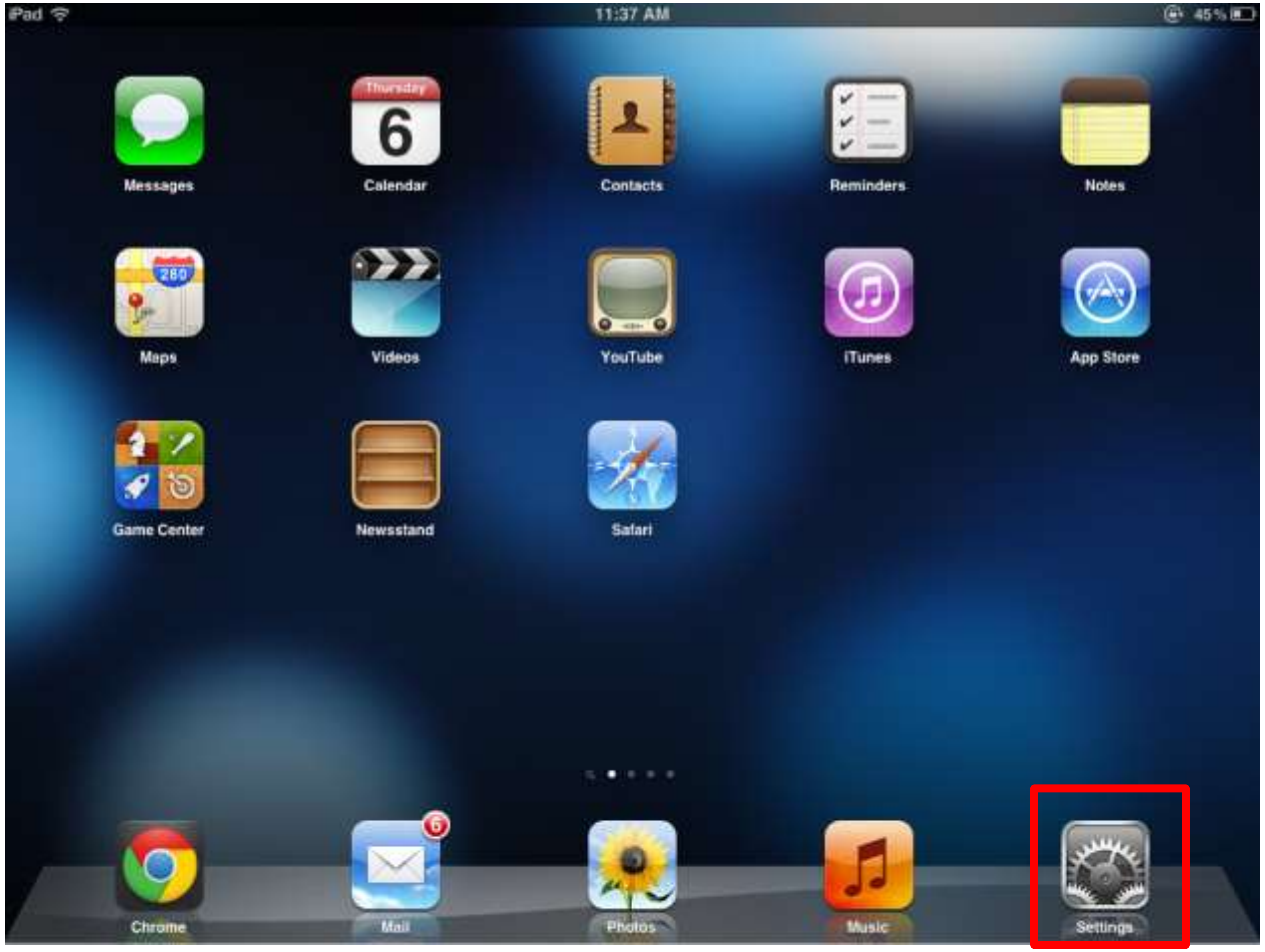
APPENDIX C – WINDOWS PHONE SECURITY

APPENDIX D – ADDITIONAL INFORMATION

IPHONE/IPAD SECURITY

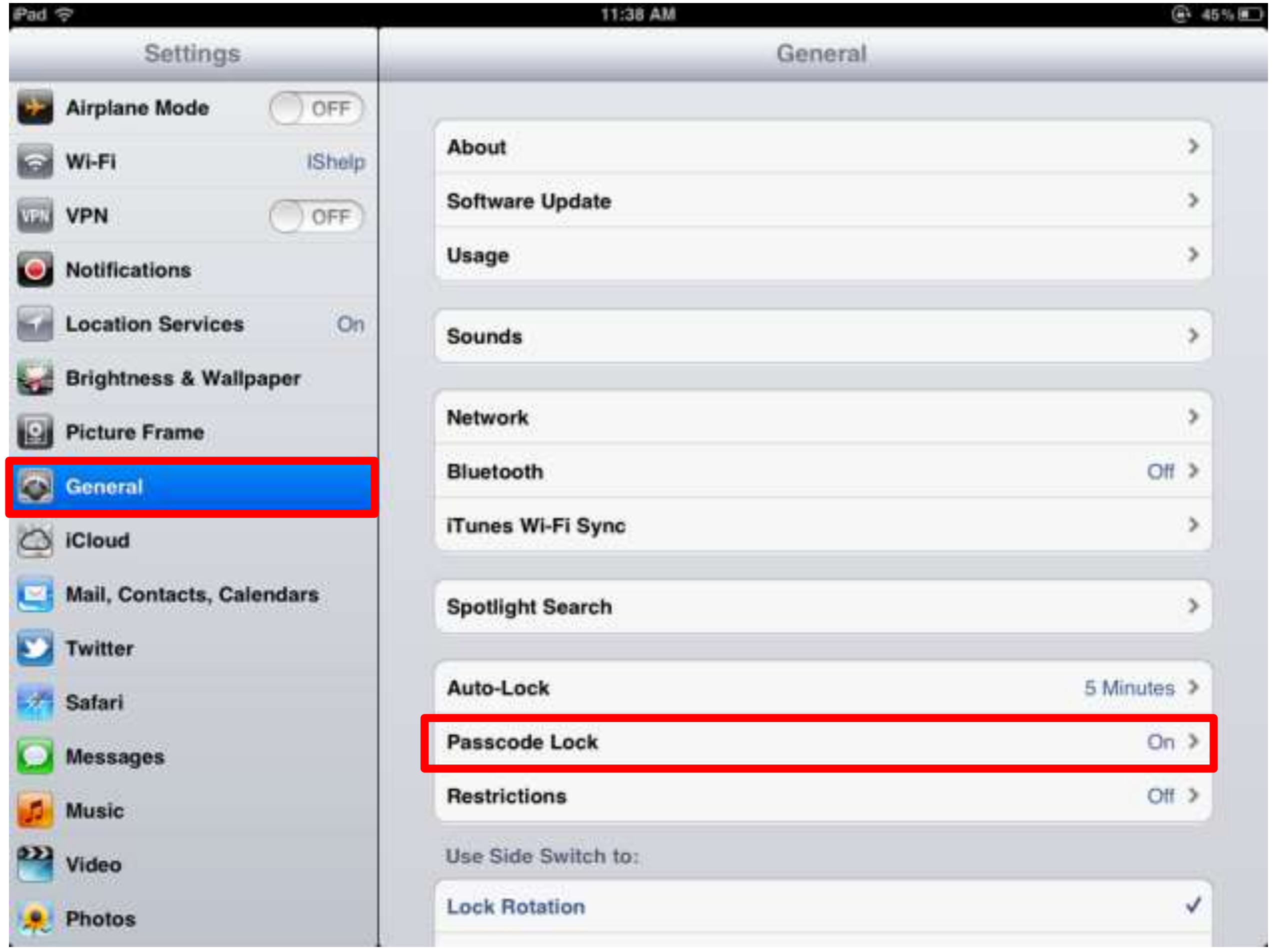
APPENDIX A

iOS Device Encryption (iPhone, iPad)



