

# Keeping Data Safe

Patients, Research Subjects, and You

# How do hackers access a system

## *Hackers Lurking in Vents and Soda Machines*

By NICOLE PERLROTH APRIL 7, 2014 **New York Times**

SAN FRANCISCO — They came in through the Chinese takeout menu.

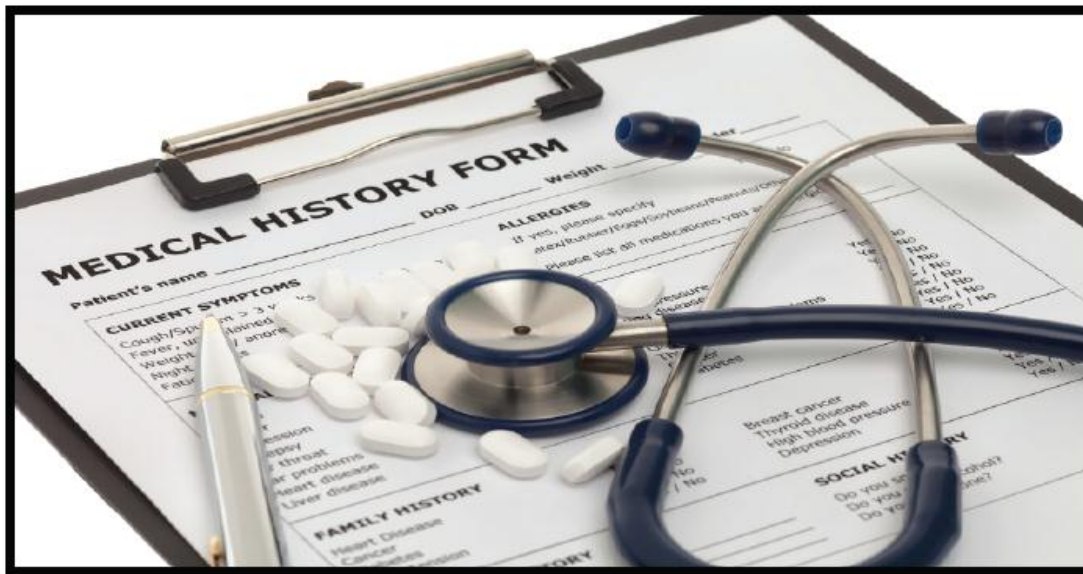
# Data Breaches in Medical/Research

- A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.
- Identifiable patient/research subject information
- HIPAA identifiers

# 18 HIPAA Identifiers

HIPAA PHI “Identifiers”	
<ul style="list-style-type: none"><li>• Names</li><li>• Geographic data (other than first 3 digits of zip code)</li><li>• All elements of dates (other than the year)</li><li>• Telephone numbers</li><li>• FAX numbers</li><li>• Email addresses</li><li>• Social Security numbers</li><li>• Medical record numbers</li><li>• Health plan beneficiary numbers</li><li>• Account numbers</li></ul>	<ul style="list-style-type: none"><li>• Certificate/license numbers</li><li>• Vehicle identifiers and serial numbers including license plates</li><li>• Device identifiers and serial numbers</li><li>• Web URLs</li><li>• Internet protocol (IP) addresses</li><li>• Biometric identifiers (i.e. retinal scan, fingerprints)</li><li>• Full face photos and comparable images</li><li>• Any unique identifying number, characteristic or code</li></ul>

