Security Tips

Introduction

It's too bad that we have to resort to some of the steps outlined below but in today's world we can't take too many precautions. You can choose to take all or none of these steps but at least you know about them.

Here's what I've done recently:
- Purchased a Yubikey for 2-Step verification with LastPass
- Switched, finally, to credit cards that are chip enabled
- Checked my Gmail alternate contact methods
- Turned on 2-Step verification with our Gmail accounts
- Enabled fingerprint access for mobile devices (not unbreakable but better than nothing)
- Turned off Simple Passcode in iPad and iPhone to allow longer passwords including characters
- Reviewed a Credit Report from Experian (does not include FICO Score)
- Check your password strength at https://www.grc.com/haystack.htm
- Placed all of my passwords on a flash drive and put it in a secure location (safe or safety deposit box or store it offsite). You can export from Lastpass but not from RoboForm. From RoboForm, click Logins, Print List.
- Updated my software with PatchMyPc
- I'm thinking about MFA with Amazon (Multi Factor Authentication – can use mobile phone)

This is no guarantee that I'm totally save but I'm at least better off.

Finally – I'm not trying to represent myself as a security expert but merely attempting to provide the information resulting from my several hours of research and many more hours of experience.

Gmail

2-Step Verification

Under Signing in you can enable 2-Step Verification by click on it as shown below.

Your first screen will look like the one below. Click Start setup.

The next screen will ask you to send a code to your cell phone. Just click Send code.

The next screen will ask you to confirm.

The next screen will ask you to Reconnect your mobile apps which you can choose to do later.
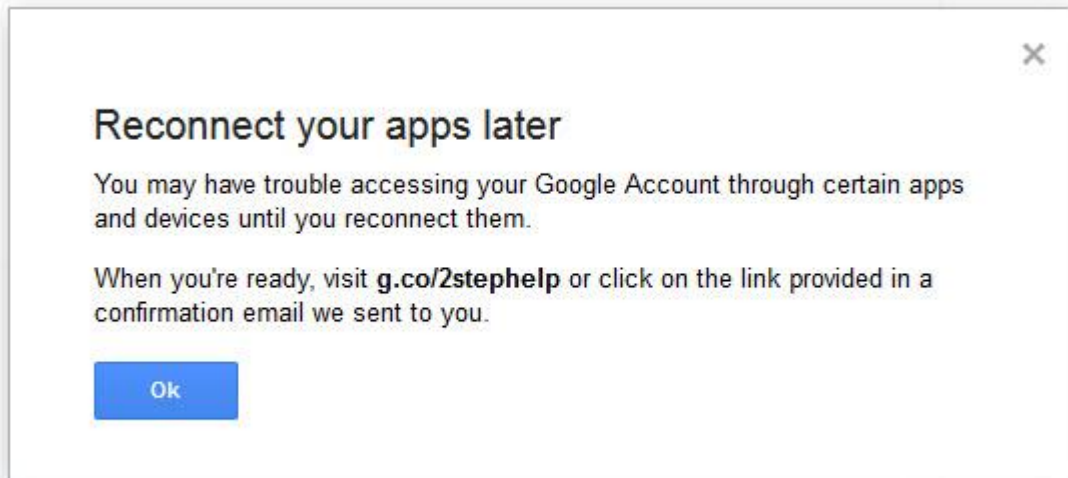
Somewhere along the line you will be given the choice to trust the PC that you are working on. This means that codes will not be required for your desktop PC or laptop.

Security check

Check your security at security.google.com or myaccount.google.com. If you are not logged in you will be given the opportunity to do so.