UW Medicine
DEPARTMENT OF MEDICINE

iOS Device Encryption (iPhone, iPad)



iPad 11:38 AM 45%

Settings

Airplane Mode OFF

Wi-Fi iShelp

VPN OFF

Notifications

Location Services On

Brightness & Wallpaper

Picture Frame

General

iCloud

Mail, Contacts, Calendars

Twitter

Safari

Messages

Music

Video

Photos

General

About

Software Update

Usage

Sounds

Network

Bluetooth Off

iTunes Wi-Fi Sync

Spotlight Search

Auto-Lock 5 Minutes

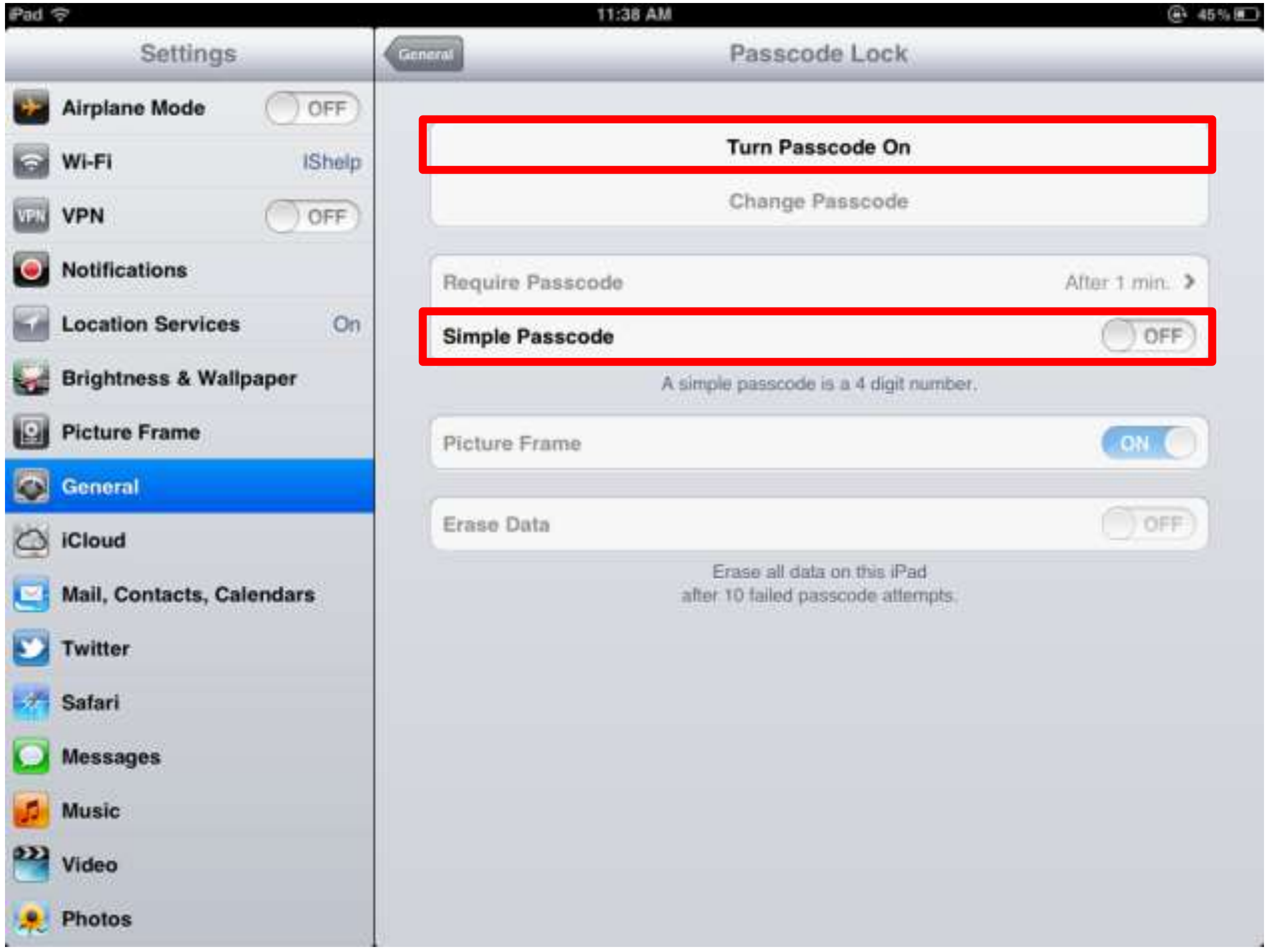
Passcode Lock On

Restrictions Off

Use Side Switch to:

Lock Rotation ✓

iOS Device Encryption (iPhone, iPad)



iPad 11:38 AM 45%

Settings

- Airplane Mode: OFF
- Wi-Fi: IShelp
- VPN: OFF
- Notifications
- Location Services: On
- Brightness & Wallpaper
- Picture Frame
- General
- iCloud
- Mail, Contacts, Calendars
- Twitter
- Safari
- Messages
- Music
- Video
- Photos

General

Passcode Lock

Turn Passcode On

Change Passcode

Require Passcode: After 1 min.

Simple Passcode: OFF

A simple passcode is a 4 digit number.

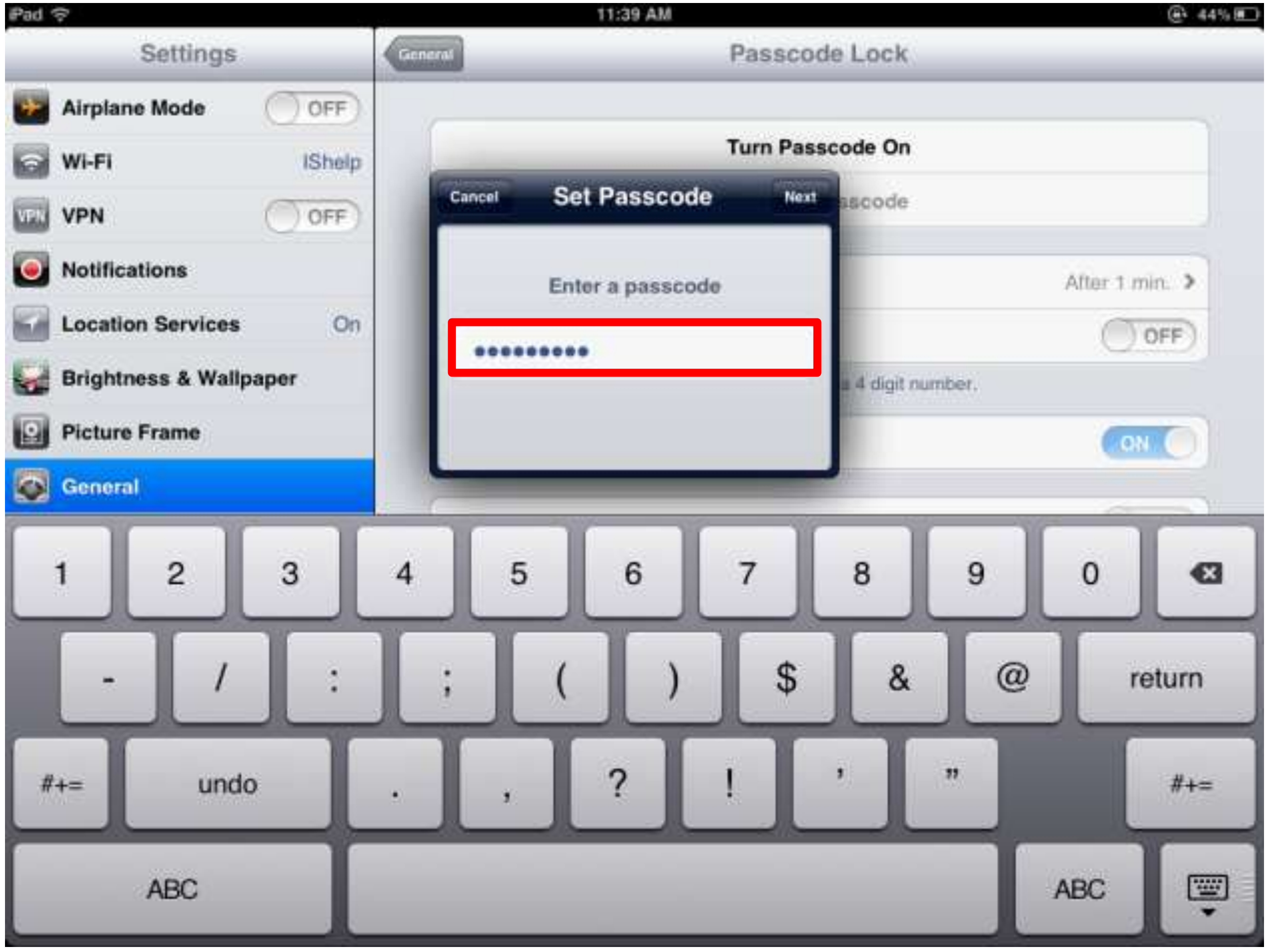
Picture Frame: ON

Erase Data: OFF

Erase all data on this iPad
after 10 failed passcode attempts.

