

# Practical Paranoia Android 4

## Security Essentials

- ☑ Easiest
- ☑ Step-By-Step
- ☑ Comprehensive
- ☑ Guide To Securing
- ☑ Data and Communications
- ☑ On Your Home and Office  
Android Phone and Tablet

Marc L. Mintz, MBA-IT, ACTC, ACSP

Practical Paranoia: Android Security Essentials for Home and Business  
Marc Mintz

Copyright © 2015, 2016 by Marc Mintz.

Notice of Rights: All rights reserved. No part of this document may be reproduced or transmitted in any form by any means without the prior written permission of the author. For information on getting permission for reprints and excerpts, contact [marcmintz@gmail.com](mailto:marcmintz@gmail.com).

Notice of Liability: The information in this document is presented on an “As Is” basis, without warranty. While every precaution has been taken in the preparation of this document, the author shall have no liability to any person or entity with respect to any loss or damage caused by or alleged to be caused directly or indirectly by the instructions contained in this document, or by the software and hardware products described within it. It is sold with the understanding that neither the author nor the publisher is engaged in rendering professional security or Information Technology service to the reader. If security or Information Technology expert assistance is required, the services of a professional person should be sought.

Trademarks: Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the author was aware of a trademark claim, the designations appear as requested by the owner of the trademark. All other product names and services identified in this document are used in editorial fashion only and for the benefit of such companies with no intention of infringement of trademark. No such use, or the use of the trade name, is intended to convey endorsement or other affiliation within this document.

Correspondence with the author may be made through email at [marc@mintzIT.com](mailto:marc@mintzIT.com) or telephone at +1 888.479.0690 or +1 505.814.1413.

Editions: 1.0: 7/2015 • 1.1: 12/2015 • 1.2: 1/2016

Cover design by Ed Brandt

ISBN-10: 1514291002

ISBN-13: 978-1514291009

# Dedication

*To Candace,  
without whose support and encouragement  
this work would not be possible*

*My great thanks to Anthony Galczak, our Android Guru,  
who painstakingly assisted with the research for this project*



# Contents At A Glance

Dedication .....	3
Contents At A Glance .....	5
Contents In Detail .....	7
Introduction .....	13
1. Vulnerability: Device .....	23
2. Vulnerability: Network.....	113
3. Vulnerability: Web Browsing .....	133
4. Vulnerability: Email .....	169
5. Vulnerability: Google Account.....	233
6. Vulnerability: Documents .....	259
7. Vulnerability: Text Messaging.....	285
8. Vulnerability: Internet Activity .....	303
9. Vulnerability: Google Wallet and Credit Cards .....	323
The Final Word.....	351
Index.....	353
<i>Your Virtual CIO &amp; IT Department</i> Mintz InfoTech, Inc. when, where, and how you want IT .....	357
Practical Paranoia Security Essentials Workshops & Books Android, iOS, OS X, Windows .....	359



# Contents In Detail

Dedication .....	3
Contents At A Glance .....	5
Contents In Detail .....	7
Introduction .....	13
Who Should Read This Book .....	14
What is Unique About This Book .....	15
Why Worry? .....	17
Reality Check .....	18
About the Author.....	20
Practical Paranoia Updates.....	21
Practical Paranoia Book Upgrades .....	22
1. Vulnerability: Device .....	23
The Great Awakening.....	24
Passwords.....	25
Assignment: Create a Screen Lock using a Pattern Lock.....	26
Assignment: Create a Screen Lock Using a Password.....	29
LastPass .....	34
Assignment: Install LastPass .....	35
Assignment: Add a Site to LastPass .....	42
System Updates .....	48
Assignment: Check for and Install Android Updates .....	48
Assignment: Update Android System Software.....	51
Assignment: Update Apps .....	62
General Security .....	65
Assignment: Enable Screen Timeout.....	65
Assignment: Require Authentication for App Purchases.....	68
Assignment: Secure Play Store from Unauthorized Apps.....	71
Malware .....	74
Assignment: Install & Configure Bitdefender Mobile Security & Antivirus .....	75

## Contents In Detail

Assignment: Scan for Malware with Bitdefender .....	80
Assignment: Restrict Access to Applications using Bitdefender's App Lock.....	83
Backups.....	86
Assignment: Backup to Google .....	87
Assignment: Verify the Google Backup via a Computer .....	91
Assignment: Data Recovery from Google.....	92
Bitdefender Anti-Theft.....	97
Assignment: Activate and Configure Bitdefender Anti-Theft.....	97
Assignment: Use Bitdefender to Find Your Device from a Computer .....	101
Preparing an Android Device for Sale .....	105
Assignment: Securely Erase an Android Device .....	105
Assignment: Format an SD Card .....	109
2. Vulnerability: Network.....	113
Wi-Fi Encryption Protocols .....	114
Firewall .....	116
NoRoot Firewall .....	117
Assignment: Install and Configure NoRoot Firewall for Android.....	117
Assignment: Allow an Application Access with NoRoot Firewall .....	122
Assignment: Use Global Filters and Access Log with NoRoot Firewall ....	127
3. Vulnerability: Web Browsing .....	133
Browser Security.....	134
Assignment: Configure Google Chrome Settings.....	134
Assignment: Google Incognito Mode.....	143
Safer Internet Searches with DuckDuckGo.....	145
Assignment: Install DuckDuckGo Search & Stories .....	145
Assignment: Use DuckDuckGo to Search and Display in an External Browser .....	147
HTTPS: How to Know You Are in a Secure Web Page.....	152
TOR.....	154
Assignment: Install Firefox .....	154
Assignment: Install and Configure Orbot .....	157
4. Vulnerability: Email .....	169
Email Encryption Protocols.....	170
Assignment: Configure the Email Application to Use TLS or SSL .....	171



## Contents In Detail

Assignment: Configure Browser Email to Use HTTPS .....	176
End-To-End Secure Email With SendInc .....	177
Assignment: Create a SendInc Account.....	178
Assignment: Create an Encrypted SendInc Email .....	180
Assignment: Receive and Respond to a SendInc Secure Email .....	182
End-To-End Secure Email With S/MIME.....	184
Assignment: (Windows) Acquire a Free Class 1 S/MIME Certificate for Personal Use.....	185
Assignment: Export S/MIME Certificate from Windows for Import to Android.....	193
Assignment: (OS X) Acquire a Free Class 1 S/MIME Certificate for Personal Use.....	202
Using S/MIME.....	208
Assignment: Install and Configure CipherMail.....	208
Assignment: Add a Private Key to CipherMail.....	214
Assignment: Compose an S/MIME Encrypted Email with CipherMail....	219
Assignment: Receive and Read S/MIME Encrypted Emails in CipherMail .....	225
Assignment: Send your S/MIME Certificate to Recipients in CipherMail	227
Assignment: Import a Certificate to CipherMail.....	229
Closing Comments on Encryption and the NSA .....	232
5. Vulnerability: Google Account.....	233
Google Account.....	234
Assignment: Create a Google Account.....	235
Assignment: Implement Two-Step Verification for Your Google Account .....	244
6. Vulnerability: Documents .....	259
Document Security .....	260
Assignment: Install Crypt4All Lite .....	260
Assignment: Encrypt a File with Crypt4All Lite .....	263
Assignment: Decrypt a File with Crypt4All Lite.....	267
Assignment: Secure Erase a File with Crypt4All Lite .....	272
Assignment: Encrypt an SD Card .....	276
7. Vulnerability: Text Messaging.....	285
Text Messaging.....	286

## Contents In Detail

Assignment: Install and Configure Wickr .....	287
Assignment: Send a Secure Text Message with Wickr.....	297
8. Vulnerability: Internet Activity .....	303
Virtual Private Network.....	304
VPNArea .....	307
Assignment: Purchase and Install VPNArea.....	307
Assignment: Configure VPNArea.....	316
9. Vulnerability: Google Wallet and Credit Cards .....	323
Assignment: Install and Configure Google Wallet.....	325
Assignment: Add a Credit Card or Bank Account with Google Wallet....	329
Assignment: Add a Loyalty Card to Google Wallet.....	335
Assignment: Enable Tap and Pay and NFC.....	341
Assignment: Use Google Wallet in Stores .....	348
The Final Word.....	351
Index.....	353
<i>Your Virtual CIO &amp; IT Department</i> Mintz InfoTech, Inc. when, where, and how you want IT .....	357
Practical Paranoia Security Essentials Workshops & Books Android, iOS, OS X, Windows .....	359

# **PRACTICAL PARANOIA ANDROID 4 SECURITY ESSENTIALS**



# Introduction

*Just because you're paranoid doesn't mean they aren't after you.*  
-Joseph Heller, *Catch-22*

*Everything in life is easy—once you know the how.*  
-Marc L. Mintz

## Who Should Read This Book

Traditional business thinking holds that products should be tailored to a laser-cut market segment. Something like: *18-25 year old males, still living at their parents home, who like to play video games, working a minimum-wage job.* Yup, we all have a pretty clear image of that market segment.