From here you have several options but the main one is Security check up. Click Get Started and log in once more and start your way down through the various settings, you can't skip around
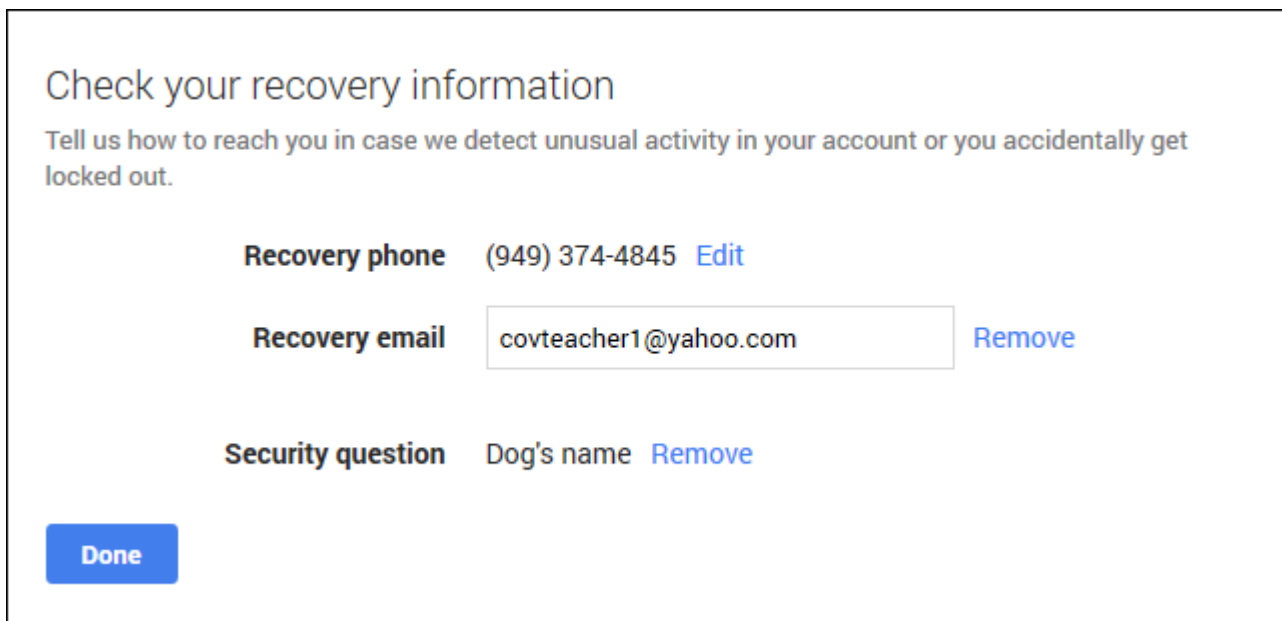
Check your 2-Step Verification settings

Please make sure that all your 2-Step Verification settings are up to date. Learn more.

Verify by

Text message to (949) 374-4845

Backup options	Added on	Details
Backup phone	Dec 22	(949) 305-2962
Backup codes	Dec 22	10 codes left

You can see that I've enabled 2-Step verification which I recommend. Here are some tips:

- You must have a cell phone or land line listed where the codes will be sent
- You can also list a secondary email address
- You can identify your desktop PC or laptop as safe devices and 2-Step Verification will not be required
- For mobile devices you will need to visit the App0specific passwords tab and click Mamage application-specific passwords to generate passwords for these devices.


2-Step Verification

Verification codes	App-specific passwords	Registered computers	Security Keys

- You can also print out a list of Backup codes for use in an emergency. Let's assume you are out of the country and can't use youe phone to receive a text message with your 4-digit access code, You can use these codes instead. There good fore 1 time access but you get 10 of them. You can also generate new ones if you run out.
- You can manage Registered computers as shown above. This means that you can Require codes on PCs that were previously tagged as safe.
- Security Keys only work with Google Chrome. I haven't tried this feature since you need a special device. A YubiKey will work but is is a different one then the one I use with LastPass. You can get one here for $17.99 on Amazon. Remember – this only works with Google Chrome. You can read about a Security Key here.

- You can always turn off 2-Step Verification by going to the right of Security Keys as shown below.

2-Step Verification is: ON

Protecting your account since Dec 22, 2014.

[Turn off]
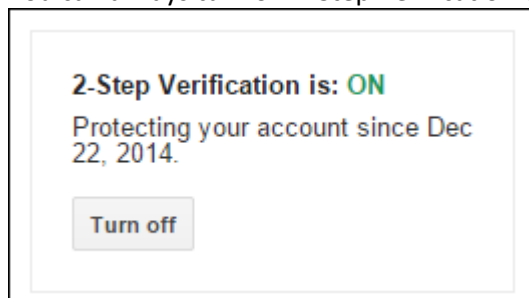
Google Location History

How to access it. Go to maps.google.com/locationhistory or click here.

- Location History and Location Reporting data may be used by any Google app or service, including in ads on and off Google. For example, Google Maps may use it to improve your search results based on the places that you've been.