UW Medicine
DEPARTMENT OF MEDICINE

iOS Device Encryption (iPhone, iPad)



Settings

- Airplane Mode OFF
- Wi-Fi iShelp
- VPN OFF
- Notifications
- Location Services On
- Brightness & Wallpaper
- Picture Frame
- General

Passcode Lock

Turn Passcode On

Set Passcode

Enter a passcode

••••••••••

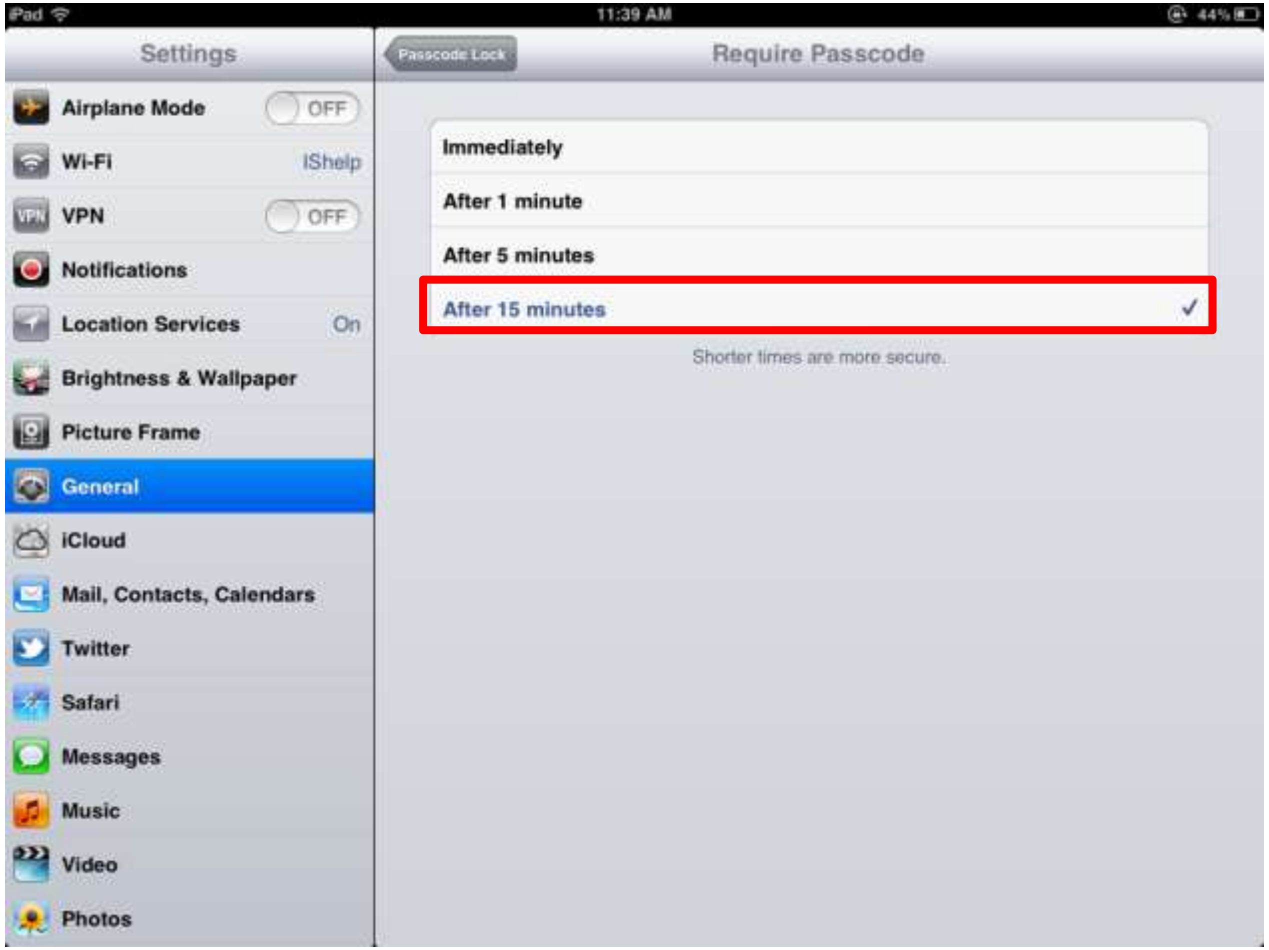
After 1 min.

OFF

4 digit number.

ON

iOS Device Encryption (iPhone, iPad)

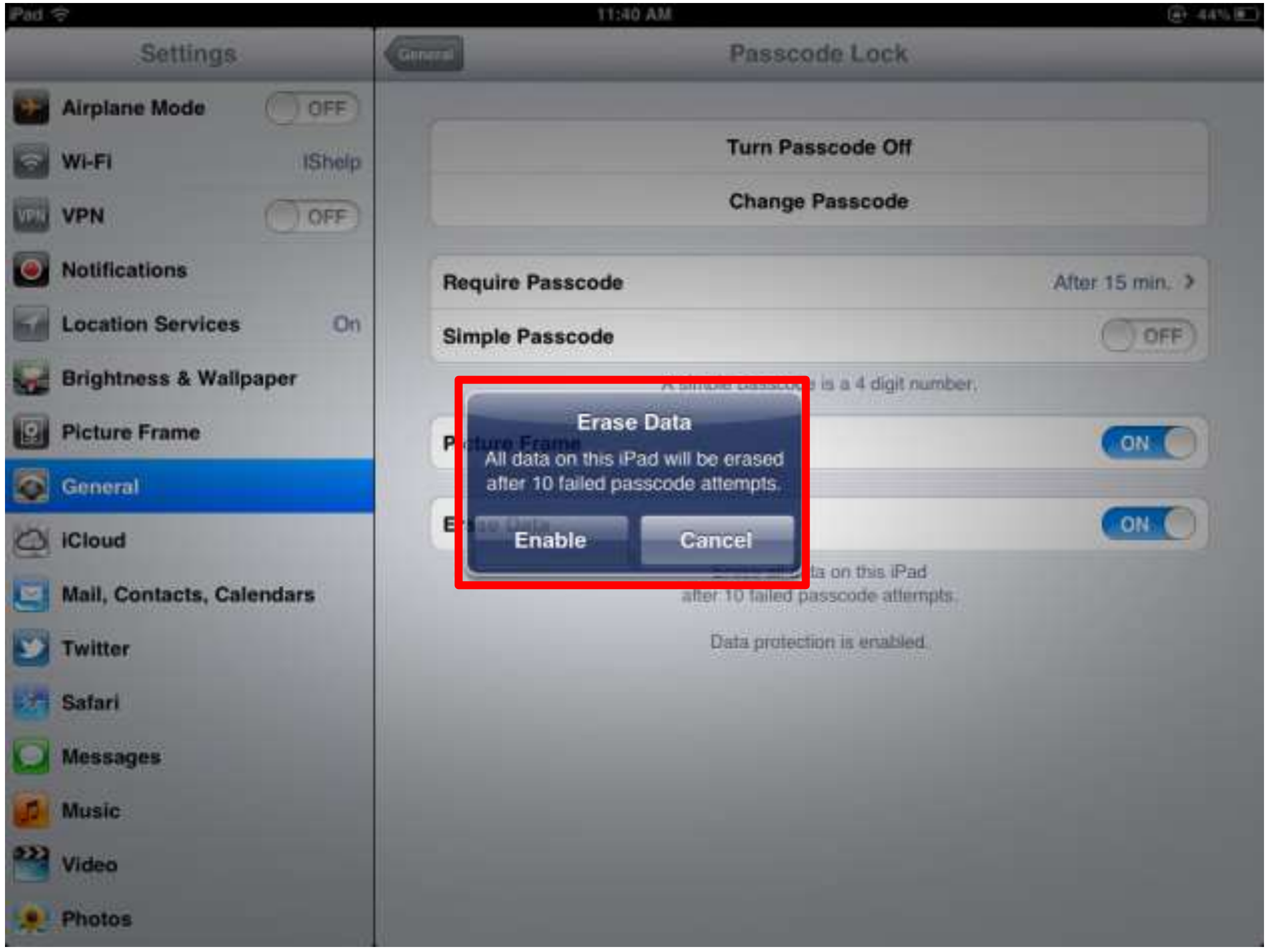


Require Passcode

- Immediately
- After 1 minute
- After 5 minutes
- After 15 minutes ✓

Shorter times are more secure.

iOS Device Encryption (iPhone, iPad)



Require Passcode After 15 min.

Simple Passcode OFF

A simple passcode is a 4 digit number.