In the case of this book, the market segment is *all users of Android 4 smartphones and tablets.* Really! From my great-Aunt Rose who is wrestling with using her first computer, to the small business, to the IT staff for major corporations and government agencies.

Even though the military may use better security on their physical front doors—MP's with machine guns protecting the underground bunker—compared to a residential home with a Kwikset deadbolt and a neurotic Chihuahua, the steps to secure OS X for home and business use are almost identical for both. There is little difference between *home-level security* and *military-grade security* when it comes to this technology.

The importance of data held in a personal computer may be every bit as important as the data held by the CEO of a Fortune 500. The data is also every bit as vulnerable to penetration.

## What is Unique About This Book

*Practical Paranoia: Android Security Essentials* is the first comprehensive security book written with the new to average user in mind—as well as the IT professional. The steps outlined here are the same steps used by my consulting organization when securing systems for hospitals, government agencies, and the military.

By following the easy, illustrated, step-by-step instructions in this book, you will be able to secure your computer to better than National Security Agency (NSA) standards.

Hardening your computers will help your business protect the valuable information of you and your customers. Should your work include HIPAA or legal-related information, to be in full compliance with regulations it is likely that you will need to be using Android 5 or higher.

For those of you caught up in the ADHD epidemic, do not let the number of pages here threaten you. This book really is a quick read because it has lots of actual screenshots. Written for use in our *Practical Paranoia: Security Essentials Workshops* as well as for self-study, this book is the ultimate step-by-step guide for protecting the new user who has no technical background, as well as for the experienced IT consultant. The information and steps outlined are built on guidelines from Google, the NSA, and my own 30 years as an IT consultant, developer, technician and trainer. I have reduced dull background theory to a minimum, including only what is necessary to grasp the need-for and how-to.

The organization of this book is simple. We provide chapters representing each of the major areas of vulnerability, and the tasks you will do to protect your data, device, and personal identity.

Although you may jump in at any section, I recommend you follow the sequence provided to make your system as secure as possible. Remember, the bad guys will not attack your strong points. They seek out your weak points. Leave no obvious weakness and they will most likely move on to an easier target.

To review your work using this guide, use the *Mintz InfoTech Android 4 Security Checklist* provided at the end of this book.

## Introduction

Theodore Sturgeon, an American science fiction author and critic, stated: *Ninety percent of everything is crap*. [https://en.wikipedia.org/wiki/Sturgeon%27s\\_law](https://en.wikipedia.org/wiki/Sturgeon%27s_law). Mintz's extrapolation of Sturgeon's Revelation is: *Ninety percent of everything you have learned and think to be true is crap*.

I have spent most of my adult life in exploration of how to distill what is real and accurate from what is, well, Sturgeon's 90%. The organizations I have founded, the workshops I've produced, and the *Practical Paranoia* book series all spring from this pursuit. If you find any area of this workshop or book that you think should be added, expanded, improved, or changed, I invite you to contact me personally with your recommendations.



## Why Worry?

In terms of network, Internet, and data security, OS X users must be vigilant because of the presence of malware such as viruses, Trojan horses, worms, phishing, and key loggers impacting our computers. Attacks on computer and smartphone users by tricksters, criminals, and governments are on a steep rise. In addition to OS X-specific attacks, we are vulnerable at points of entry common to all computer users, including Flash, Java, compromised websites, and phishing, as well as through simple hardware theft. How bad is the situation?

- According to a study by Symantec, an average enterprise-wide data breach has a recovery cost of \$5 million. With little attention paid to mobile devices, it may be faster and easier to penetrate the corporate network via a compromised smartphone than through a computer.
- According to the New York Times, half of all robberies in San Francisco involved a cellphone.
- In New York, theft of smart devices account for 14 percent of all crimes.
- Most Android users do not create a phone lock, making their data instantly available to anyone with a few seconds to look through their device.
- The typical email is clearly readable at dozens of points along the Internet highway on its trip to the recipient. And most likely is read by somebody you don't know.
- The Cyber Intelligence Sharing and Protection Act (CISPA) [http://en.wikipedia.org/wiki/Cyber\\_Intelligence\\_Sharing\\_and\\_Protection\\_Act](http://en.wikipedia.org/wiki/Cyber_Intelligence_Sharing_and_Protection_Act) promises the government easy access to all of your electronic communications.
- PRISM [http://en.wikipedia.org/wiki/PRISM\\_\(surveillance\\_program\)](http://en.wikipedia.org/wiki/PRISM_(surveillance_program)) allows government agencies to collect and track data on any American.

The list goes on, but we have lives to live and you get the point. It is not a matter of *if* your data will ever be threatened. It is only a matter of *when*, and how often the attempts will be made.

## Reality Check

*Nothing* can 100% guarantee 100% security 100% of the time. Even the White House and CIA websites and internal networks have been penetrated. We know that organized crime, as well as the governments of China, North Korea, Russia, Great Britain, United States, and Australia have billions of dollars and tens of thousands of highly skilled security personnel on staff looking for *zero-day exploits*. These are vulnerabilities that have not yet been discovered by the developer. As if this is not enough, the U.S. government influences the development and certification of most security protocols. This means that industry-standard tools used to secure our data often have been found to include vulnerabilities introduced by government agencies.

With these odds against us, should we just throw up our hands and accept that there is no way to ensure our privacy? Well, just because breaking into a locked home only requires a rock through a window, should we give up and not lock our doors?

Of course not. We do everything we can to protect our valuables. When leaving on vacation we lock doors, turn on the motion detectors, notify the police to prompt additional patrols, and stop mail and newspaper delivery.

The same is true with our digital lives. For the very few who are targeted by the NSA, there is little that can be done to completely block them from reading your email, following your chats, and recording your web browsing. But you can make it extremely time and labor intensive.

For the majority of us not subject to an NSA targeted attack, we are rightfully concerned about our digital privacy being penetrated by criminals, pranksters, competitors, and nosy people as well as about the collateral damage caused by malware infestations.

You *can* protect yourself, your data, and your devices from such attack. By following this book, you should be able to secure fully your data and your first device in two days, and any additional devices in a half day. This is a very small price to pay for peace of mind and security.

## Introduction

Remember, penetration does not occur at your strong points. A home burglar will avoid hacking at a steel door when a simple rock through a window will gain entry. A strong password and encrypted drive by themselves do not mean malware can't slip in with your email, and pass all of your keystrokes – including usernames and passwords – to the hacker.

It is imperative that you secure all points of vulnerability.

1. NOTE: Throughout this book we provide suggestions on how to use various free or low-cost applications to help enforce your protection. Neither Marc L. Mintz nor Mintz InfoTech, Inc. receives payment for suggesting them. We have used them with success, and thus feel confident in recommending them.

## About the Author

Marc Louis Mintz is one of the most respected IT consultants and technical trainers in the United States. His technical support services and workshops have been embraced by hundreds of organizations and thousands of individuals over the past 3 decades.

Marc holds an MBA-IT (Masters of Business Administration with specialization in Information Technology), Chauncy Technical Trainer certification, Post-Secondary Education credentials, and over a dozen industry certifications.