# 2014 Survey of 91 Healthcare Organizations



## Fourth Annual Benchmark Study on Patient Privacy & Data Security

---

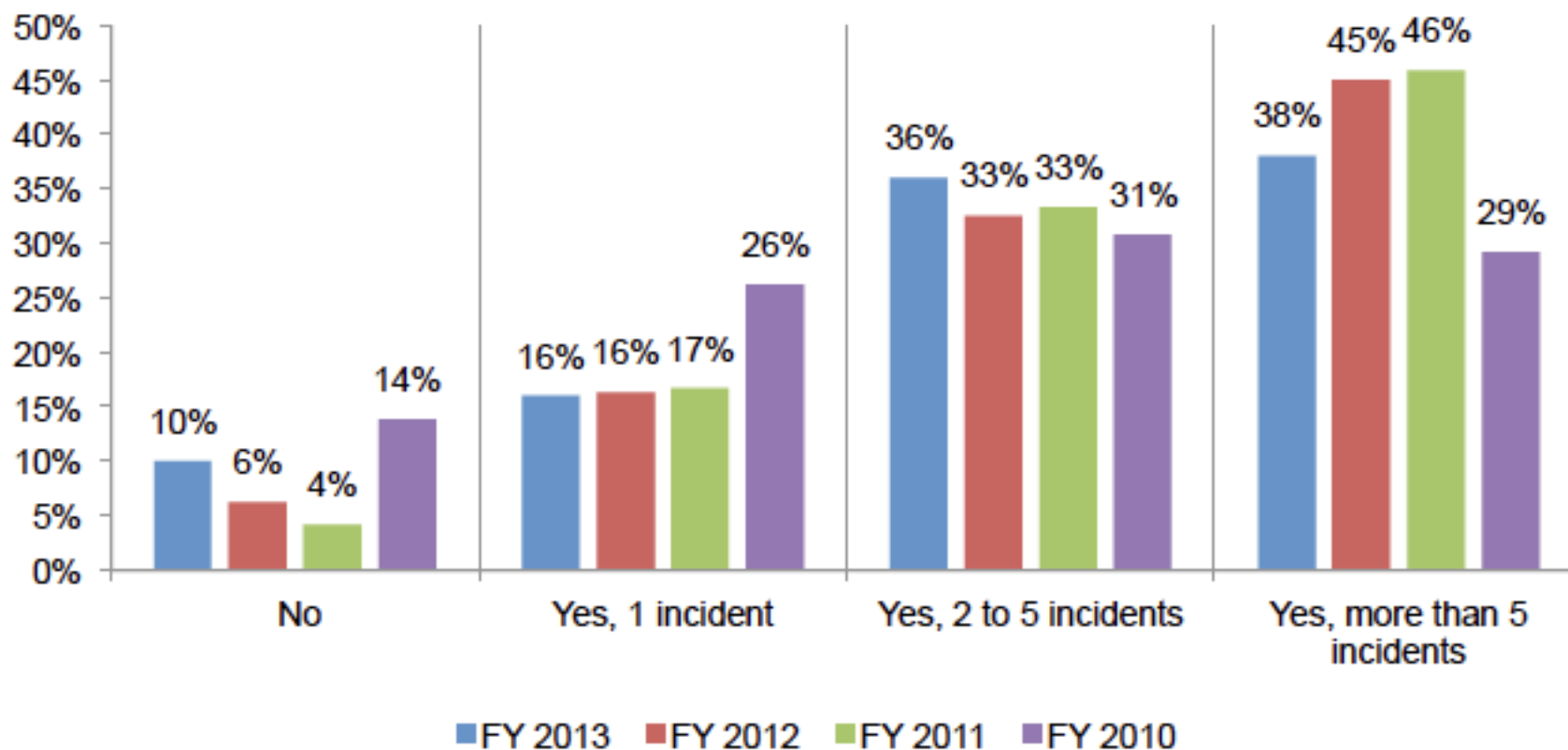
**Sponsored by ID Experts**

Independently conducted by Ponemon Institute LLC

Publication Date: March 2014

# Data Breaches Are Common

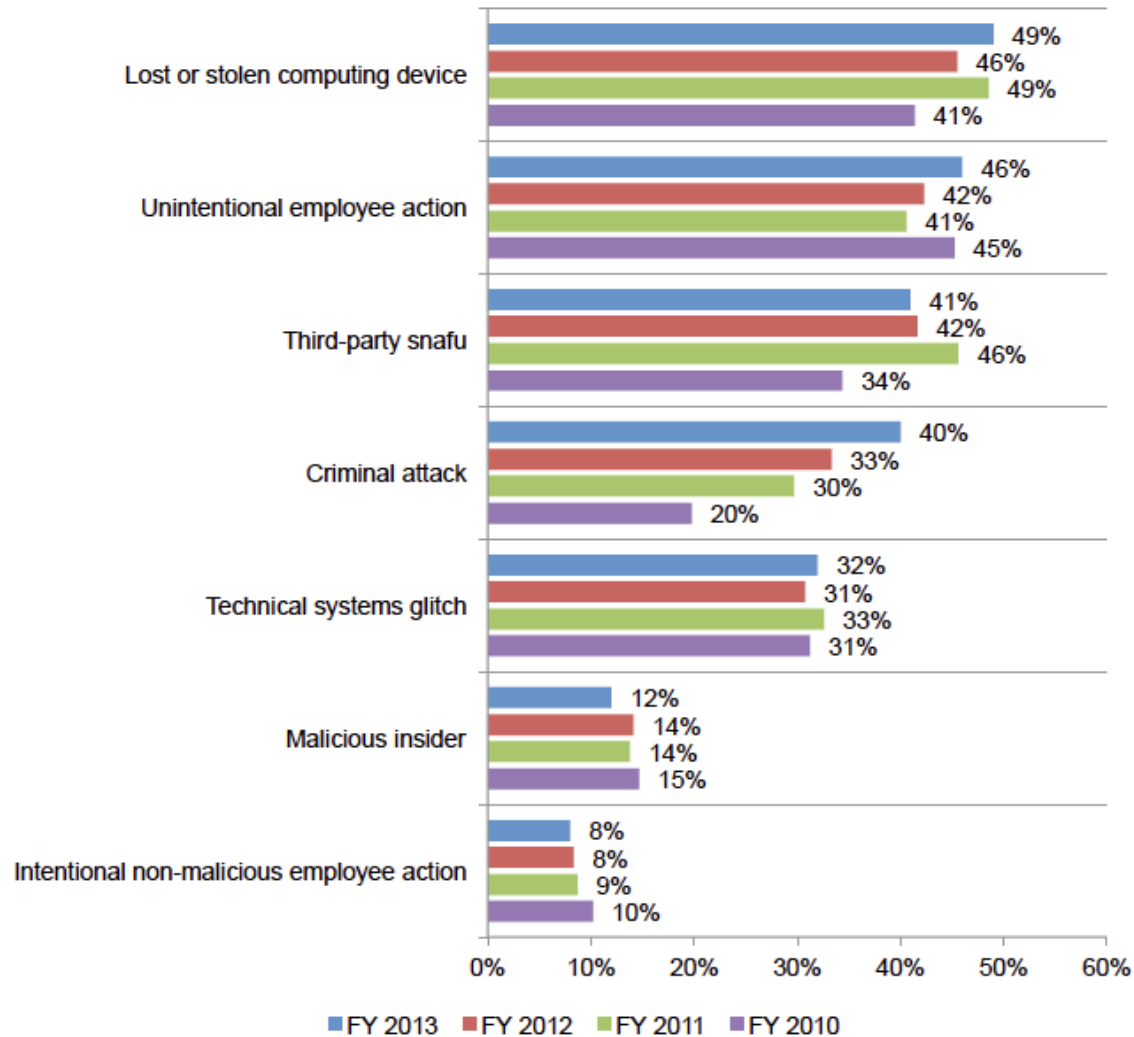
**Figure 1. Experienced a data breach involving the loss of patient data in the past two years**