Picture Frame ON

Erase Data ON

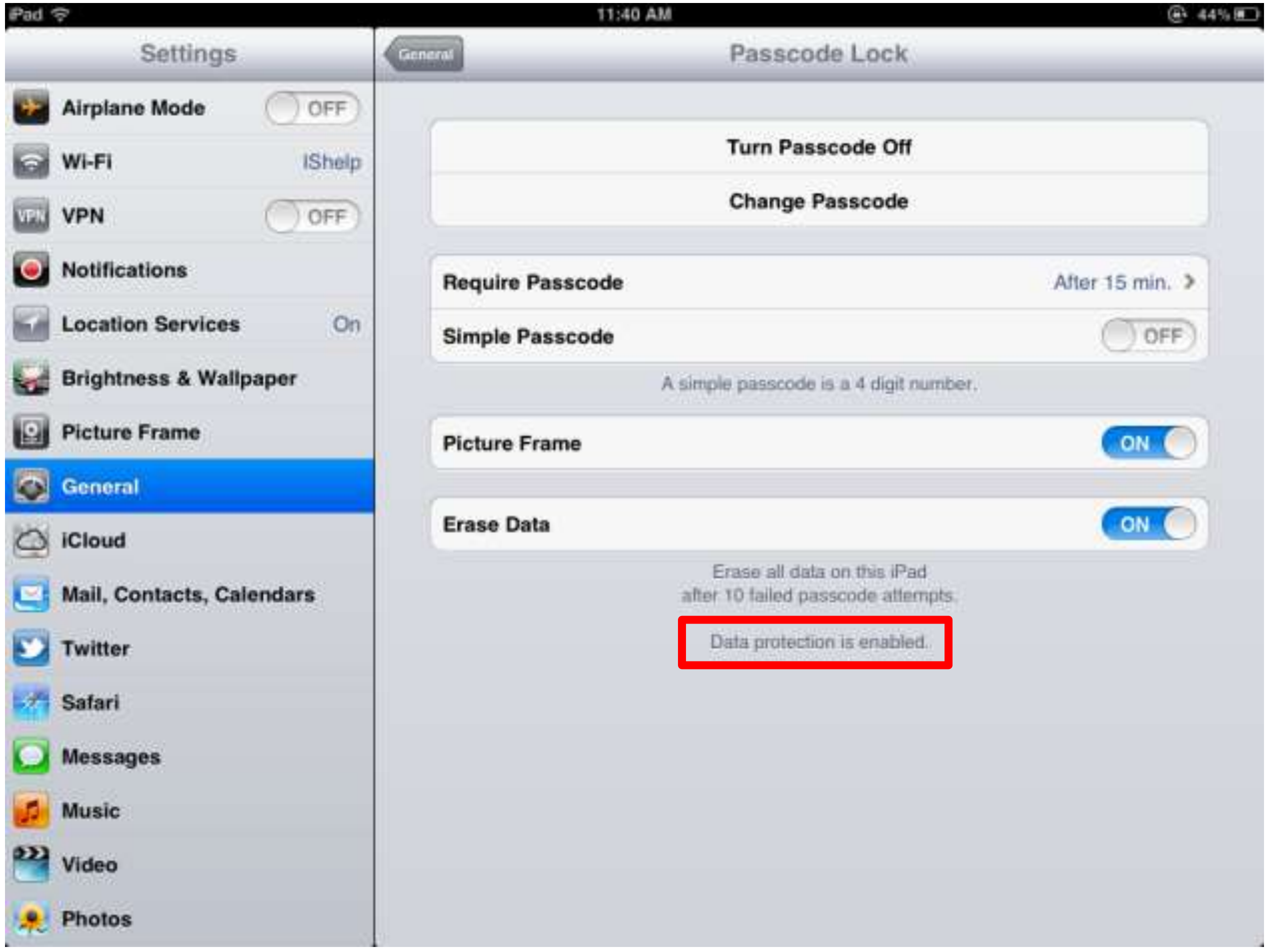
Erase all data on this iPad after 10 failed passcode attempts.

Data protection is enabled.

Erase Data

All data on this iPad will be erased after 10 failed passcode attempts.

iOS Device Encryption (iPhone, iPad)



Passcode Lock

Turn Passcode Off

Change Passcode

Require Passcode: After 15 min.

Simple Passcode: OFF

A simple passcode is a 4 digit number.

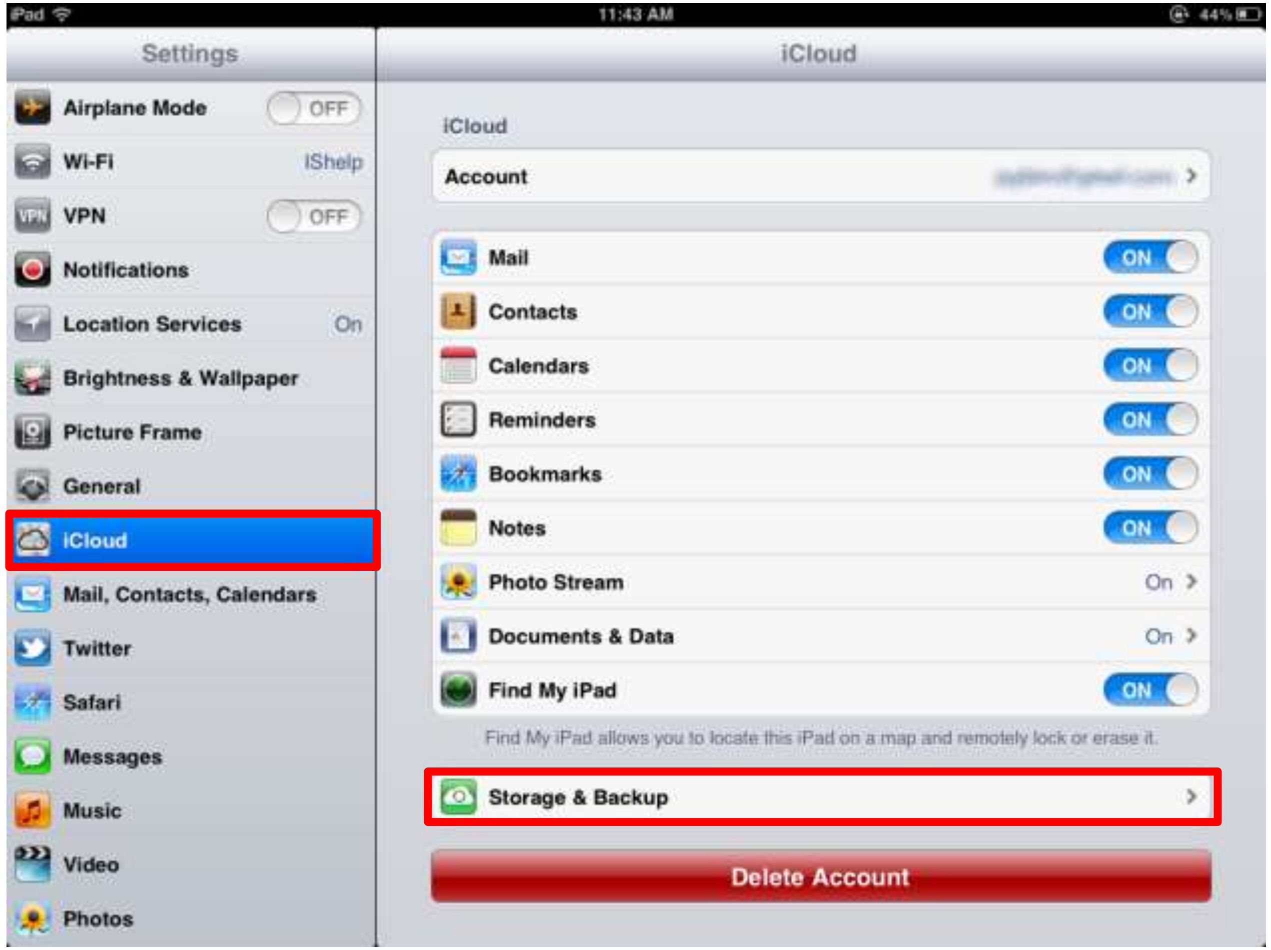
Picture Frame: ON

Erase Data: ON

Erase all data on this iPad
after 10 failed passcode attempts.

Data protection is enabled.

Disable iCloud Backups(iPhone, iPad)



iPad 11:43 AM 44%

Settings

Airplane Mode OFF

Wi-Fi iShelp

VPN OFF

Notifications

Location Services On

Brightness & Wallpaper

Picture Frame

General

iCloud

Mail, Contacts, Calendars

Twitter

Safari

Messages

Music

Video

Photos

iCloud

iCloud

Account [redacted]