Marc's enthusiasm, humor, and training expertise have been honed on leading edge work in the fields of motivation, management development, and technology. He has been recruited to present software and hardware workshops nationally and internationally. His technical workshops are consistently rated by seminar providers, meeting planners, managers, and participants as *The Best* because he empowers participants to see with new eyes, think in a new light, and problem solve using new strategies.

When away from the podium, Marc is right there in the trenches, working to keep client Android, iOS, OS X, and Windows systems securely connected.

The author may be reached at:

Marc L. Mintz

Mintz InfoTech, Inc.

1000 Cordova Pl

#842

Santa Fe, NM 87505

+1 888.479.0690

Email: [marc@mintzIT.com](mailto:marc@mintzIT.com)

Web: <http://mintzIT.com>

## **Practical Paranoia Updates**

Information regarding IT security changes daily, so we offer you newsletter, blog and Facebook updates to keep you on top of everything.

### **Newsletter**

Stay up to date with your Practical Paranoia information by subscribing to our free weekly newsletter.

1. Visit <http://mintzIT.com>
2. Scroll to the bottom of the home page to the *Contact Us* form.
3. Enter your Name, and Email, and then select the *Sign Up* button.

### **Blog**

Updates and addendums to this book also will be included in our free *Mintz InfoTech Blog*. Go to: <http://mintzit.com>, and then select the *Blog* link.

### **Facebook**

Updates and addendums to this book also will be found in our *Practical Paranoia Facebook Group*. Go to <https://www.facebook.com/groups/PracticalParanoia/>

## Practical Paranoia Book Upgrades

We are constantly updating *Practical Paranoia* so that you have the latest, most accurate resource available. If at any time you wish to upgrade to the latest version of *Practical Paranoia* at the lowest price we can offer:

1. Tear off the front cover of ***Practical Paranoia***.
2. Make check payable to Mintz InfoTech for \$30.
3. Send front cover, check, and mailing information to:
4. Mintz InfoTech, Inc.
5. 1000 Cordova Pl
6. #842
7. Santa Fe, NM 87505
8. Your new copy of ***Practical Paranoia*** will be sent by USPS. Please allow up to 4 weeks for delivery.

# 1. Vulnerability: Device

*For a people who are free, and who mean to remain so, a well-organized and armed militia is their best security.*

–Thomas Jefferson

*Knowledge, and the willingness to act upon it, is our greatest defense.*

–Marc L. Mintz

## The Great Awakening

In June, 2013, documents of the National Security Agency origin were leaked to The Guardian newspaper [http://en.wikipedia.org/wiki/NSA\\_warrantless\\_surveillance\\_controversy](http://en.wikipedia.org/wiki/NSA_warrantless_surveillance_controversy)>. The documents provided evidence that the NSA was both legally and illegally spying on United States citizens' cell phone, email, and web usage. These documents, though causing gasps of outrage and shock by the general public, revealed little that those of us in the Information Technology field had either known or suspected for decades—every aspect of our digital lives is subject to eavesdropping. The more cynical amongst us go even further, stating that *everything* we do on our computers *is* recorded and subject to government scrutiny.

But few of us have anything real to fear from our government. Where the real problem with digital data theft comes from are local kids hijacking networks, professional cyber-criminals who have fully automated the process of scanning networks for valuable information, and malware distributed by criminals, foreign governments, and our own government that finds its way into our systems.

The first step to securing your data is to secure your computer. Remember, you're not in Kansas anymore!



### Passwords

Yes, you know you need passwords. Right? But do you know that every password can be broken? Start by trying “1.” If that doesn’t work, try “2,” and then “3.” Eventually, the correct string of characters will get you into the system. It is only a matter of time.

Thankfully, there are a variety of ways to secure your Android device from the lock screen. The most common screen lock methods are *Face Unlock*, *Pattern*, *PIN*, and *Password*. There are disadvantages and advantages for each method, however when it comes to security I personally prefer the password method.

When using *Face Unlock* one would think that this is a very secure method of locking your device, as you need to be physically in front of your phone in order to gain access to it. The clever part on the attacker’s front is that a high-resolution picture of you taken from Facebook or any social media site is enough to break this type of security.

The *Pattern lock* is a very common type of security used on Android and is one of my favorites due to its simplicity and speed of use. The problem arises for the security-minded as one of the methods to break this type of security is “reverse smudge engineering”. Reverse smudge engineering is just how it sounds, someone physically looking at your touch screen can see where there are more/recent smudges, helping to guess your screen pattern. One way to counteract this process is to create a pattern lock that crosses back on itself at least twice to create possible endpoints. Doing so it makes it far more difficult to trace back the original pattern. I recommend this method of security as a minimum countermeasure for those who want to access your information, but it is not the most ideal method for highly sensitive data.

Lastly, using a *PIN* or a *Password* are really the most foolproof ways of securing your device. If given a choice between using a PIN - which is a fixed set of 4 digits 0-9 (10,000 combinations)–and a variable length password, I believe it’s a no-brainer to pick the Password method.

For those who prefer long passwords, just how long should you make it? As of this writing, Microsoft’s Security Chief recommends a minimum of 14 characters.

## 1. Vulnerability: Device

Cisco recommends a minimum of 24. My recommendation to clients is a minimum of 14, in an easy-to-remember, easy-to-enter phrase.

In addition to password length, it is critical to use a variety of passwords. In this way, should the bad guys gain access to your Facebook password, it cannot be used to access your bank account.

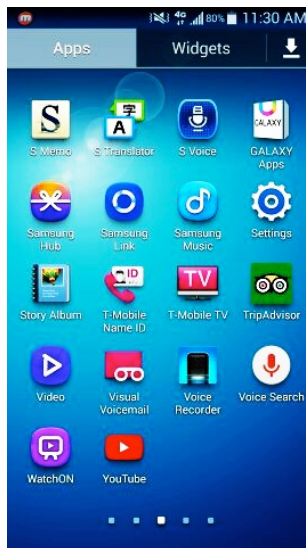
Yes, pretty soon you will have more than a drawer full of passwords for all of your different accounts, email, social networks, financial institutions, etc. How to keep all of them organized and easily accessed amongst all of your various Android devices? More on that later in this book (*LastPass*)!

### **Assignment: Create a Screen Lock using a Pattern Lock**

If your Android device does not currently have any security assigned, continue with this assignment and at least setup a Pattern Lock.

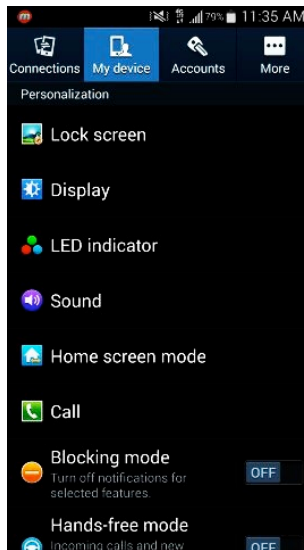
In this assignment, we will configure your Android device to use a Pattern Lock which is the minimum security recommended for your device.