## Where Are the Leaks?

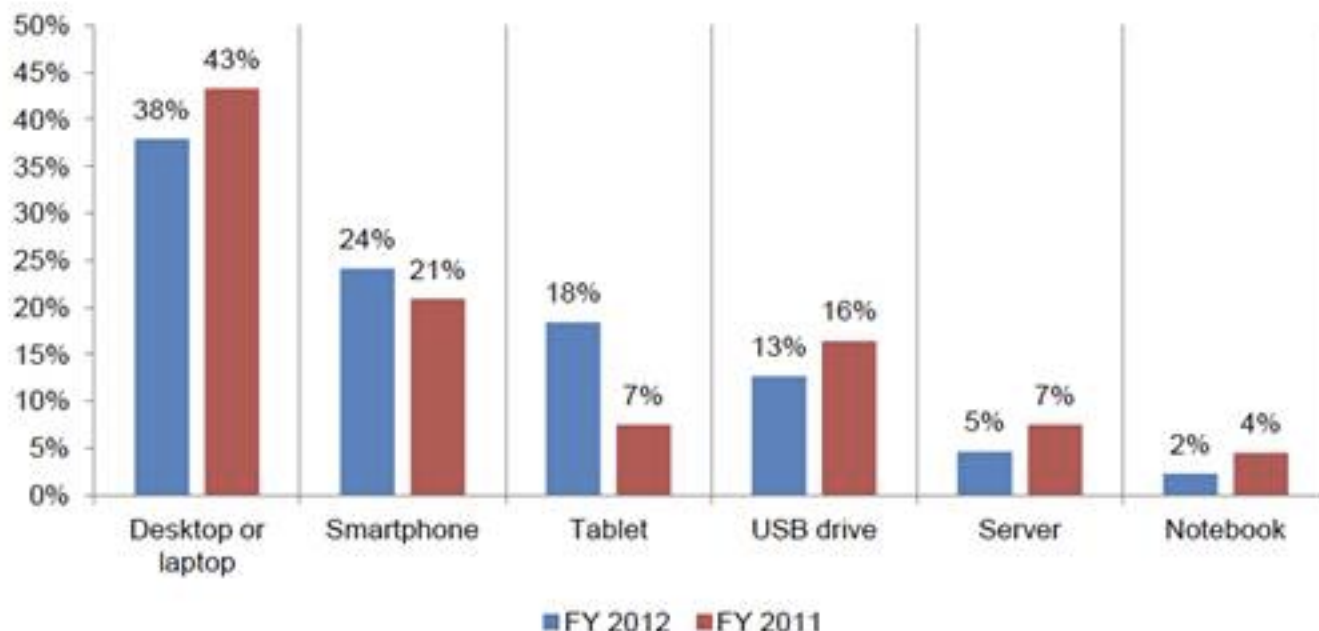
**Figure 8. Nature of the incident**

More than one choice permitted



# Types of Lost “Devices”

**Figure 2. Types of devices that have been lost or stolen and compromised confidentiality of PHI.**



From **Third Annual Benchmark Study on Patient Privacy & Data Security**. Ponemon Institute, LLC. [www2.idexpertsCorp.com/ponemon2012/](http://www2.idexpertsCorp.com/ponemon2012/)



# Data security is a real issue here at BUMC too

- Missing hard drives after room cleaning at BMC
- Stolen student laptop / usb drive
- Phishing compromise of email account with patient data in it
- Phishing theft of pay checks

# What Can You Do to Avoid PHI Loss

- If you don't need it, don't collect it.
- Remove HIPAA identifiers

HIPAA PHI “Identifiers”	
<ul style="list-style-type: none"><li>• Names</li><li>• Geographic data (other than first 3 digits of zip code)</li><li>• All elements of dates (other than the year)</li><li>• Telephone numbers</li><li>• FAX numbers</li><li>• Email addresses</li><li>• Social Security numbers</li><li>• Medical record numbers</li><li>• Health plan beneficiary numbers</li><li>• Account numbers</li></ul>	<ul style="list-style-type: none"><li>• Certificate/license numbers</li><li>• Vehicle identifiers and serial numbers including license plates</li><li>• Device identifiers and serial numbers</li><li>• Web URLs</li><li>• Internet protocol (IP) addresses</li><li>• Biometric identifiers (i.e. retinal scan, fingerprints)</li><li>• Full face photos and comparable images</li><li>• Any unique identifying number, characteristic or code</li></ul>

# Is Your Research Team Compliant?

- Assure that everyone who has access to PHI knows and complies with security standards (e.g., from your boss to the students and trainees)
- Assure that everyone who accesses PHI does so on a secure device (e.g., are your students' laptops secure?)

# Seek first to understand

- Know what you have; know the requirements
- BU/BUMC
  - The BU Data Protection Standards
    - Classifications: Public, Internal, Confidential, Restricted Use
    - <http://www.bu.edu/infosec/policies/data-protection-standards/>
  - The BU Minimum Security Standards
    - <http://www.bu.edu/tech/about/policies/info-security/1-2-e-minimum-security-standards/>
- BMC
  - Section 40 on the BMC Policy & Procedure website:
    - <http://internal.bmc.org/policy/>

# Store sensitive information securely


- Secure Network Storage
  - Security, access monitoring, backups, archival
- Special purpose applications
  - Redcap, eClinica
- Encryption on your laptop, phone/tablet, USB, CD/DVD
  - Enterprise (SecureDoc, McAfee)
  - Personal (Bitlocker, FileVault)
- Sensitive information and personal phones/devices
  - Recommendation vs. prohibition
- Avoid shadow systems

# Transmit sensitive information securely

- Limits of regular email
- Secure email
  - BU SecureMail
    - <http://www.bu.edu/tech/comm/email/datamotion/>
  - Secure email and file transfer from BMC
- A word about cloud storage



# Secure your devices

1. Don't "jailbreak" or "root" your phone
  - Don't run your computer as "Administrator"
2. Pick a strong password  require it at startup
3. Have your device automatically lock when inactive
4. Encrypt your device
5. Set up your system to receive updates automatically
6. Install a trusted Anti-Malware package
7. Have your data backed up regularly
8. Connect securely using VPN when on public wi-fi



# Free software and services from BU

- SecureDoc

- Enterprise encryption for Windows and Mac



- SecureMail

- <http://www.bu.edu/tech/comm/email/datamotion/>



- McAfee

- <http://www.bu.edu/tech/support/desktop/removal/security/mcafee/>



- CrashPlan

- <http://www.bu.edu/tech/support/desktop/crashplan/>



# Free software and services from BMC

- Secure email
  - McAfee anti-malware and encryption
  - Secure file transfer
  - Secure remote access
- 
- Contact the BMC IT Service Desk at 617-414-4500

The background is a solid dark blue. It features a large, faint, light blue circle in the center. Overlaid on this are several sets of concentric, thin, light blue circles that form a wavy, ripple-like pattern across the slide.

Q: How do bad guys usually  
get around security

A: They ask you to do it



Dear BU Employee,

Our new intrusion monitoring system that checkmates the increased incidents of phishing attacks and database compromise detected that your "BU" account was accessed from a blacklisted IP located in Arizona. Here are the details:

IP:	23.19.88.141
Registered to:	Nobis Technology Group, LLC. Phoenix, Arizona
Time of compromise:	8:17 AM, Eastern Standard Time (EST) -0500 UTC
Date of compromise:	Saturday, November 30, 2013

Did you access your account from this location? If this wasn't you, your computer might have been infected by malicious software. To protect your account from any further compromise, kindly follow these two steps immediately:

1. Follow this ITS secure link below to reconfirm your login details and allow the new IP monitoring alert system automatically block the suspicious IP (23.19.88.141) from further future compromise

<http://netid-bu.edu/blockIP&malware>


2. Update your anti-malware software and scan your PC immediately

With these two steps taken, your account will be secured.