Mail ON

Contacts ON

Calendars ON

Reminders ON

Bookmarks ON

Notes ON

Photo Stream On

Documents & Data On

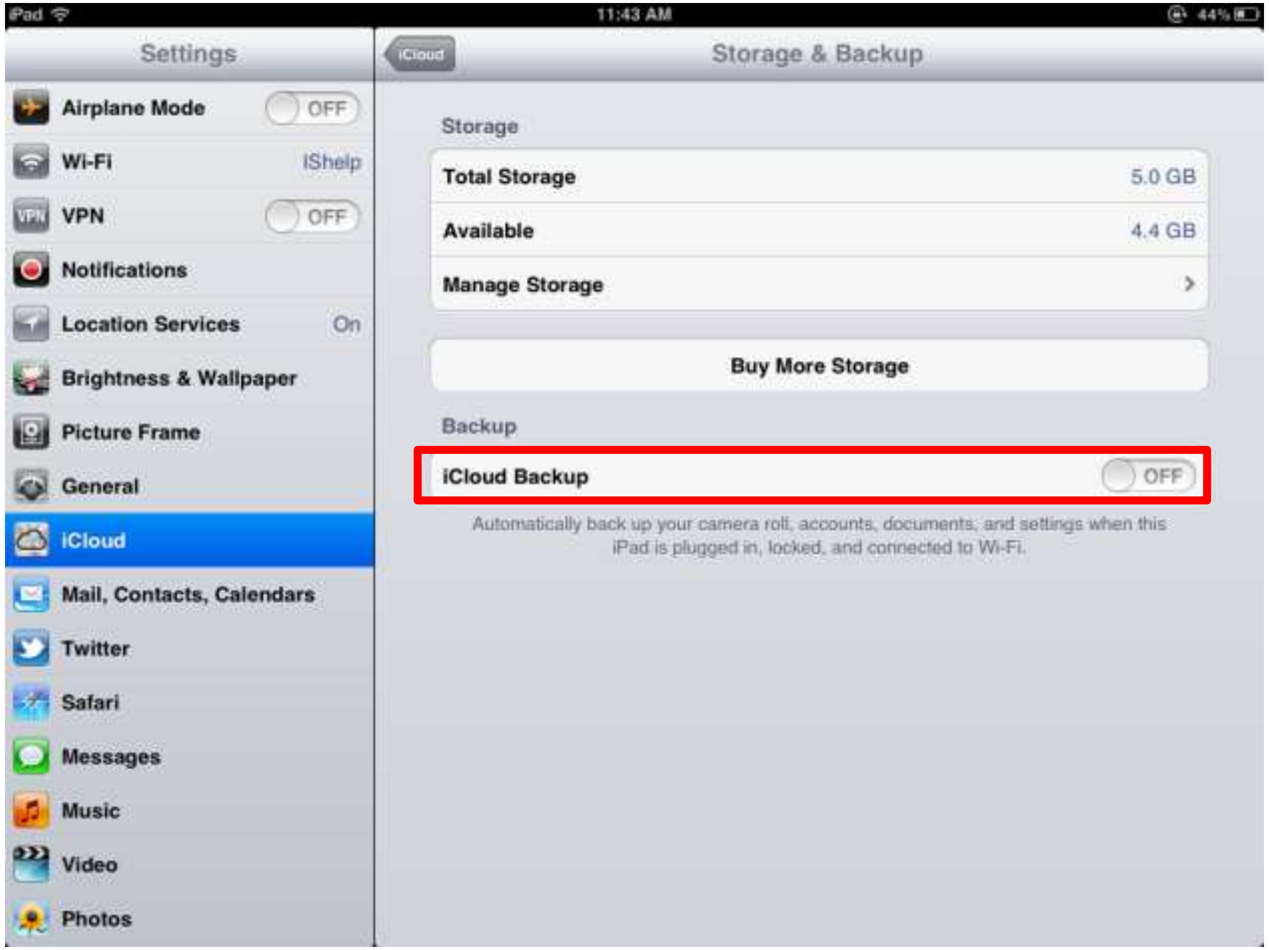
Find My iPad ON

Find My iPad allows you to locate this iPad on a map and remotely lock or erase it.

Storage & Backup

Delete Account

Disable iCloud Backups (iPhone, iPad)



Airplane Mode OFF
Wi-Fi iShelp
VPN OFF
Notifications
Location Services On
Brightness & Wallpaper
Picture Frame
General
iCloud
Mail, Contacts, Calendars
Twitter
Safari
Messages
Music
Video
Photos

Storage

Total Storage 5.0 GB
Available 4.4 GB
Manage Storage ›

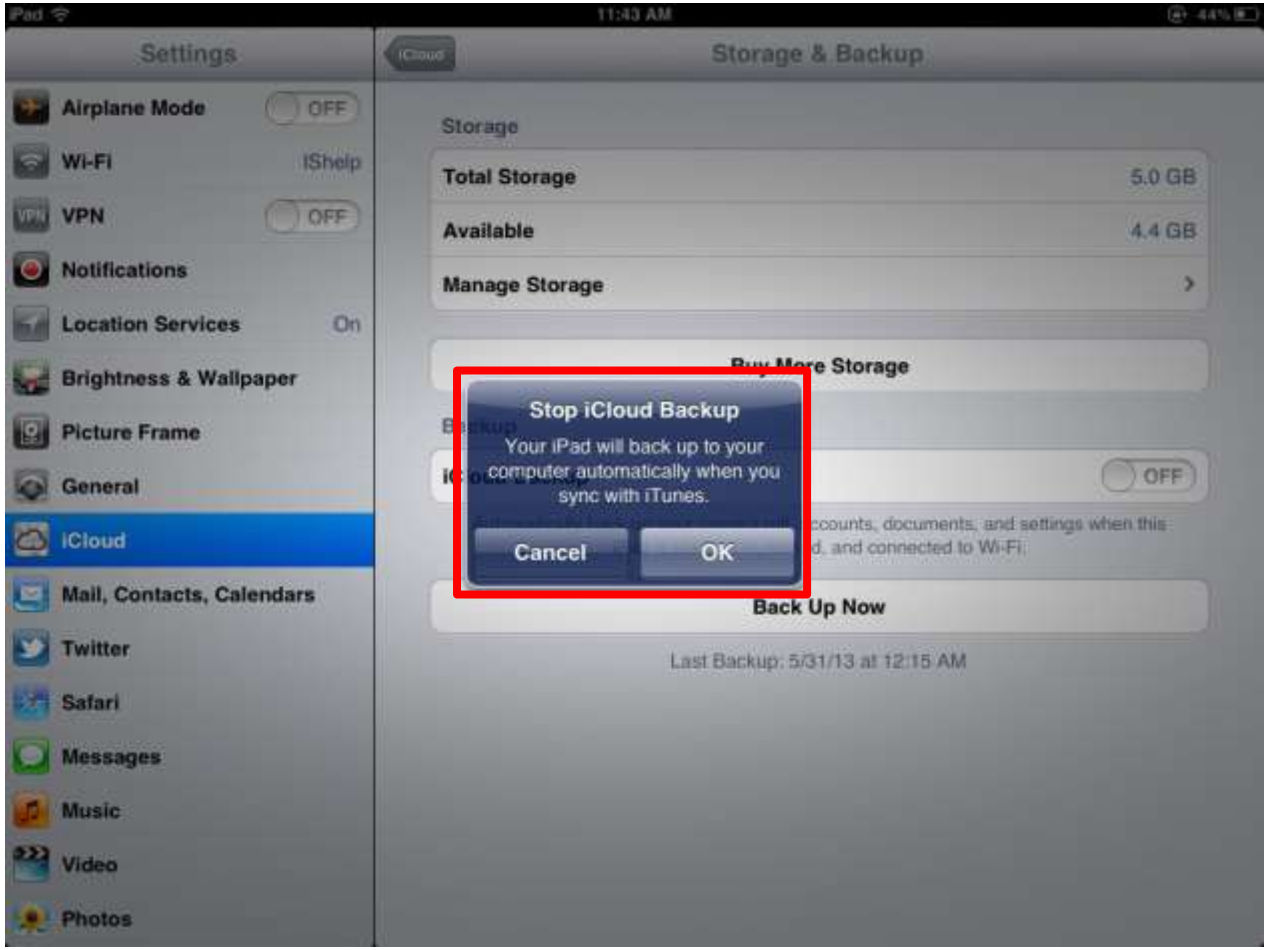
Buy More Storage

Backup

iCloud Backup OFF

Automatically back up your camera roll, accounts, documents, and settings when this iPad is plugged in, locked, and connected to Wi-Fi.

Disable iCloud Backups (iPhone, iPad)



Airplane Mode OFF

Wi-Fi IShelp

VPN OFF

Notifications

Location Services On

Brightness & Wallpaper

Picture Frame

General

iCloud

Mail, Contacts, Calendars

Twitter

Safari

Messages

Music

Video

Photos

Storage

Total Storage	5.0 GB
Available	4.4 GB
Manage Storage	›

Buy More Storage

Backup

iCloud Backup OFF

...ccounts, documents, and settings when this ...d, and connected to Wi-Fi.

Stop iCloud Backup

Your iPad will back up to your computer automatically when you sync with iTunes.