- **Location Reporting:** Allows Google to periodically store and use your device's most recent location data, as well as activities like driving, walking, and biking, in connection with your Google Account.
- **Location History:** Allows Google to store a history of your location data from all devices where you are logged into your Google Account and have enabled Location Reporting. You can turn off Location History at any point, but doing so won't delete your Location History. It also will not turn off Location Reporting, GPS, or Wi-Fi location services for your device.

- iPhone – go to Settings, Privacy, Location Services
- Turn Location Reporting on or off using Google Settings
  - Open Google Settings from your device's apps menu.
    - Devices running Android 4.3 or lower: Touch Location > Location Reporting.
    - Devices running Android 4.4: Touch Account History > Google Location History > Location Reporting.
    - Slide the switch ON or OFF.
    - For Android 2.3-3.0 devices, check the box next to "Location Reporting."
    - Turn Location Reporting on or off using the Location menu in Google Settings
  - This setting is available on devices running Android 4.4.
    - Open Google Settings from your device's apps menu.
    - Touch Location > Google Location Reporting > Location Reporting.
    - Slide the switch ON or OFF.

Here's a sample form my Location History. You can tell that I was in San Juan on that day.
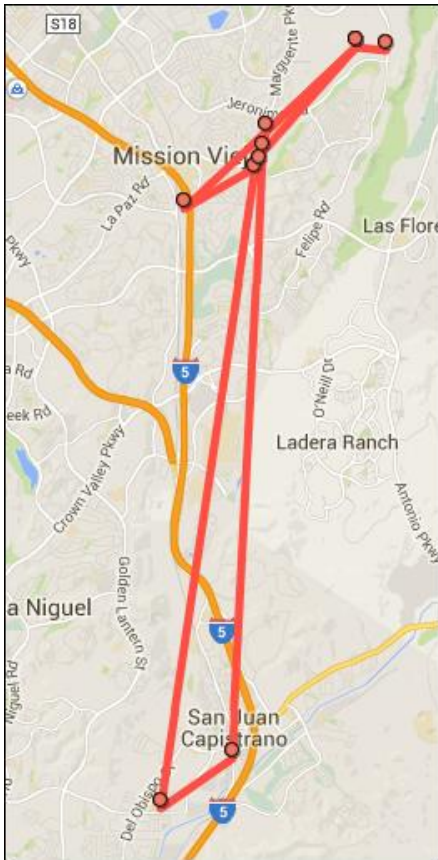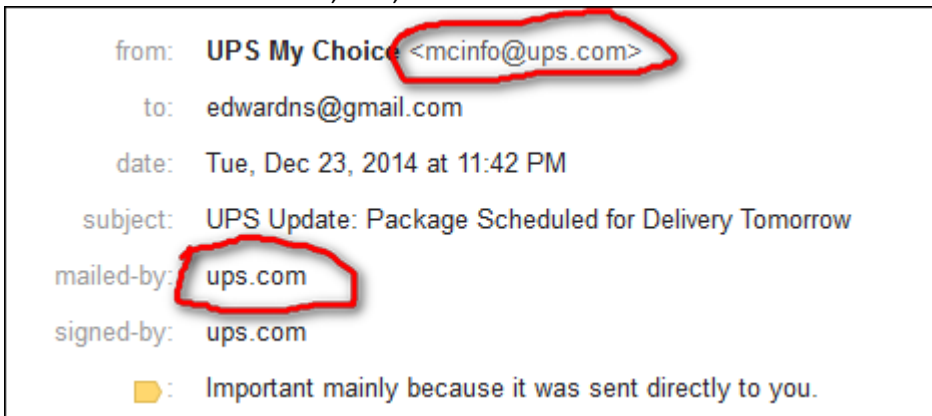
Use the Show Details feature in emails

When you receive an email it's not always from who you think it is. To see who the sender really is, especially if you are suspicious, click the little arrow as shown below.
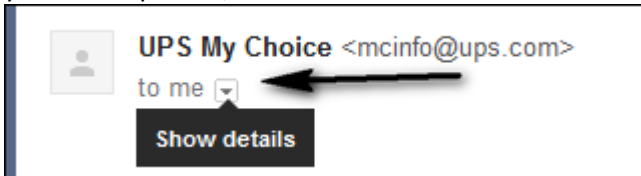
This reveals the real sender, UPS, as shown below.

Google Safety Center

Go to google.com/safetycenter or click here. We will explore this site in class. This site is mostly about educating you so you can be more secure or in some cases browse without leaving a trail.