Serving you better,  
ITS and Database Security, Boston University

BU Boston University | Web Login

← → ↻

 Web Login

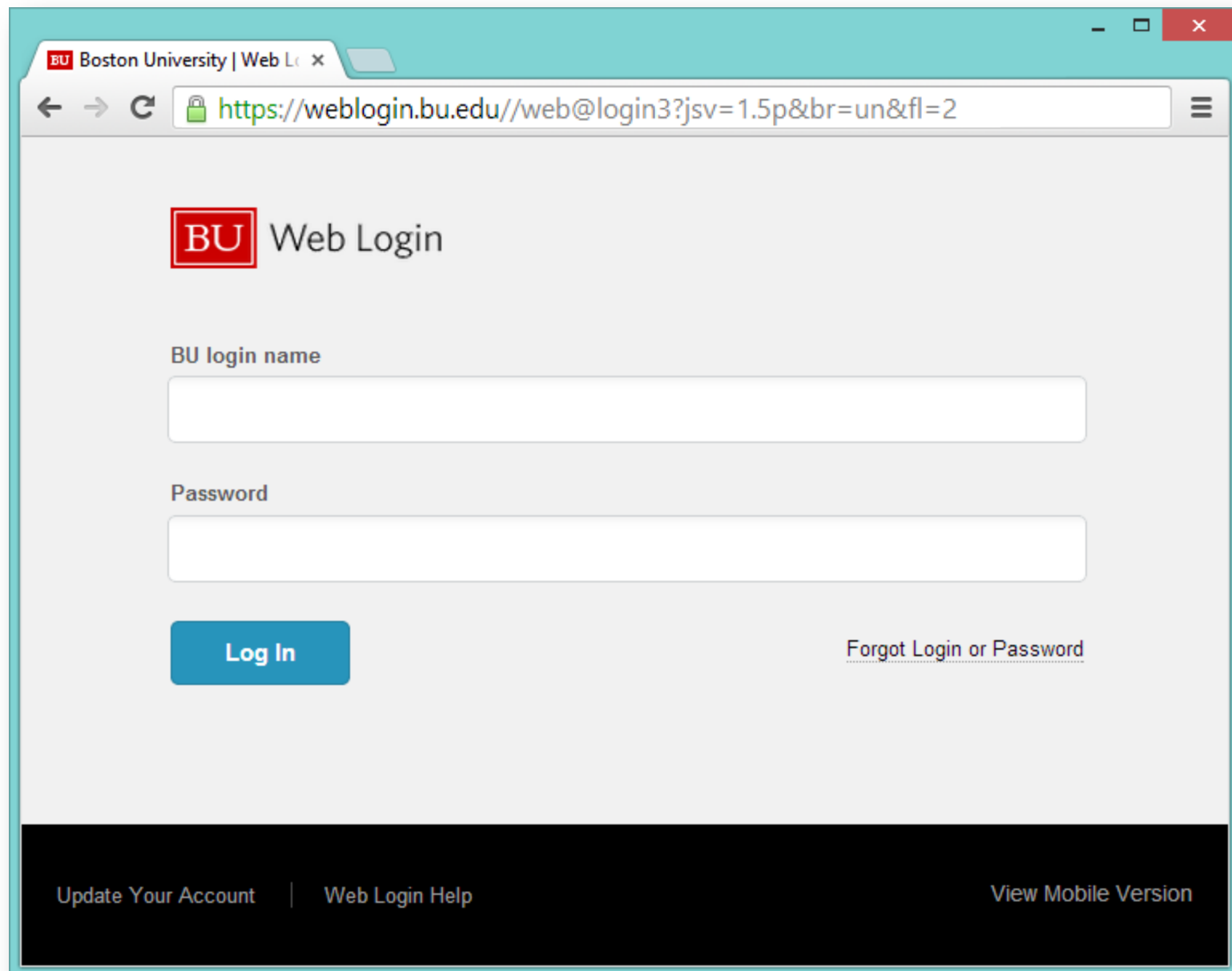
BU login name

Password

[Log In](#)

[Forgot Login or Password](#)

[Update Your Account](#) | [Web Login Help](#) [View Mobile Version](#)



The image shows a web browser window with a teal header bar. The browser's address bar displays the URL <https://weblogin.bu.edu/web@login3?jsv=1.5p&br=un&fl=2>. The page content features the Boston University logo (a red square with 'BU' in white) followed by the text 'Web Login'. Below this, there are two input fields: 'BU login name' and 'Password'. A blue 'Log In' button is positioned to the left of a link that reads 'Forgot Login or Password'. At the bottom of the page, a black footer bar contains three links: 'Update Your Account', 'Web Login Help', and 'View Mobile Version'.

BU Boston University | Web Login

BU login name

Password

Log In

[Forgot Login or Password](#)

[Update Your Account](#) | [Web Login Help](#) [View Mobile Version](#)

**Not Encrypted: no https**

**Not going to the real .bu.edu**

Dark part of link is the  
real web server: "Msprotect-bu.edu"

The image shows a web browser window with a single tab titled "Boston University | Web Login". The address bar displays the URL "http://Msprotect-bu.edu/BUphishaler...". The page content includes a red "BU" logo followed by the text "Web Login". Below this, there are two input fields labeled "BU login name" and "Password". A blue "Log In" button is positioned below the password field. To the right of the button is a link that reads "Forgot Login or Password". At the bottom of the page, there is a dark footer bar containing three links: "Update Your Account", "Web Login Help", and "View Mobile Version".

Annotations on the screenshot:

- A green arrow points from the text "Not Encrypted: no https" to the "http" portion of the address bar.
- A black arrow points from the text "Dark part of link is the real web server: 'Msprotect-bu.edu'" to the "Msprotect-bu.edu" portion of the address bar.

The top part is controlled by your computer and the server

The image shows a web browser window with a green border. The address bar shows the URL `https://weblogin.bu.edu/web@login3?jsv=1.5p&br=un&fl=2`. The page content is a login form with a red border. The form includes the BU logo, the text "Web Login", a "BU login name" label, a text input field, a "Password" label, another text input field, a blue "Log In" button, and a link "Forgot Login or Password".