Cancel OK

Back Up Now

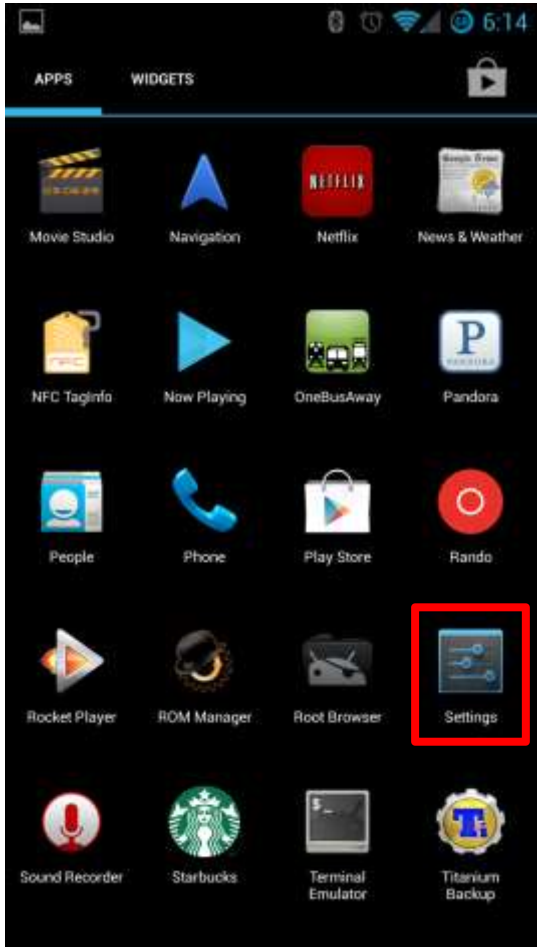
Last Backup: 5/31/13 at 12:15 AM

ANDROID SECURITY

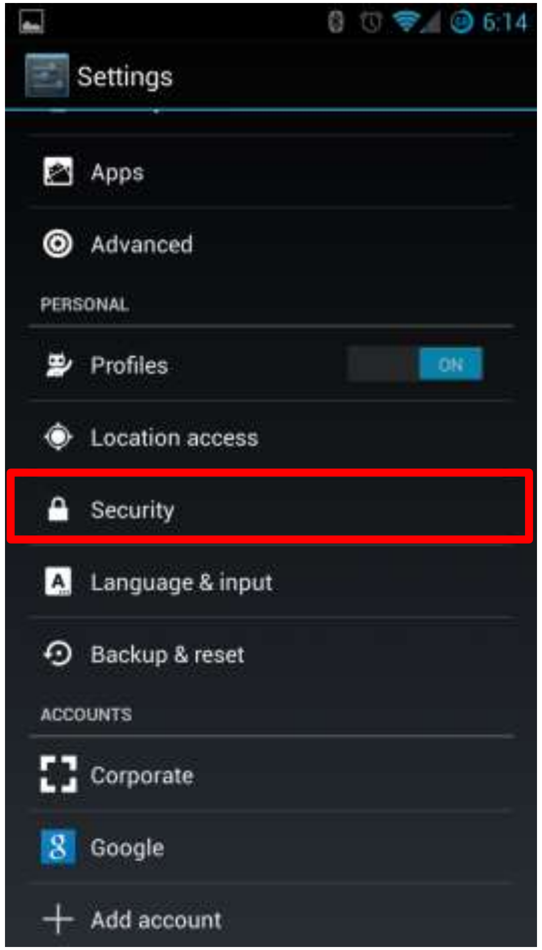
APPENDIX B

Android Device Security

Android Device Security

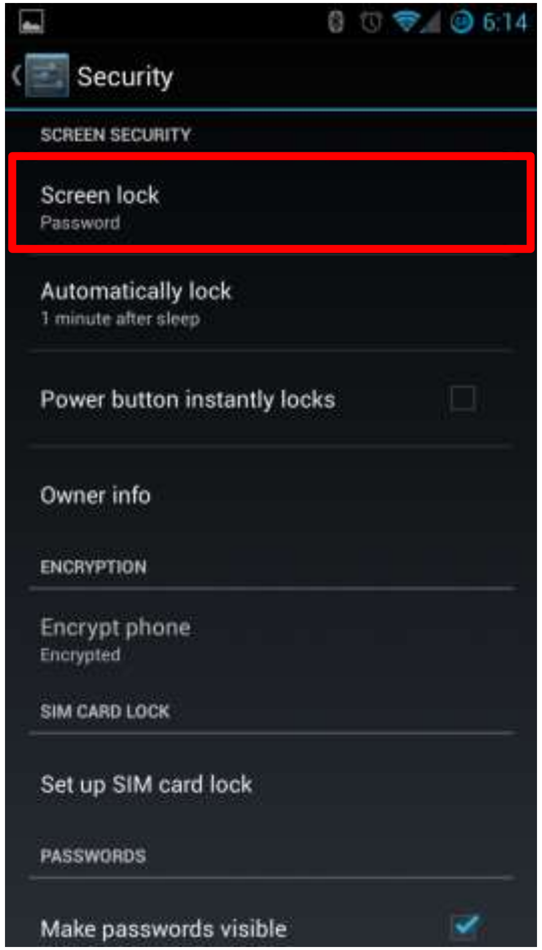


Android Device Security



UW Medicine
DEPARTMENT OF MEDICINE

Android Device Security



Security

SCREEN SECURITY

Screen lock
Password

Automatically lock
1 minute after sleep

Power button instantly locks □

Owner info

ENCRYPTION

Encrypt phone
Encrypted

SIM CARD LOCK

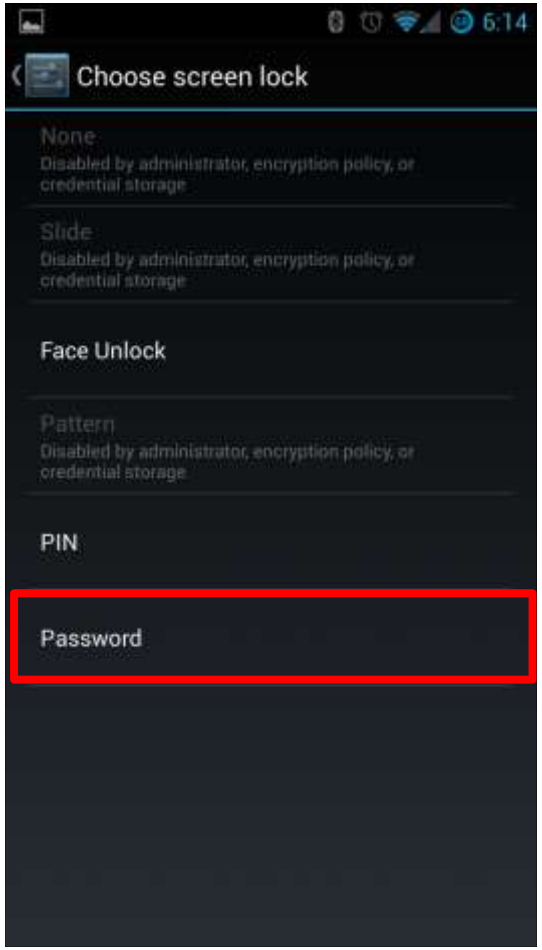
Set up SIM card lock

PASSWORDS

Make passwords visible ☑

UW Medicine
DEPARTMENT OF MEDICINE

Android Device Security



Choose screen lock

None
Disabled by administrator, encryption policy, or credential storage

Slide
Disabled by administrator, encryption policy, or credential storage

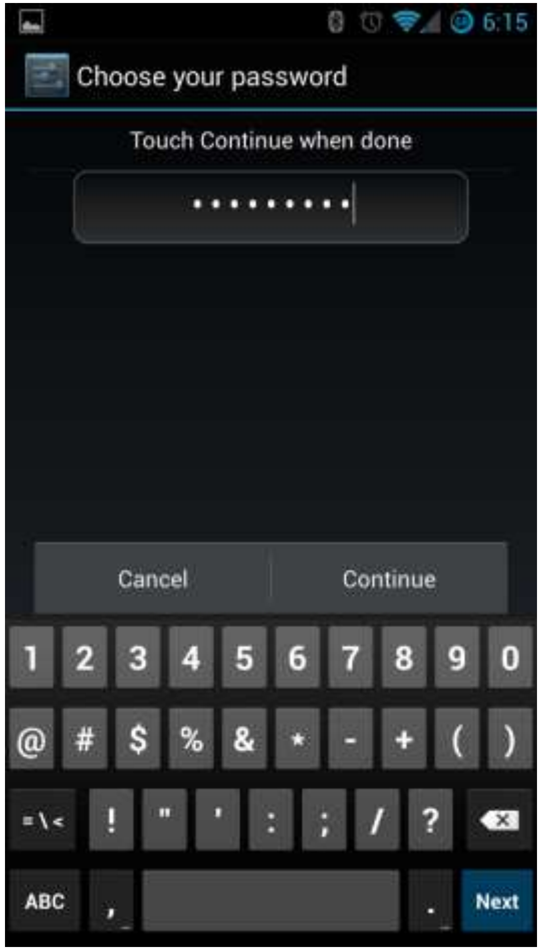
Face Unlock

Pattern
Disabled by administrator, encryption policy, or credential storage

PIN

Password

Android Device Security



6:15

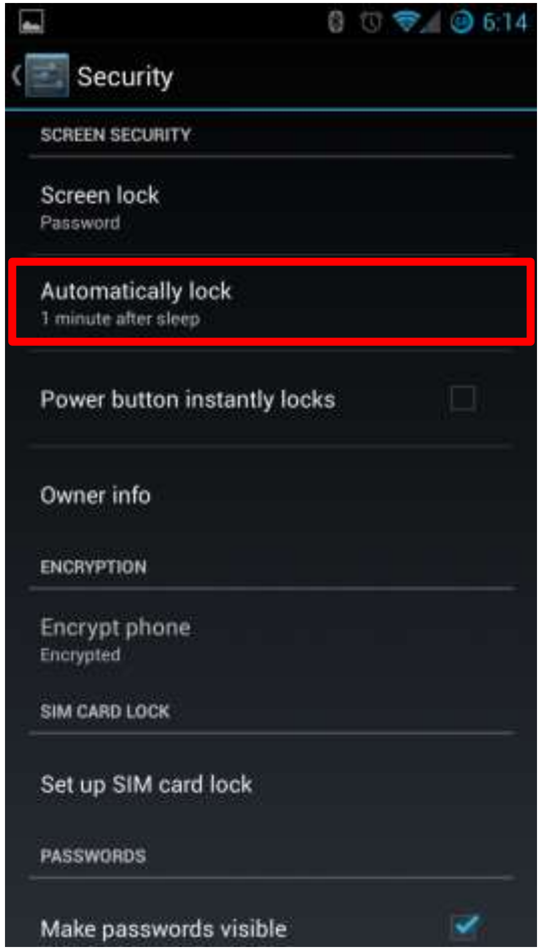
Choose your password

Touch Continue when done

••••••••••

UW Medicine
DEPARTMENT OF MEDICINE

Android Device Security



6:14

Security

SCREEN SECURITY

Screen lock
Password

Automatically lock
1 minute after sleep

Power button instantly locks □

Owner info

ENCRYPTION

Encrypt phone
Encrypted

SIM CARD LOCK

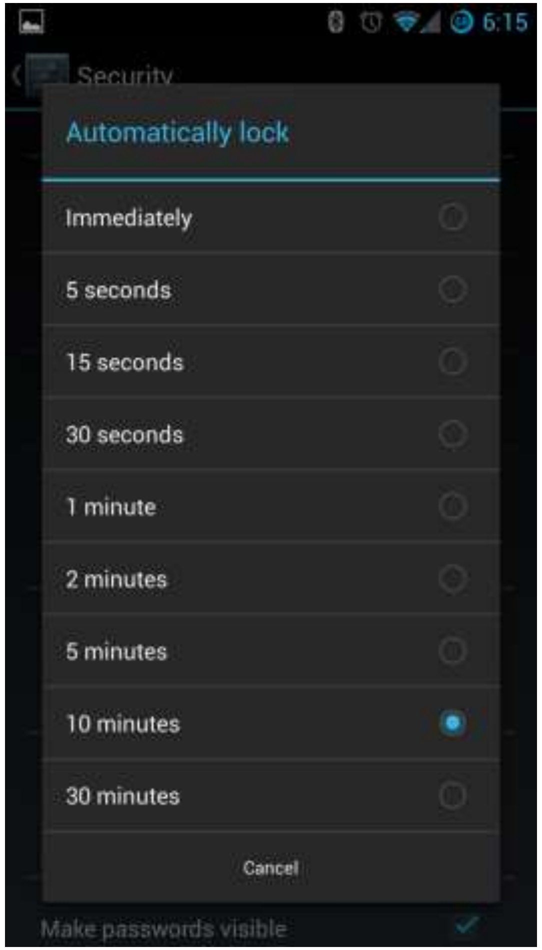
Set up SIM card lock

PASSWORDS