1. Select Apps/Applications > Settings.

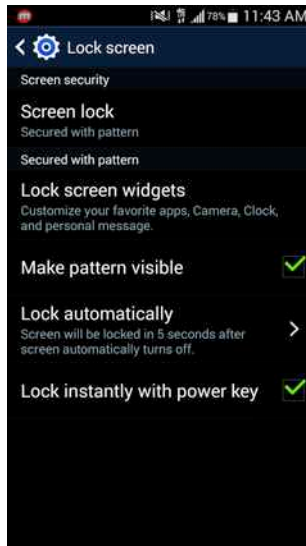


## 1. Vulnerability: Device

2. Select *My Device* > *Lock Screen*.

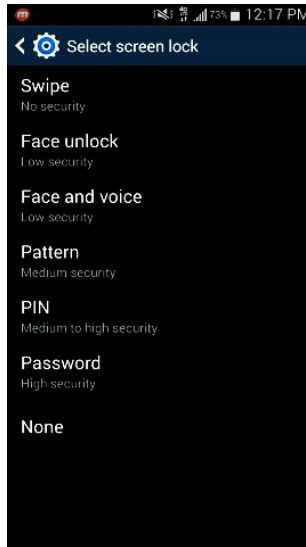


3. Select *Screen Lock*.

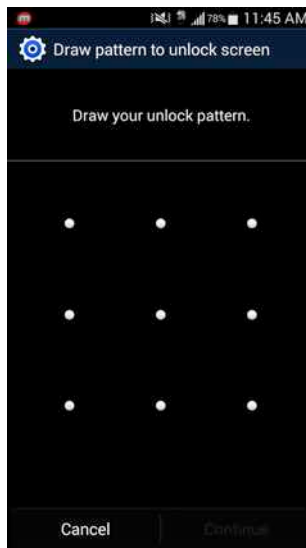


## 1. Vulnerability: Device

### 4. Select Pattern.

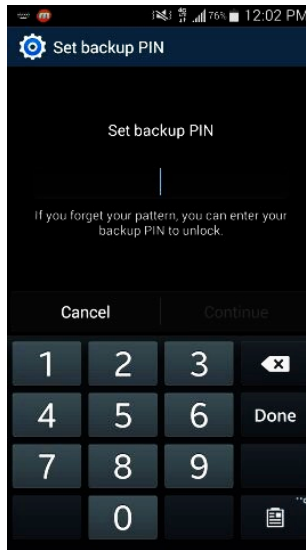


### 5. Draw and confirm your unlock pattern.



## 1. Vulnerability: Device

6. Setup and confirm backup PIN, and then select *Done*. This is necessary in case the pattern is forgotten.



7. Press *Home* to exit *Settings*.

Congratulations! You have just done more to secure your device than the majority of users!

### **Assignment: Create a Screen Lock Using a Password**

If you would prefer to have a strong password instead of a pattern lock for your device, continue with this assignment. Otherwise, feel free to skip over.

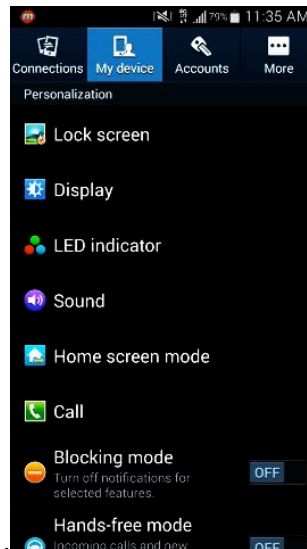
In this assignment we will turn off the Pattern lock, opting for a Password instead.

## 1. Vulnerability: Device

1. Select Apps/Applications > Settings.

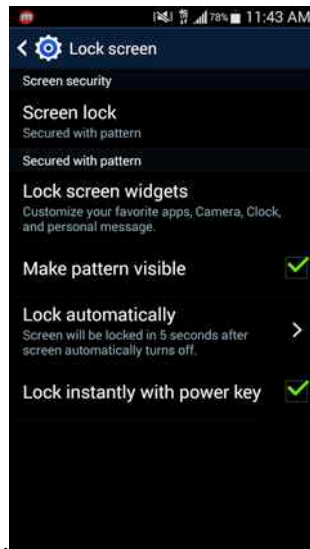


2. Select *My Device* > *Lock Screen*.

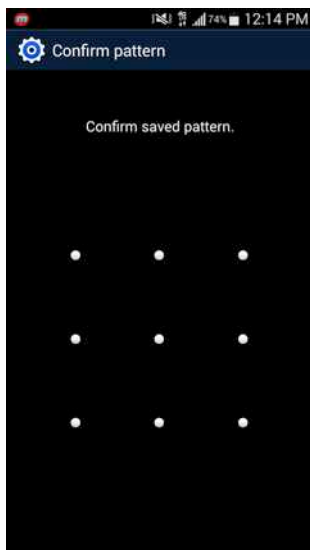


## 1. Vulnerability: Device

### 3. Select *Screen Lock*.

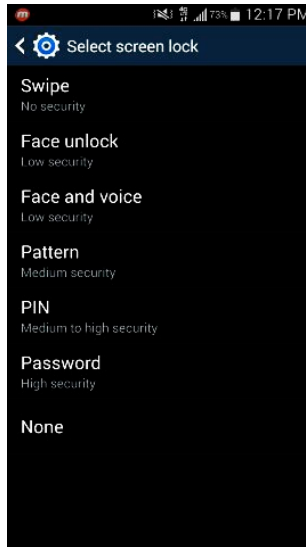


### 4. Confirm saved pattern (or input current security measures such as PIN, face unlock, swipe.)

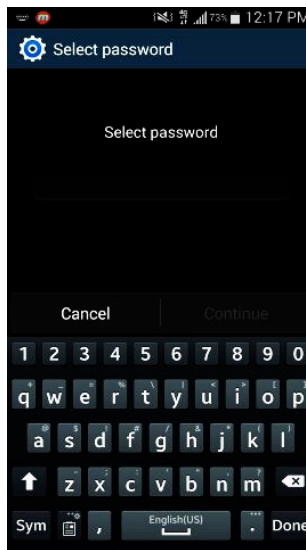


## 1. Vulnerability: Device

5. Tap Password.



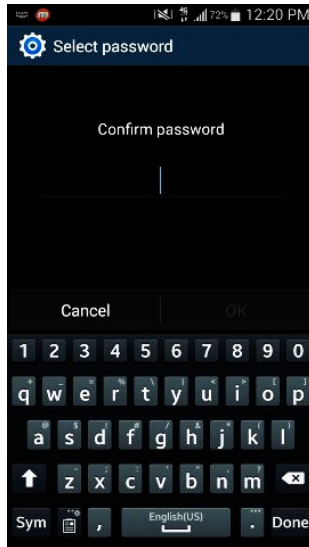
6. Create your strong Password, and then tap *Continue*.





## 1. Vulnerability: Device

7. Confirm your strong Password, and then tap *OK*.



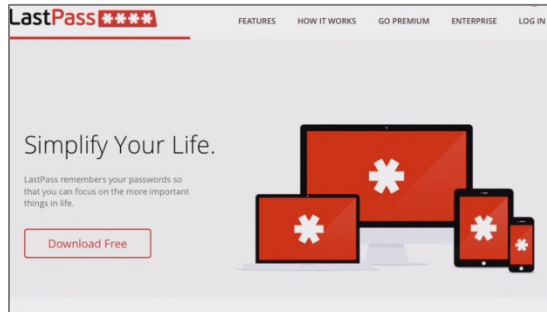
8. Press *Home* to exit *Settings*.

To change back to a *Pattern Lock*, simply repeat the steps in the previous assignment.

## 1. Vulnerability: Device

### LastPass

A great solution to the problem of password management is *LastPass* <<http://www.LastPass.com>>.



The most important advantage of LastPass is that you no longer have to concern yourself with Internet passwords—the issue becomes automatic. LastPass will have your Internet passwords available in each of your browsers and all of your devices—even across operating systems. It also securely stores manually entered data such as challenge Q&A. LastPass provides the following solutions:

- Provides free (ad supported) and premium (no ads) options
- Automatically remembers your Internet passwords, fully encrypted
- Auto fills web-based forms and authentication fields
- Stores notes and challenge Q&A, fully encrypted
- Synchronizes across multiple browsers
- Synchronizes across multiple computers
- Synchronizes across Android, Blackberry, iOS, OS X, Windows, and Windows Phone
- Automatically generate very strong passwords, which since you don't need to remember them, provides for even greater online security.

## 1. Vulnerability: Device

### Assignment: Install LastPass

In this assignment we will download and install LastPass on your Android device. As this is the free version, it will synchronize across all of your various computers and devices, but only for 14 days. The free version works indefinitely across computers, but to synchronize with mobile devices beyond the 14-day trial requires upgrading to *LastPass Premium*.