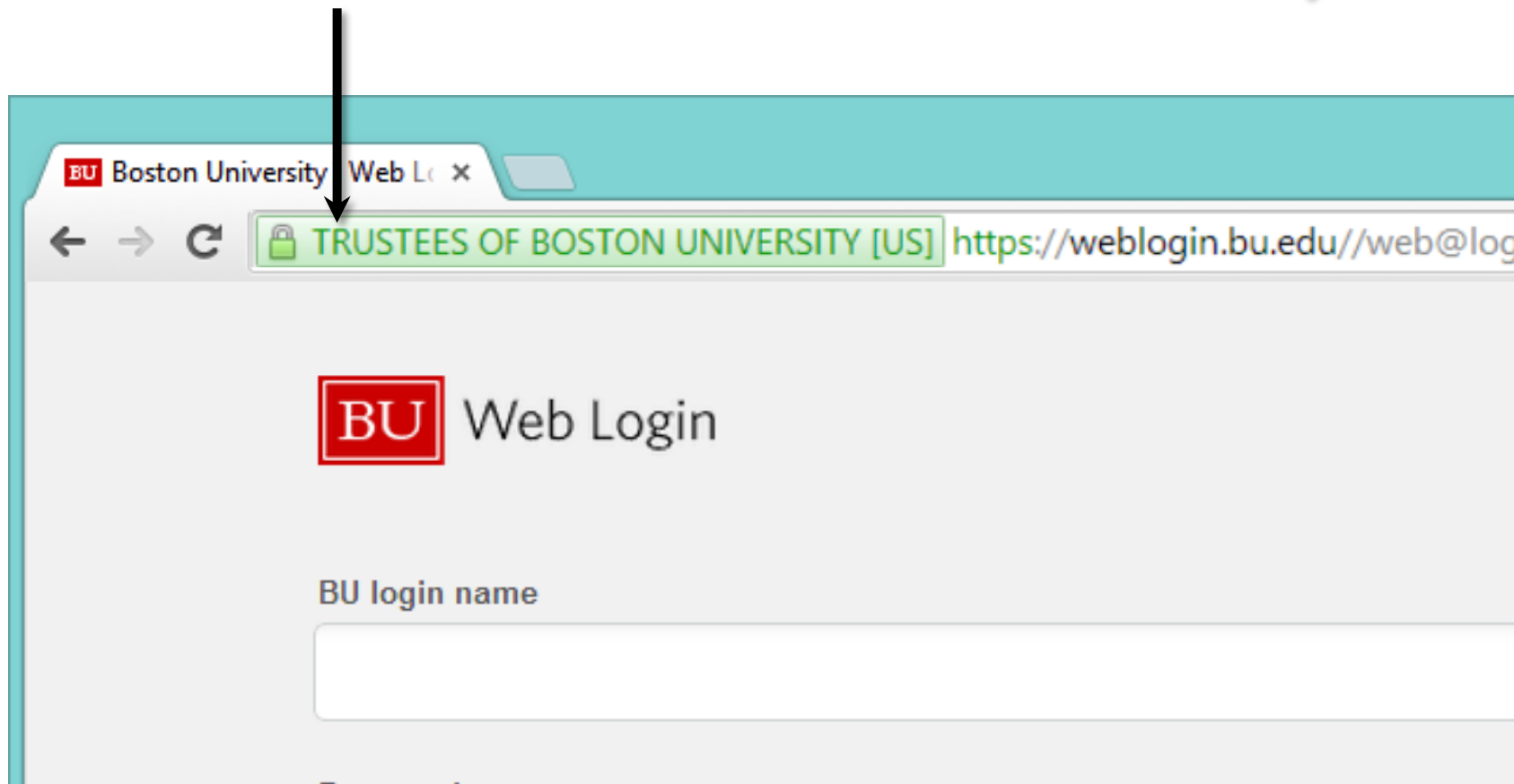
The display window is completely controlled by the page author



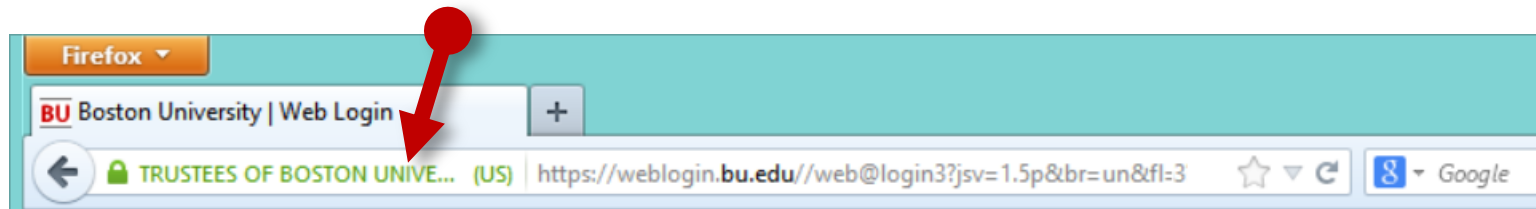
# What the *new* weblogin looks like

Special Certificate  
shown in Green:

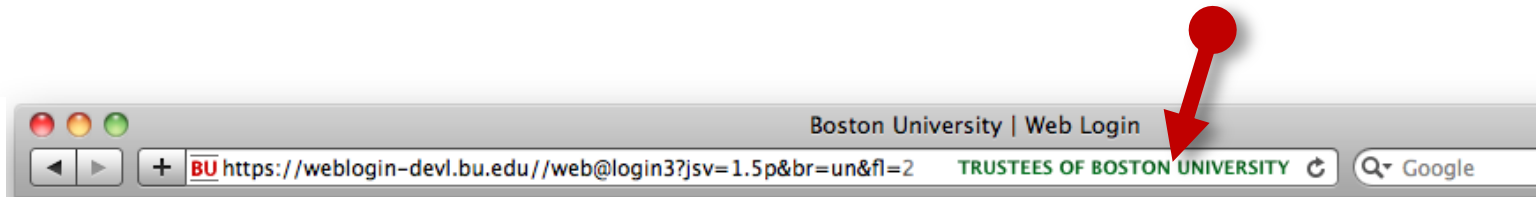
Trustees of Boston University



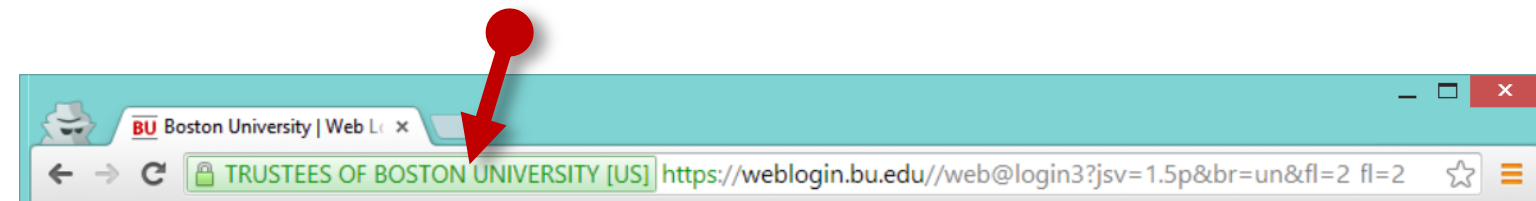
## Firefox



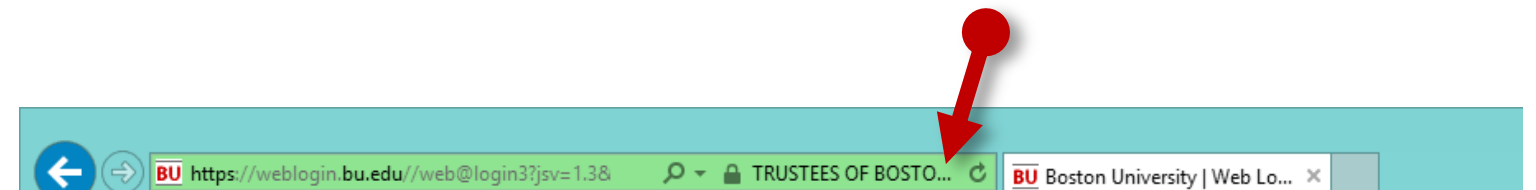
## Safari



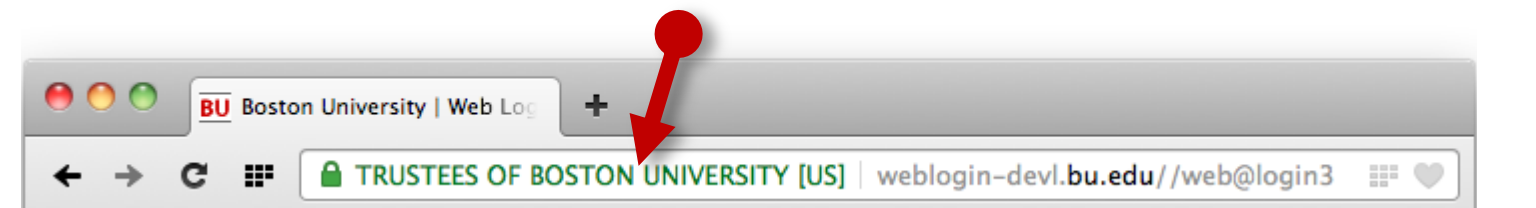
## Chrome



## Internet Explorer

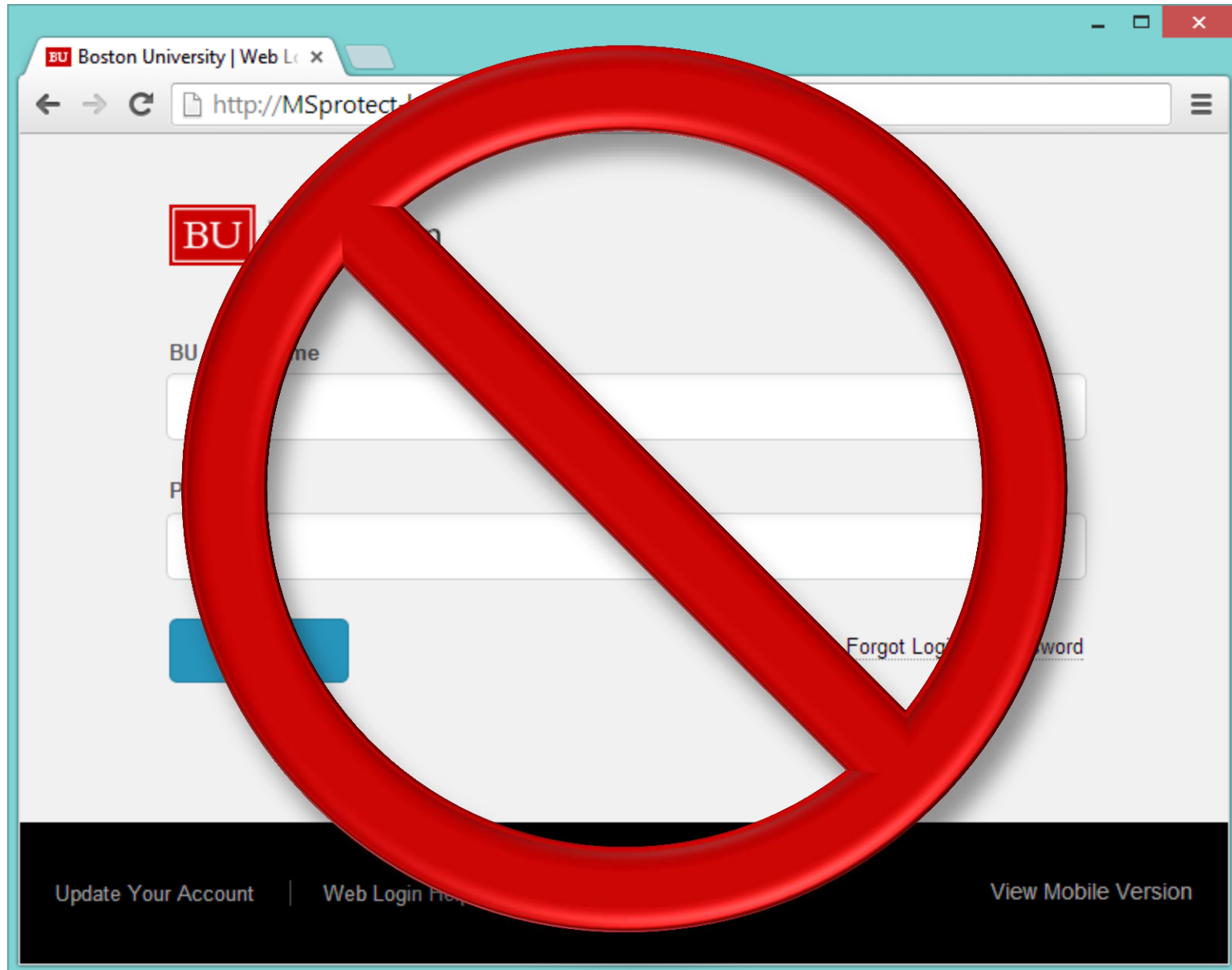


## Opera





No Green, No Go

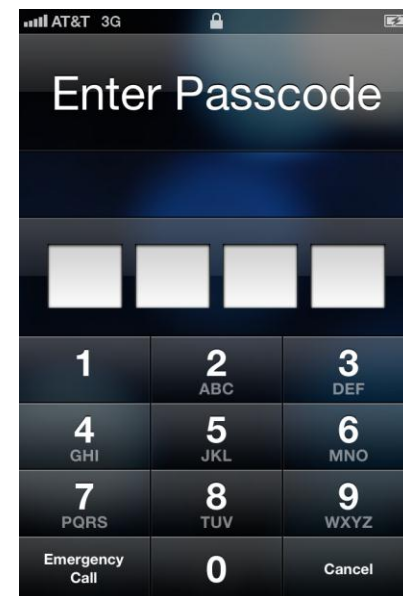
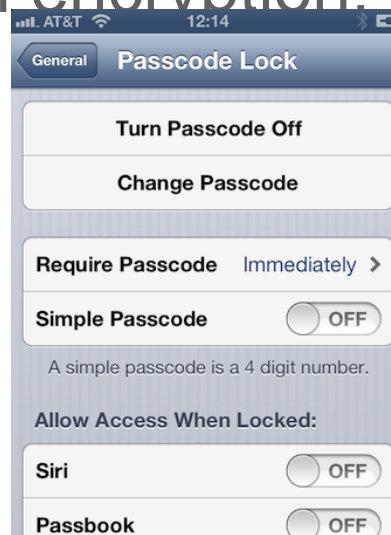
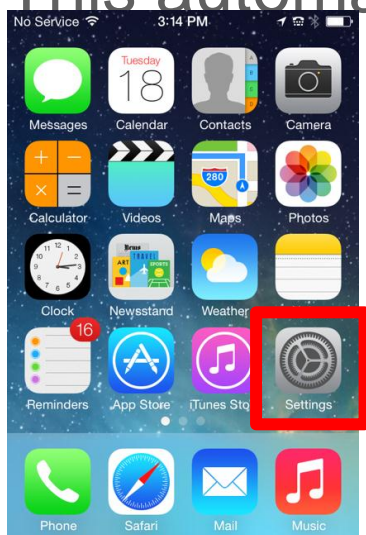