Make passwords visible ☑

UW Medicine
DEPARTMENT OF MEDICINE

Android Device Security



6:15

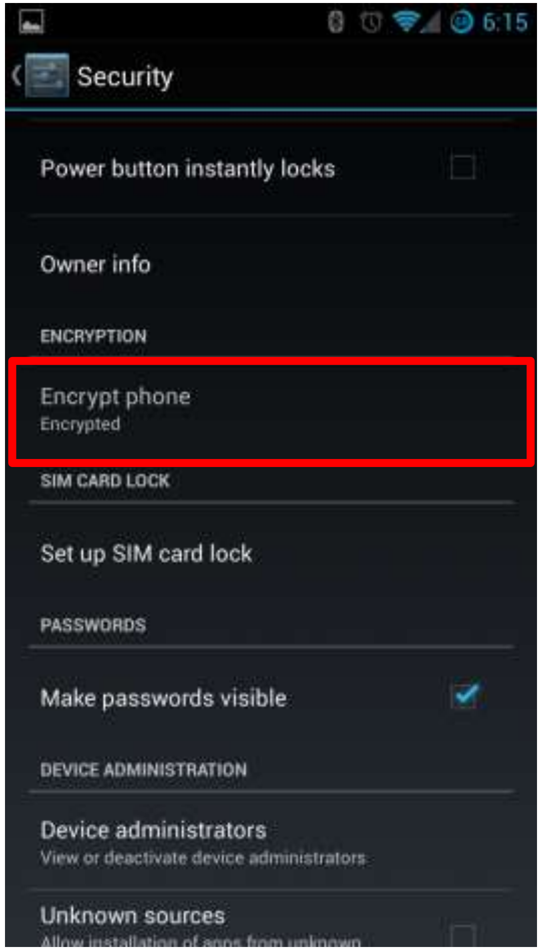
Security

Automatically lock

- Immediately ○
- 5 seconds ○
- 15 seconds ○
- 30 seconds ○
- 1 minute ○
- 2 minutes ○
- 5 minutes ○
- 10 minutes ●
- 30 minutes ○

Make passwords visible ✓

Android Device Security



6:15

Security

Power button instantly locks □

Owner info

ENCRYPTION

Encrypt phone
Encrypted

SIM CARD LOCK

Set up SIM card lock

PASSWORDS

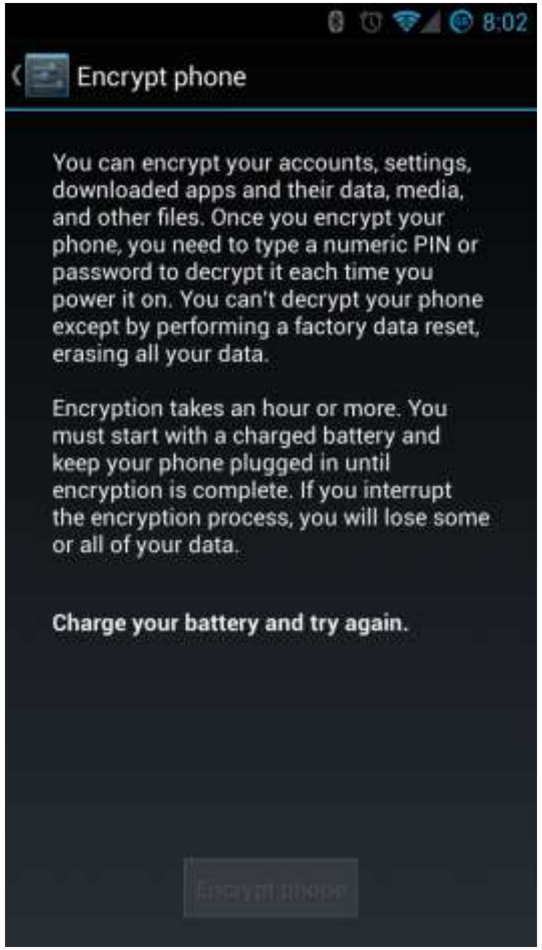
Make passwords visible ☑

DEVICE ADMINISTRATION

Device administrators
View or deactivate device administrators

Unknown sources □
Allow installation of apps from unknown

Android Device Security



Encrypt phone

You can encrypt your accounts, settings, downloaded apps and their data, media, and other files. Once you encrypt your phone, you need to type a numeric PIN or password to decrypt it each time you power it on. You can't decrypt your phone except by performing a factory data reset, erasing all your data.

Encryption takes an hour or more. You must start with a charged battery and keep your phone plugged in until encryption is complete. If you interrupt the encryption process, you will lose some or all of your data.

Charge your battery and try again.

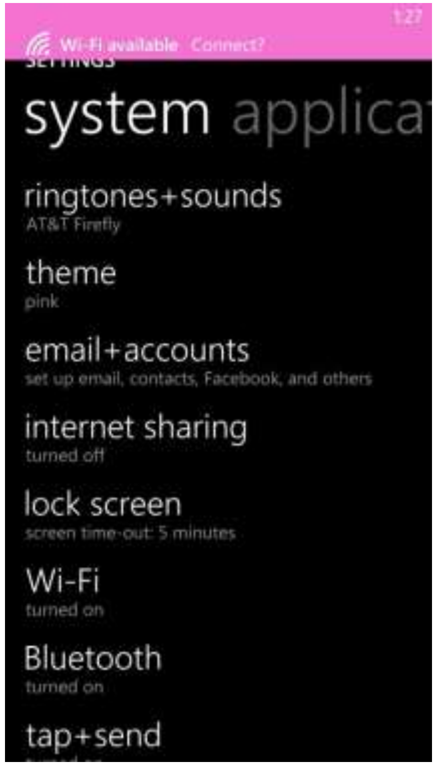
WINDOWS PHONE SECURITY

APPENDIX C

UW Medicine

DEPARTMENT OF MEDICINE

Windows Phone 7/8 Security



1:27

Wi-Fi available Connect?