1. On your device, open *Internet*, and go to <http://lastpass.com>. Select the *Download Free* button.



2. Select the *Mobile* button.



## 1. Vulnerability: Device

3. Scroll to the *LastPass for Android* section, and then select the *Download* button.

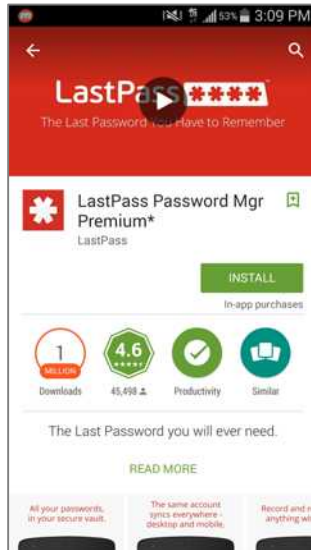


4. A dialog box will appear, Select *Play Store*, and then tap *Just once*.

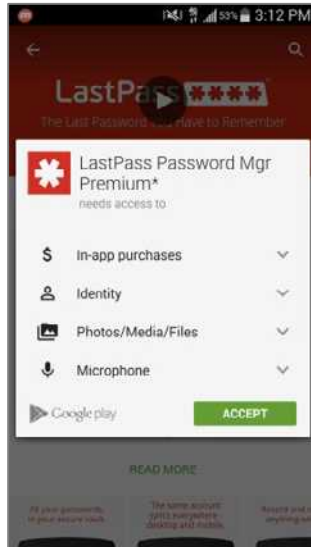


## 1. Vulnerability: Device

5. Your device is taken to the *Play Store* > *LastPass* screen. Select the *Install* button.

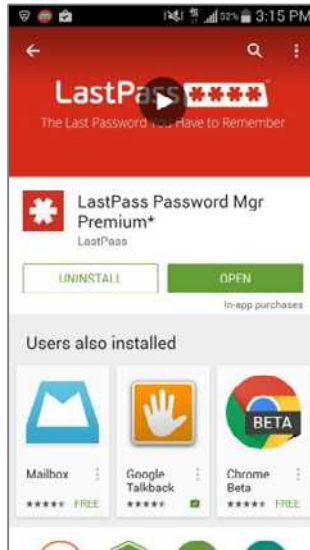


6. *Accept* the access requirements.

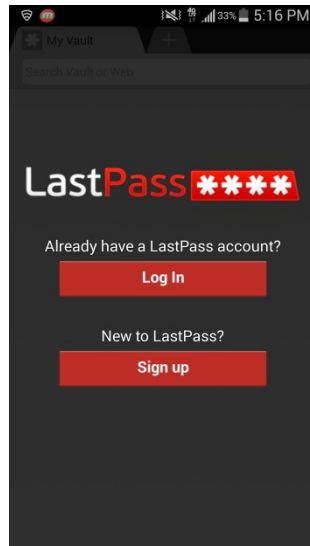


## 1. Vulnerability: Device

7. Once downloaded and installed on your device, select the *Open* button.

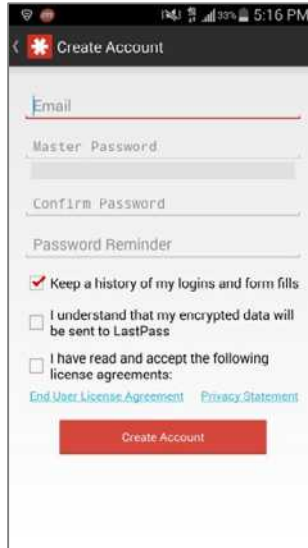


8. When LastPass is launched it will ask you to *Log In* or *Sign Up*. Unless you have an existing LastPass account, select the *Sign Up* button.

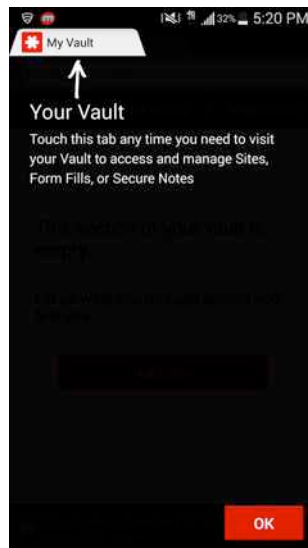


## 1. Vulnerability: Device

9. Under the *Create Account* screen enter your *Email* address, the *Master Password* you will use for LastPass and a *Password Reminder*. Check the boxes for the EULA and privacy statements, and then select *Create Account*.

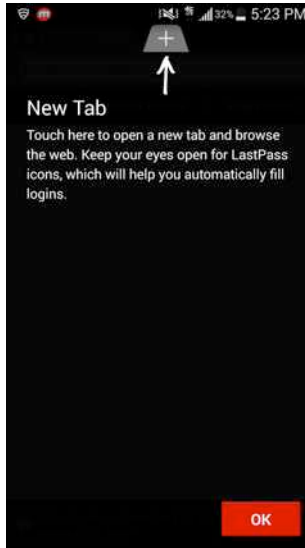


10. The first time LastPass is launched it will take you through a brief tutorial. The first item it introduces you is *Your Vault*. Select *OK* to continue.

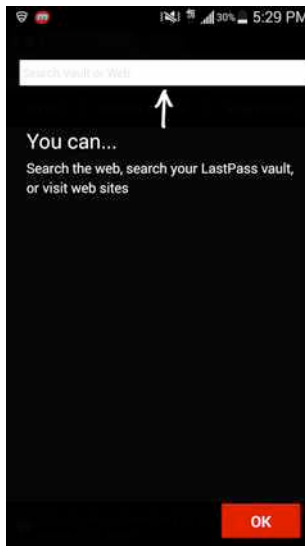


## 1. Vulnerability: Device

11. It then introduces you to the *New Tab* functionality in the LastPass browser. Select *OK* to continue.



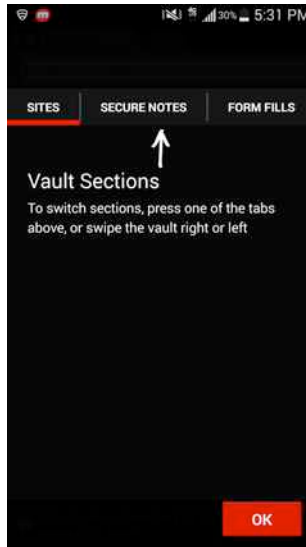
12. It also shows you the *Search* for the LastPass browser. Select *OK* to continue.



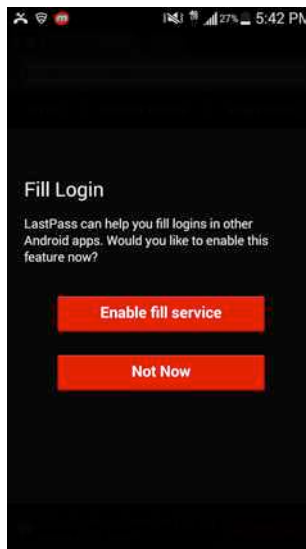


## 1. Vulnerability: Device

13. LastPass displays the different *Vault Sections*. Select *OK* to continue.



14. Lastly, it asks to do a *Fill Login* for other Android applications. This can cause a security loophole when using other applications that are not as secure. Select *Not Now* to continue.



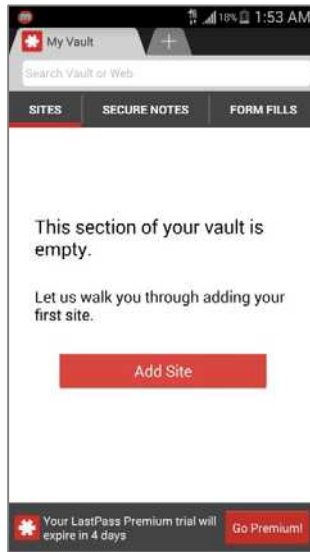
Congratulations! LastPass is now installed and ready to use.