The background is a solid dark blue. It features several thin, light blue wavy lines that sweep across the frame from the top left towards the bottom right. A large, semi-transparent light blue circle is positioned in the center-left area, partially behind the text.

# Setting up Security on your phone and laptop

# Setting a passcode on an iPhone

- Go to **Settings**
- Choose **General > Passcode** (or Touch ID & Passcode)
- Enter a passcode (4-digit or better)
- This automatically turns on encryption!





# Setting a passcode on an iPad

- Go to **Settings**
- Choose **General > Passcode**
- Enter a passcode (4-digit or better)
- This automatically turns on encryption!

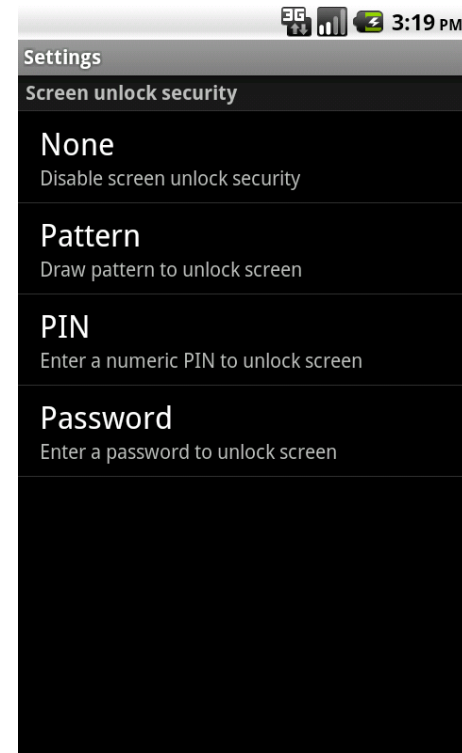
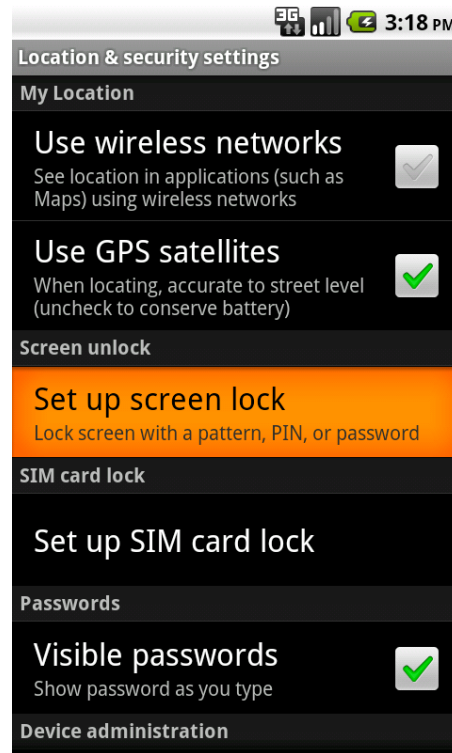
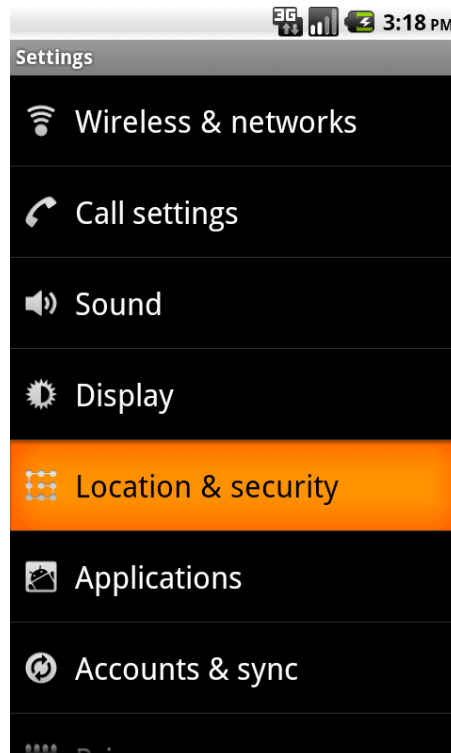
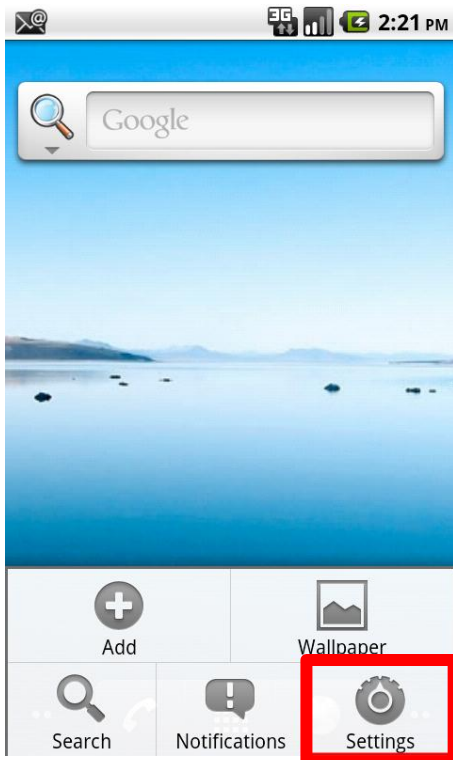


# Setting a passcode on an Android

- From your home screen, click the **Menu** button, then **Settings**
- Scroll down. Click **Location & Security**
- Scroll down. Under the heading **Screen Unlock**, select **Set Up Screen Lock**.
- Select which type of password you would like to use:
  - None - Disables any previously set screen unlock security.
  - Pattern - Sets an unlock screen which requires the user to draw a specific pattern between 9 on-screen points.
  - PIN - Sets an unlock screen requiring the user to enter a numeric code.
  - Password - Sets an unlock screen that requires entering an alphanumeric password (numbers, letters, and symbols).