SETTINGS

system applica

ringtones+sounds
AT&T Firefly

theme
pink

email+accounts
set up email, contacts, Facebook, and others

internet sharing
turned off

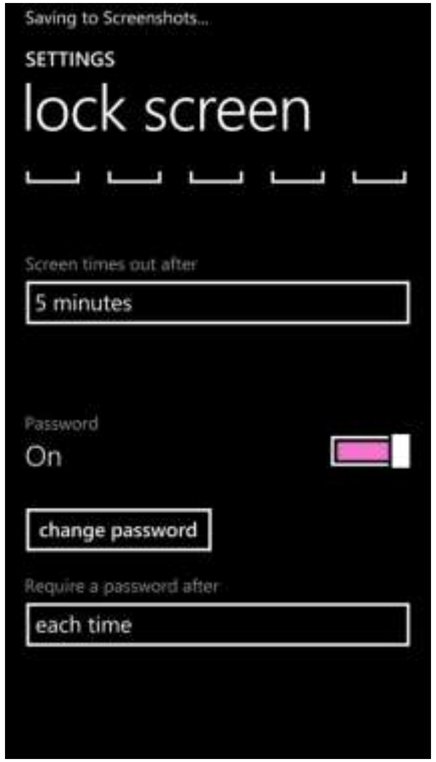
lock screen
screen time-out: 5 minutes

Wi-Fi
turned on

Bluetooth
turned on

tap+send

Windows Phone 7/8 Security



Saving to Screenshots...

SETTINGS

lock screen

Screen times out after

5 minutes

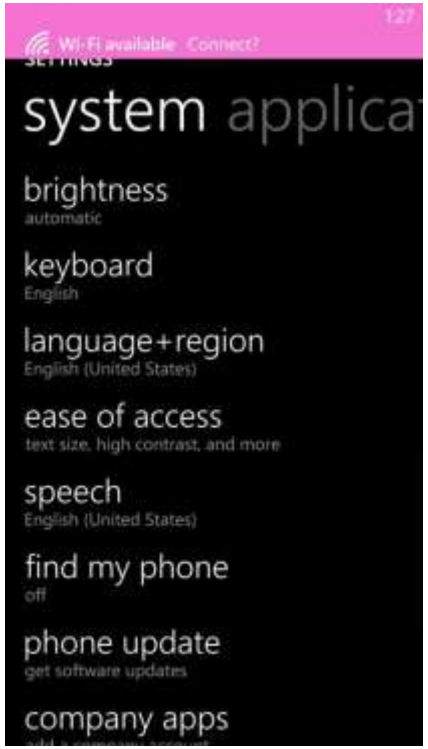
Password

On

Require a password after

each time

Windows Phone 7/8 Security



127

Wi-Fi available Connect?

SETTINGS

system applicat

brightness
automatic

keyboard
English

language+region
English (United States)

ease of access
text size, high contrast, and more

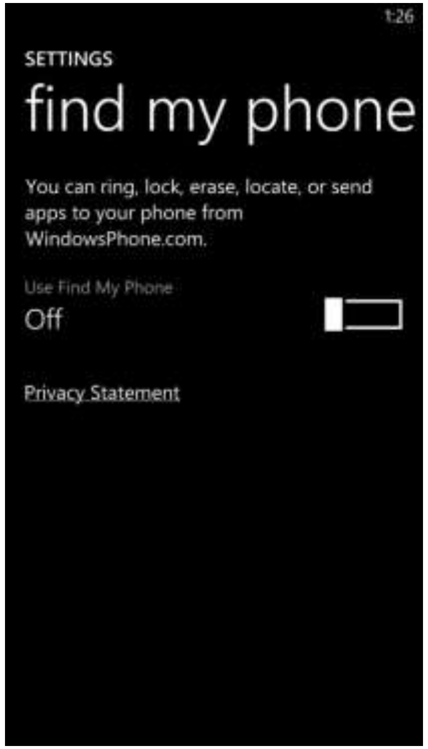
speech
English (United States)

find my phone
off

phone update
get software updates

company apps
add a company account

Windows Phone 7/8 Security



1:26

SETTINGS

find my phone

You can ring, lock, erase, locate, or send apps to your phone from WindowsPhone.com.

Use Find My Phone

Off

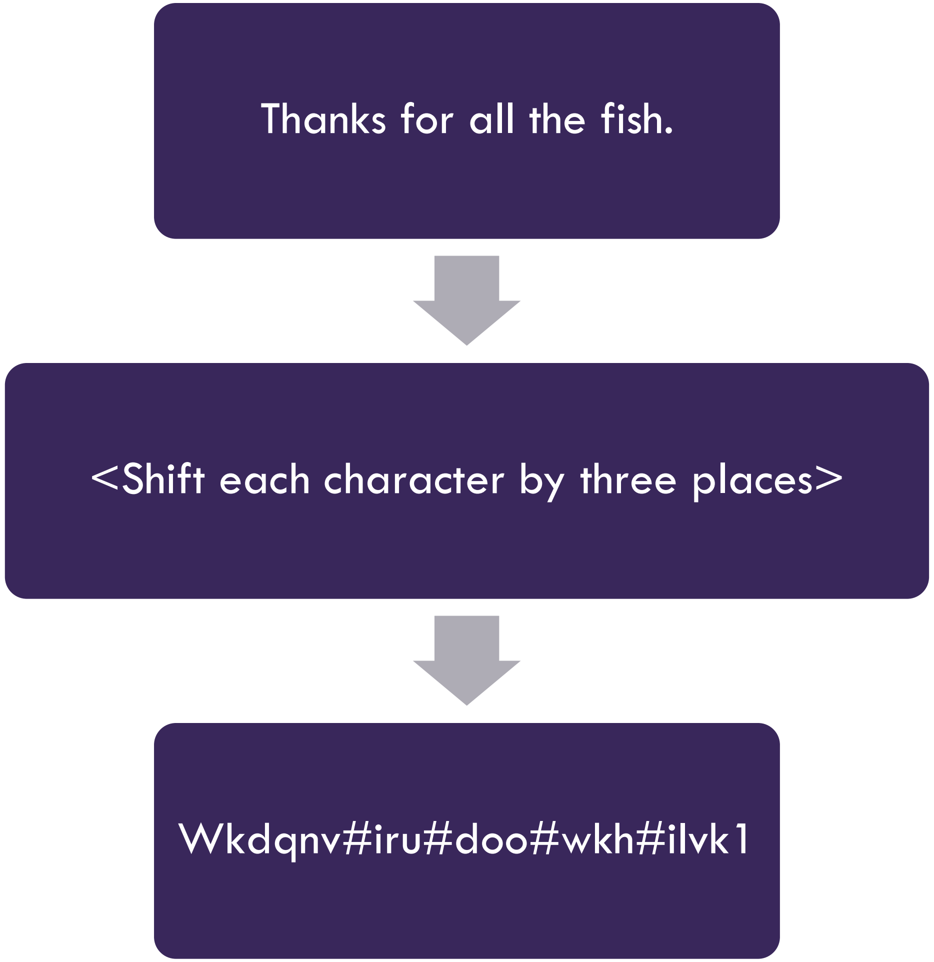
Privacy Statement

SUPPLEMENTAL INFORMATION

APPENDIX D

Simple Encryption Example

- Encryption is the process of encoding data so that only privileged parties can decrypt (decode) it.
- Data is "scrambled" so that it is unreadable.
- Only the key used to encrypt the data can be used to decrypt ("unscramble") it to make it usable again.
  - Recovery of encrypted data without the key is realistically impossible.



Thanks for all the fish.

<Shift each character by three places>

Wkdqnv#iru#doo#wkh#ilvk1

Extended Password Complexity

- Use the full keyboard
  - All lowercase passwords: 26 possibilities per character.
  - Mixed-case passwords: 52 possibilities per character.
  - Full-keyboard passwords: 95 possibilities per character.

The Virtue of Long Passwords

- 6 Characters – 735 billion possible combinations
  - Approximately 1 hour to crack
- 7 Characters – 70 trillion possible combinations
  - Approximately 4 days to crack
- 8 Characters – 6.6 quadrillion possible combinations
  - Approximately 382 days to crack
- 12 Characters – 540 sextillion possible combinations
  - Approximately 85.7 million years to crack

All figures based on brute-force methods using the 95 common characters of the ASCII set. Times assume rough figures for readily-available end-user hardware.

Basics of Viruses

- Viruses are pieces of malicious software that run (usually) unnoticed on a computer.
- They can allow remote attackers to log keystrokes, view your screen, and/or take over your keyboard and mouse.
- They can allow attackers to use your computer in distributed online attacks.
- Use antivirus software on all of your computers.
  - Many antivirus products are available for free.
    - Windows: Microsoft Security Essentials, Sophos, AVG, Avast!
    - Mac: Sophos (available through the University)