## 1. Vulnerability: Device

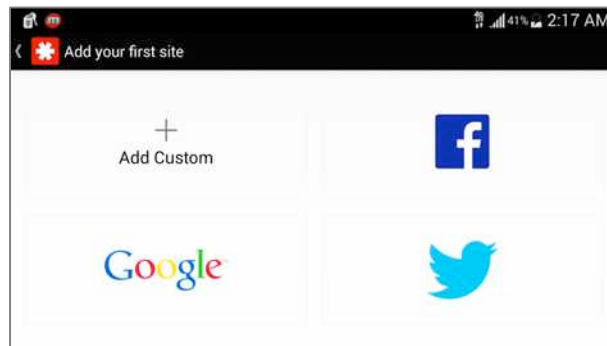
### Assignment: Add a Site to LastPass

With LastPass installed, let's add your first site to it.

1. If you have just completed the previous assignment, LastPass is waiting to take you step by step through adding your first site. Select the *Add Site* button

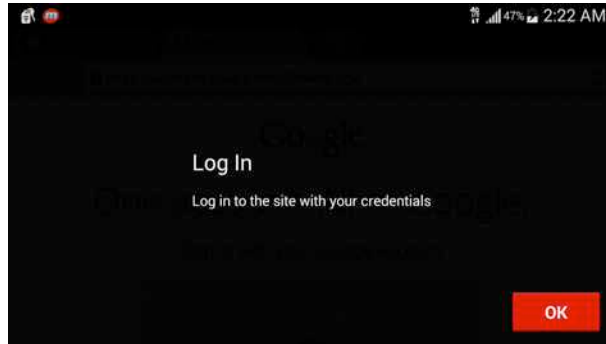


2. The *Add your first site* screen appears. Scroll through the list, and then select a site you visit. For this example, I am using Google.

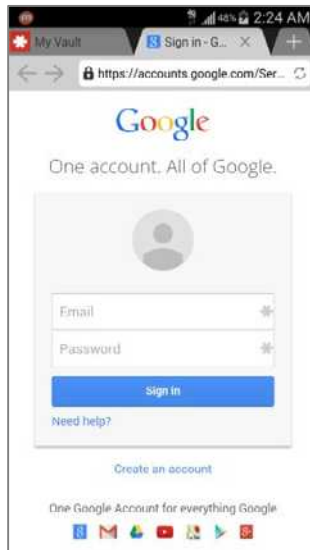


## 1. Vulnerability: Device

3. As this is a tutorial, LastPass will instruct you at each step. At the *Log In* screen, select the *OK* button.

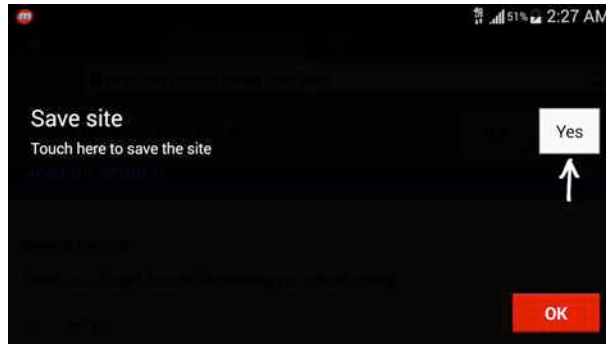


4. The login page for your target website appears. Enter your credentials (in this example using Google, that would be *Email* and *Password*), and then tap the *Sign In* button.

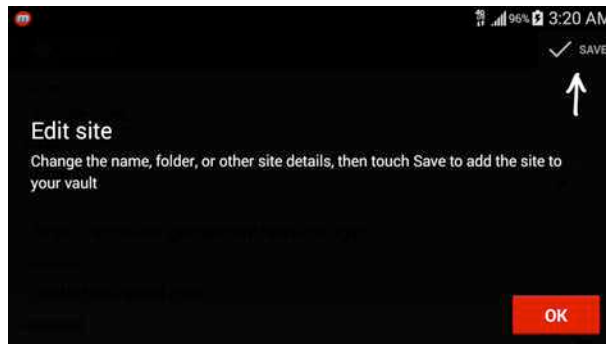


## 1. Vulnerability: Device

5. Again, as this is the first attempt, a tutorial screen appears. Select the *OK* button.

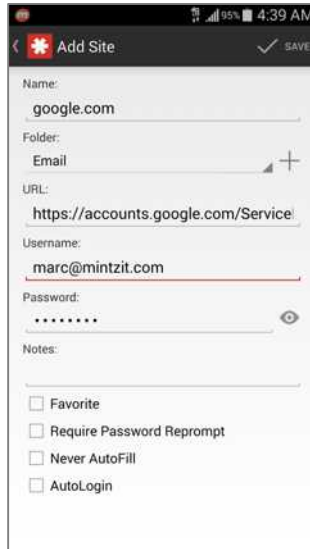


6. Select the *Yes* button in reply to *Do you want LastPass to save this site?*
7. Again with the tutorial (it's a shame you can't hear my impression of a Yiddish accent.) Select the *OK* button.



## 1. Vulnerability: Device

8. If there is anything you wish to edit in the LastPass record for this site, you can do so now. Normally, there is nothing to do but select the *Save* button.



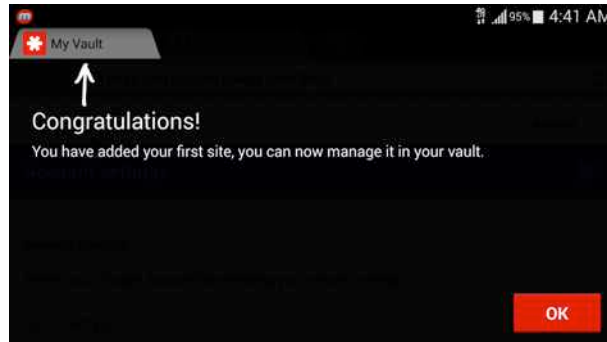
A screenshot of the LastPass mobile application's 'Add Site' form. The form is titled 'Add Site' and has a 'SAVE' button in the top right corner. The fields are as follows:

- Name: google.com
- Folder: Email
- URL: https://accounts.google.com/Service
- Username: marc@mintzit.com
- Password: [masked with dots]
- Notes: [empty]

Below the form are four checkboxes:

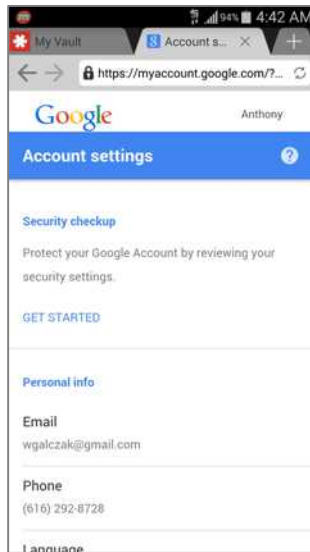
- Favorite
- Require Password Reprompt
- Never AutoFill
- AutoLogin

9. Oh, and once again with the tutorial (really, my Yiddish accent kills.) Tap the *OK* button.



## 1. Vulnerability: Device

10. Success! You are now logged in to your web site. But don't get all amped about it yet. The test is when you allow LastPass to do the login all by itself.

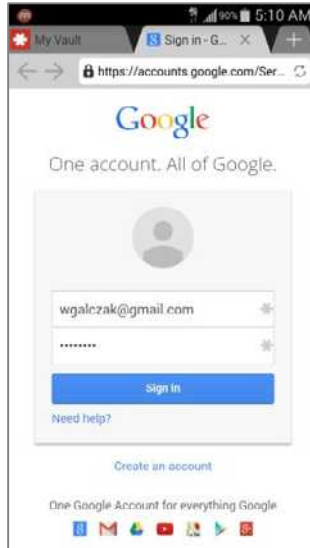


11. Quit Internet.

12. Launch Internet.

## 1. Vulnerability: Device

13. To test, enter the URL of the same site. In my example this was <http://www.google.com>. If LastPass is doing its job, you will see something like this—all login credentials entered for you.



Now we can go and celebrate with some Manischewitz.

## System Updates

I never cease to be amazed at the percentage of users who intentionally do not update their operating system or their applications. In most cases they give the reason that it slows down the device, or they are concerned about introducing instability.