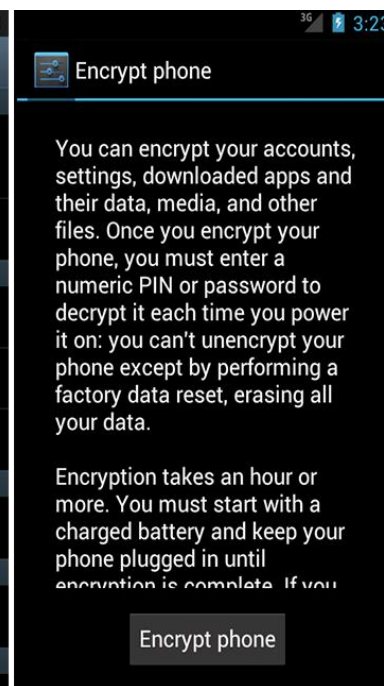
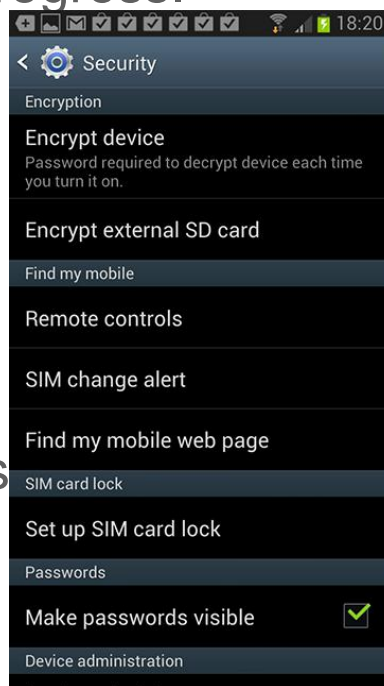


# Setting a passcode on an Android



# Setting encryption on an Android

- **Backup your device**
- Note: Pattern will not work. Set a PIN or password
- Plug your phone in to the charger, do not disconnect or disrupt encryption while in progress.
- Go to **Menu**
  - > **Settings**
  - > **Security**
- Select **Encrypt Phone** or **Encrypt Tablet**
- Read the instructions and notes and begin



# Encryption on your Laptop

- For institutionally-owned machines, Use enterprise encryption solutions
  - Encryption key backup
  - Enables easy support by IT
- Contact your Information Security department.
  - BU: Brian Gerdon – [gerd@bu.edu](mailto:gerd@bu.edu)
  - BMC: Contact the BMC IT Service Desk at 617-414-4500

# Encrypting your personal Laptop

- ***In all cases:***
  - Before you begin, back up your data
  - You will need admin privileges
  - Copy your decryption recovery key somewhere else
  - Performance during the initial encryption will be slower, performance after this is complete will be back to normal
- Windows 7 “Bitlocker”
- Windows 8
  - “Device Encryption” (automatic for supported systems)
  - “Bitlocker” otherwise
- Mac “FileVault2”
- Truecrypt for encryption of files, folders or “containers”

# Windows 7 “Bitlocker”

- Read this page and follow the instructions:
  - [http://technet.microsoft.com/en-us/library/dd835565\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd835565(v=ws.10).aspx)
  - [http://technet.microsoft.com/en-us/library/ee424299\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/ee424299(v=ws.10).aspx)
- Overview of the steps
  1. Click **Start**, click **Control Panel**, click **System and Security**, and then click **BitLocker Drive Encryption**.
  2. Click **Turn On BitLocker** for the operating system drive.
  3. BitLocker setup wizard prompts you to choose how to store the recovery key. It is *crucial* that you back this up somewhere other than the computer you are encrypting.
  4. The BitLocker setup wizard asks if you are ready to encrypt the drive. Confirm that the **Run BitLocker system check** check box is selected, and then click **Continue**.
  5. Confirm that you want to restart the computer by clicking **Restart now**.
  6. If it is ready for encryption, the **Encrypting** status bar is displayed, which shows the progress of the drive encryption.

# Windows 8 “Device Encryption”

- Read this page and follow the instructions:
  - <http://windows.microsoft.com/en-us/windows-8/using-device-encryption>
- Overview of the steps
  1. If you have performed a clean install of Windows 8.1, device encryption is turned on by default. If you have upgraded a previous Windows installation to Windows 8.1, you can turn device encryption on by using **PC info**.
  2. To open **PC info**, swipe in from the right edge of the screen, tap **Settings**, and then tap **Change PC settings**. (If you're using a mouse, point to the upper-right corner of the screen, move the mouse pointer down, click **Settings**, and then click **Change PC settings**.)
  3. Tap or click **PC & devices**, and then tap or click **PC info**. The **Device Encryption** section appears at the bottom of the **PC info** page.
  4. In the **Device Encryption** section, select **Turn On**.
  5. Device encryption cannot be turned off on devices running Windows RT. For other devices, in the **Device Encryption** settings portion of **PC info**, you can select **Turn Off** if you want to stop using device encryption for any reason.

# Windows 8 “Bitlocker”

- Read this page and follow the instructions:
  - <http://windows.microsoft.com/en-us/windows-8/bitlocker-drive-encryption>
- Overview of the steps
  1. Go to the **Start Screen** and type “BitLocker”, in the Settings search result, click on **Manage BitLocker**
  2. (or go to **Control Panel > All Control Panel Items > BitLocker Drive Encryption**)
  3. Click on the drive or partition where you store your personal files and folders and then click on **Turn BitLocker on**.
  4. Choose **Use a password to unlock the drive**, the longer the phrase you use, the better.
  5. This is *crucial*: Store a copy of your recovery key in case you forget or lose your BitLocker encryption password. Print it out or store it on a USB key or network drive, not the system you are encrypting Don't forget where it is!
  6. Once you've saved your recovery key you can choose to encrypt just the used space or the entire drive. If it's a brand new never been used before laptop then select the **Encrypt used disk space option**, for a PC that's been in use choose **Encrypt entire drive**. Click on **Start encrypting** to protect your files.

# Mac “FileVault”

- Read this page and follow the instructions:
  - <http://support.apple.com/kb/ht4790>
- Overview of the steps
  1. Go to **System Preferences > Security & Privacy > FileVault**
  2. Choose which accounts you will enable to log into the protected system
  3. This is crucial: When shown a copy of your recovery key, print it out or store it on a USB key, on a network drive or with Apple, do not store it on the system you are encrypting. Don't forget where it is!
  4. Complete turning on FileVault.
  5. Follow the prompts to restart your machine.
  6. Log in to unlock the disk and begin the one-time encryption process



[www.bu.edu/infosec](http://www.bu.edu/infosec)