Google Dashboard

This is not so much about security but it's worth a visit nonetheless. You can visit it at google.com/settings/dashboard or click here. We will review it in class.

As a minimum you should scroll down to Gmail and click Privacy and security as shown below.
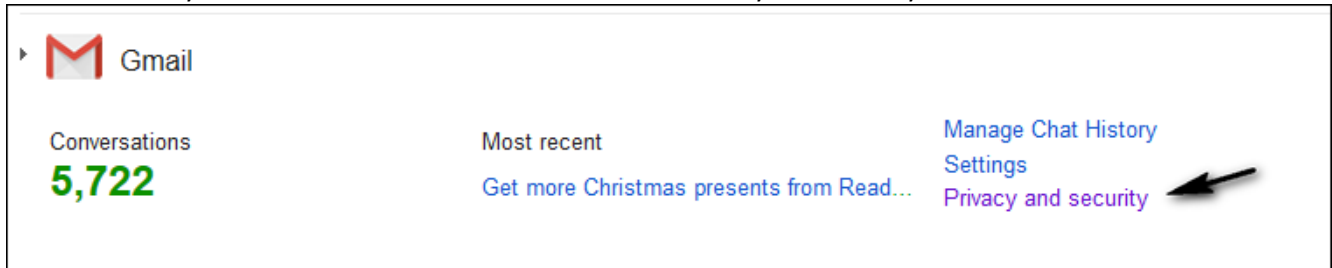
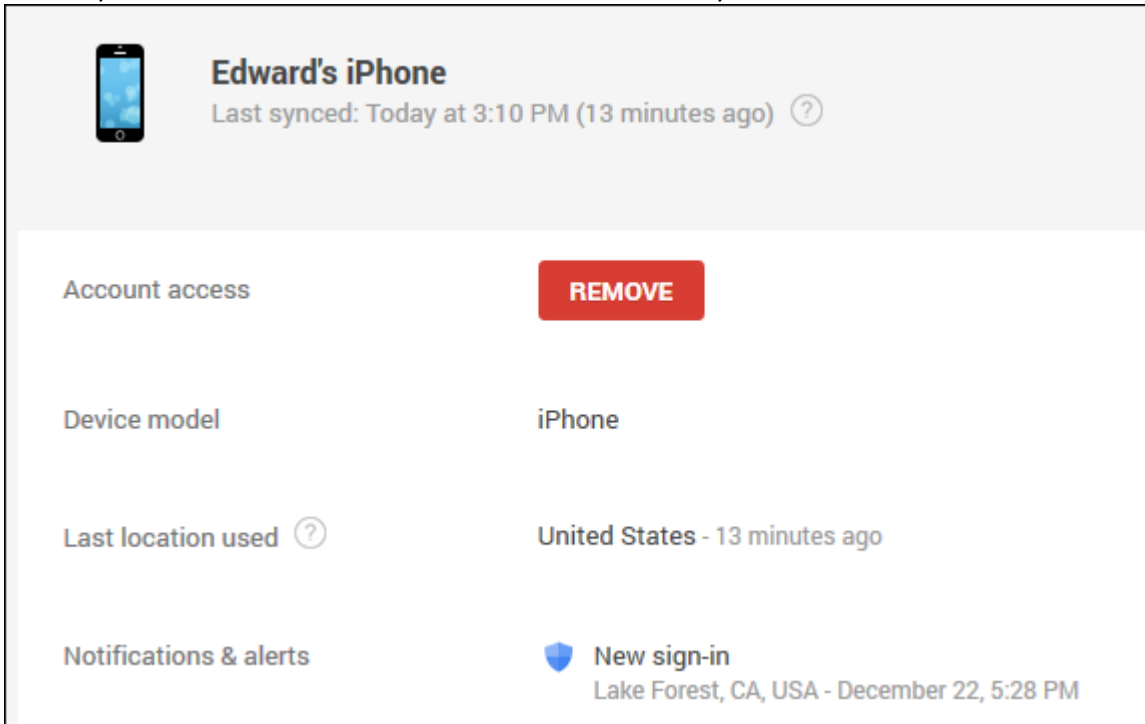Check out the links there, some are very informative, especially the Security Checklist.

Check your Devices and Activities

Go to security.google.com/settings/security/activity or click here. Look for any suspicious activity.