It is true that while the download is in progress your device is busy doing other things and may not be as responsive to your needs as you would like, but that will all pass quickly. As with all computers, with each update and upgrade, there is more functionality, which brings more and more complex code, so the device may run a bit slower. It is also true that the updates may introduce instability—but it is far more likely that not updating will create even greater instability.

There are fundamentally three reasons for updates and upgrades:

- **Bug fixes.** All software and hardware have bugs. We will simply never be rid of them. Developers do want to squash as many as possible so that you are happy with their product and will continue to pay for upgrades.
- **Monetization.** Updates to operating systems and applications are almost always free, or included in the price of the original purchase. Upgrades typically are for fee. Developers include significant new features in an upgrade to encourage the market to purchase.
- **Security patches.** Although rarely talked about, one of the most important reasons for updates is to patch newly discovered security holes. Without the update, your computer may be highly vulnerable to attack.

It is for this last reason alone that I implore clients to be consistent with the update process. In fact, US-CERT (the division of the Department of Homeland Security tasked with protecting us from cyber terrorism) strongly recommends updating both OS and applications/apps within 48 hours of release in order to have the greatest protection from penetration and vulnerabilities.

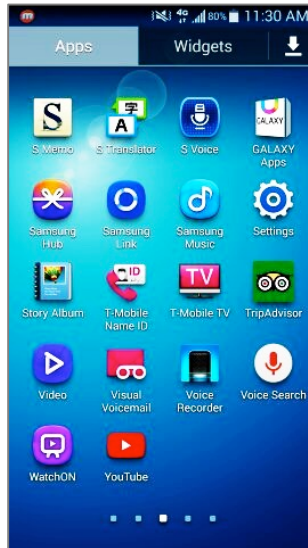
### **Assignment: Check for and Install Android Updates**

In this assignment we will verify our Android update status.

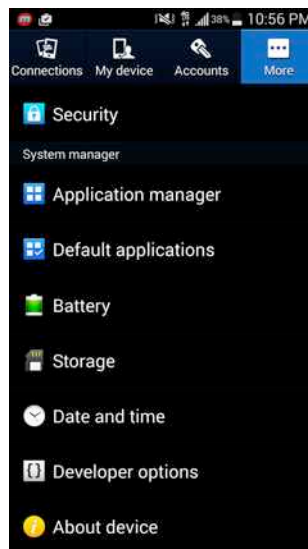


## 1. Vulnerability: Device

1. Select *Apps/Applications* > *Settings*.

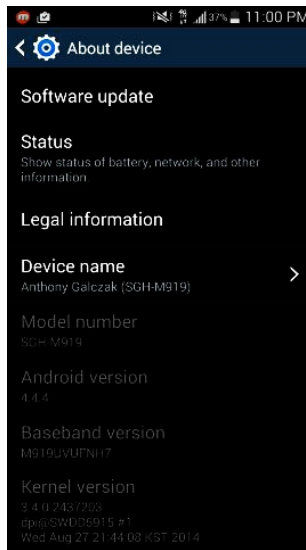


2. Select *More* at the top and then scroll slightly down and select *About Device*.

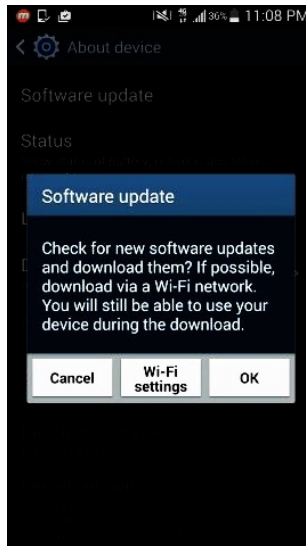


## 1. Vulnerability: Device

3. Select *Software Update*.



4. Select *OK* to check for software updates and download any available updates.



## 1. Vulnerability: Device

5. Give the device a few moments to *Check for Updates*.



6. You will see one of two messages. *The latest updates have already been installed*, or a message stating that a new version is available, with the option to *Update*.
7. If your Android software is up to date, *Hooray*, you are done. If you have new Android software available to download, there is a bit of work ahead of you in the next assignment.

### **Assignment: Update Android System Software**

If your Android system software is up to date, skip this exercise.

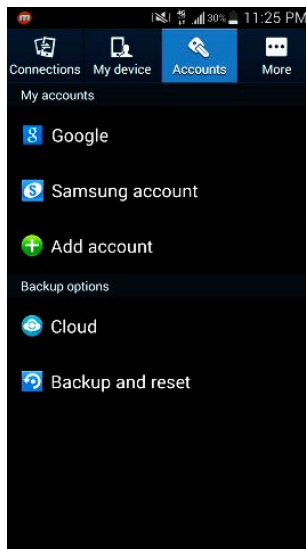
In this exercise we will update your Android system software. Although it happens only rarely, occasionally Murphy strikes during software updates. To help ensure you end up with a perfectly healthy system should Murphy strike, we will take a couple of precautions prior to starting the update.

## 1. Vulnerability: Device

1. Plug your device into power. Depending on the size of the update, and the speed of your Internet, an update may take an hour or more. Should the battery bottom out before the update completes, your device will be left with only half a brain.
2. Back up your device. This can be done via your Google account or through *Samsung Kies* (Or your brand's applicable backup software).

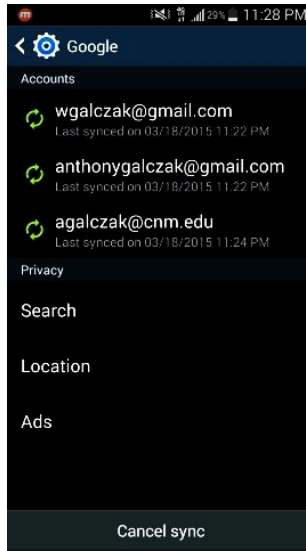
Backup via the device using cloud services.

3. Select *Apps/Applications > Settings*.
4. Select *Accounts > Google*.

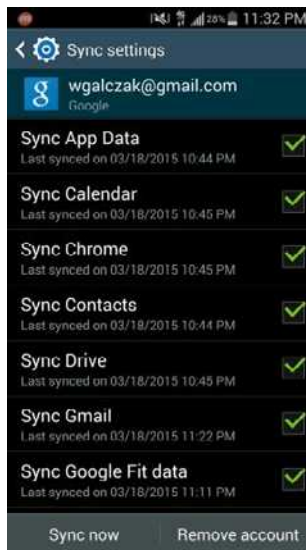


## 1. Vulnerability: Device

5. Select the Google account you'd like to backup data to.
  - Note if you are using multiple Google accounts you will have to backup each one.

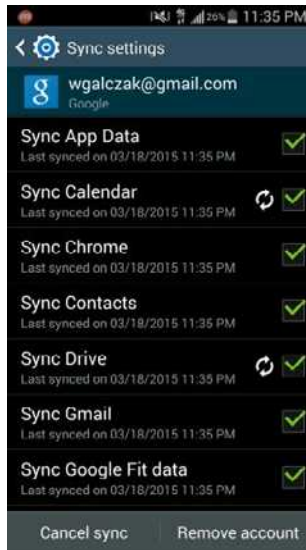


6. Make sure each field to be backed up is checked. If you're unsure, just check all the boxes and then select *Sync Now*.



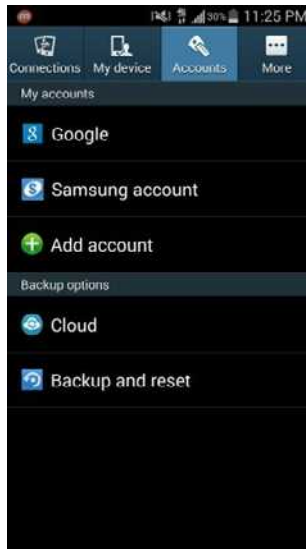
## 1. Vulnerability: Device

7. After you have selected *Sync Now*, double arrows will appear next to some check boxes. Wait for each double arrow to disappear before continuing.