Here's my recent activities.

Click any of the devices to view more information. Here's my iPhone info.

Using Java

Why is Java a security risk?
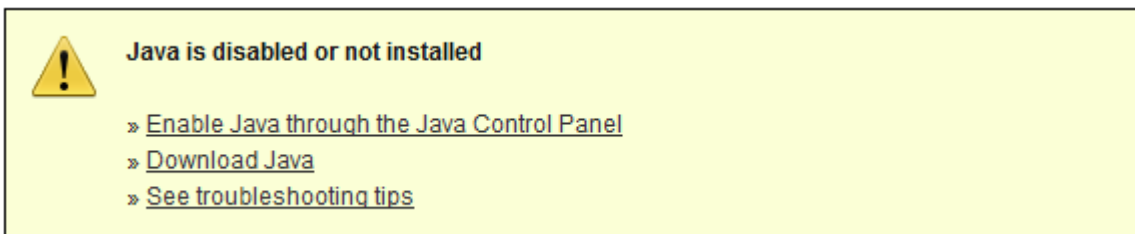- It is exploitable by hackers
- Users do not patch it regularly

Find out if you have Java installed by going to http://www.java.com/en/download/installed.jsp
Here's my status below with no Java on my PC or with it disabled in my browsers.

Here's the message that I received during the Java installation since I have Java disabled in my browsers.

Here's the status of my Java after allowing it in my browsers.

Java Versions on Your Computer

✅ **Congratulations!**
You have the recommended Java installed
Version 8 Update 25

No out-of-date versions of Java were found.

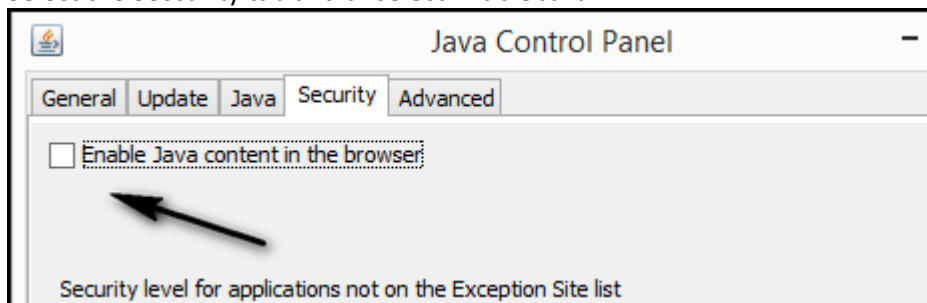Return to the Java.com home page
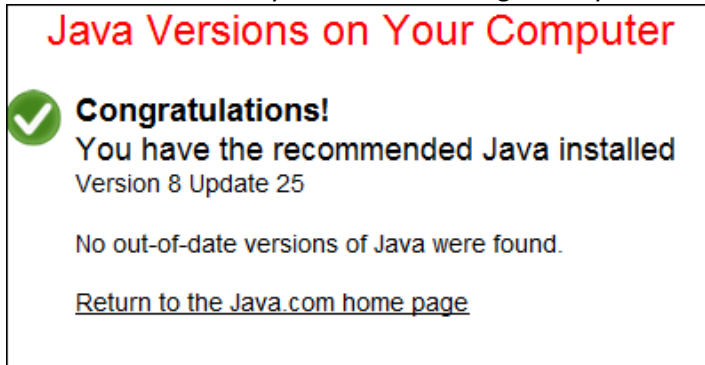
How do you know if you need Java? One way to find out if you need it is to remove it and determine what you can no longer do.

- My recommendations – uninstall it if you don't need it.
- As a minimum, disable it in your browsers as follows
  - Open the Control Panel and click Java (32-bit)

    HomeGroup
    Java (32-bit)
    Location Settings
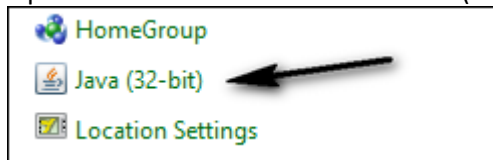
  - Select the Seccurity tab and unselect Enable Java

    Java Control Panel

    General | Update | Java | Security | Advanced

    ☐ Enable Java content in the browser

    Security level for applications not on the Exception Site list

Mobile devices

- Make sure you have passcode and fingerprint sensing turned on

Resources

- For Identity Theft - read the information here and here.