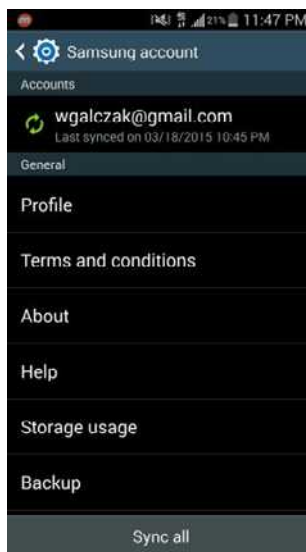


## 1. Vulnerability: Device

8. Now to back up your brand-specific data. Press the *Back* button 2 times to go back to the Accounts screen, and then select *Samsung account*.
  - Note: This will vary on your device brand, tap LG if you have an LG device for example.

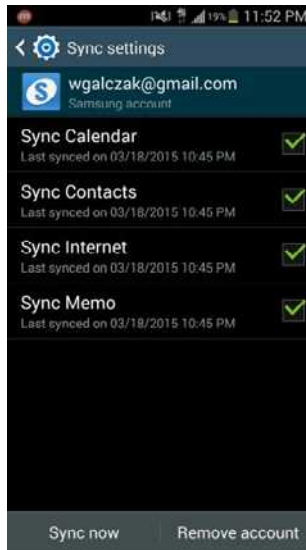


9. Select the Samsung account you would like to back up.



## 1. Vulnerability: Device

10. Check all the boxes of the data you'd like to backup, and then select *Sync now*. Remember to wait for all the double arrows to disappear before continuing.



11. Press the *Back* button 2 times and then select *More > About Device*.

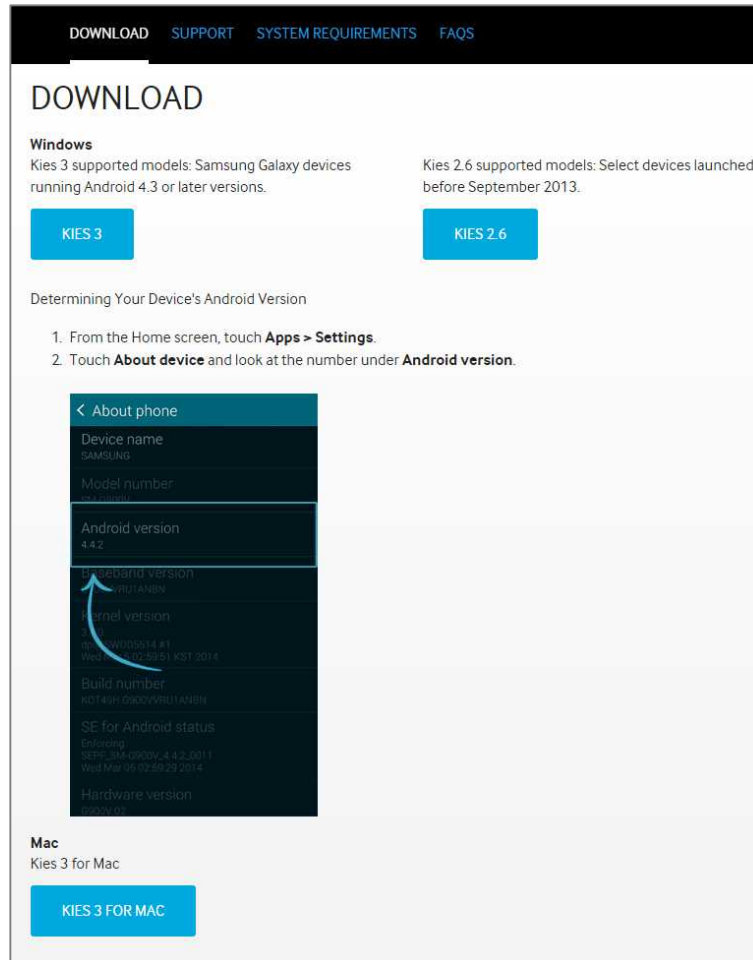




## 1. Vulnerability: Device

Backup using *Samsung Kies* to save data directly on your computer.

12. Open your browser of choice, download Samsung Kies at [www.samsung.com/us/kies](http://www.samsung.com/us/kies), and then click on *Kies 3*.



The screenshot shows the Samsung Kies website's download page. At the top, there is a navigation bar with links for [DOWNLOAD](#), [SUPPORT](#), [SYSTEM REQUIREMENTS](#), and [FAQS](#). The main heading is "DOWNLOAD".

Under the "Windows" section, there are two columns of information:

- KIES 3**: Kies 3 supported models: Samsung Galaxy devices running Android 4.3 or later versions.
- KIES 2.6**: Kies 2.6 supported models: Select devices launched before September 2013.

Below this, there is a section titled "Determining Your Device's Android Version" with two numbered steps:

1. From the Home screen, touch **Apps > Settings**.
2. Touch **About device** and look at the number under **Android version**.

An inset image shows a smartphone screen with the "About phone" settings page. A blue arrow points to the "Android version" field, which displays "4.4.2". Other visible fields include "Device name" (SAMSUNG), "Model number" (SM-N900L), "Baseband version" (PRL1.ABN9), "Kernel version" (3.0.0), "Build number" (KOT49H.D000VBU14009), "SE for Android status" (Enabling), and "Hardware version" (Rev. 01).

At the bottom, under the "Mac" section, it says "Kies 3 for Mac" with a button labeled "KIES 3 FOR MAC".

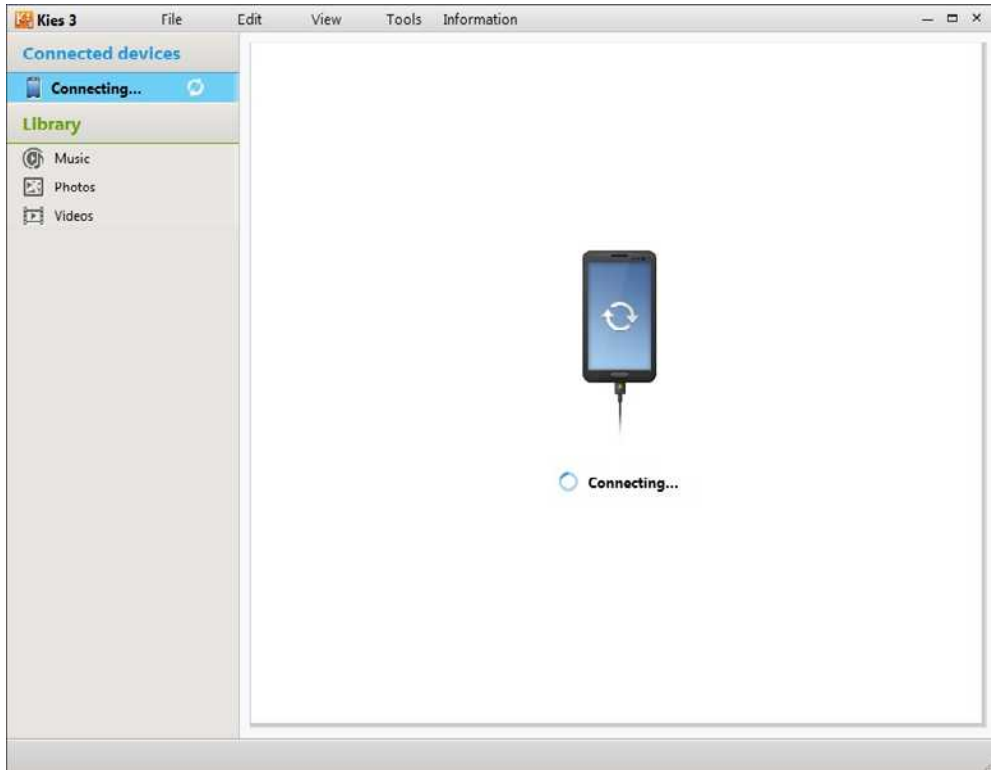
## 1. Vulnerability: Device

13. Install Samsung Kies. Run the executable you downloaded and follow the Installation prompts.



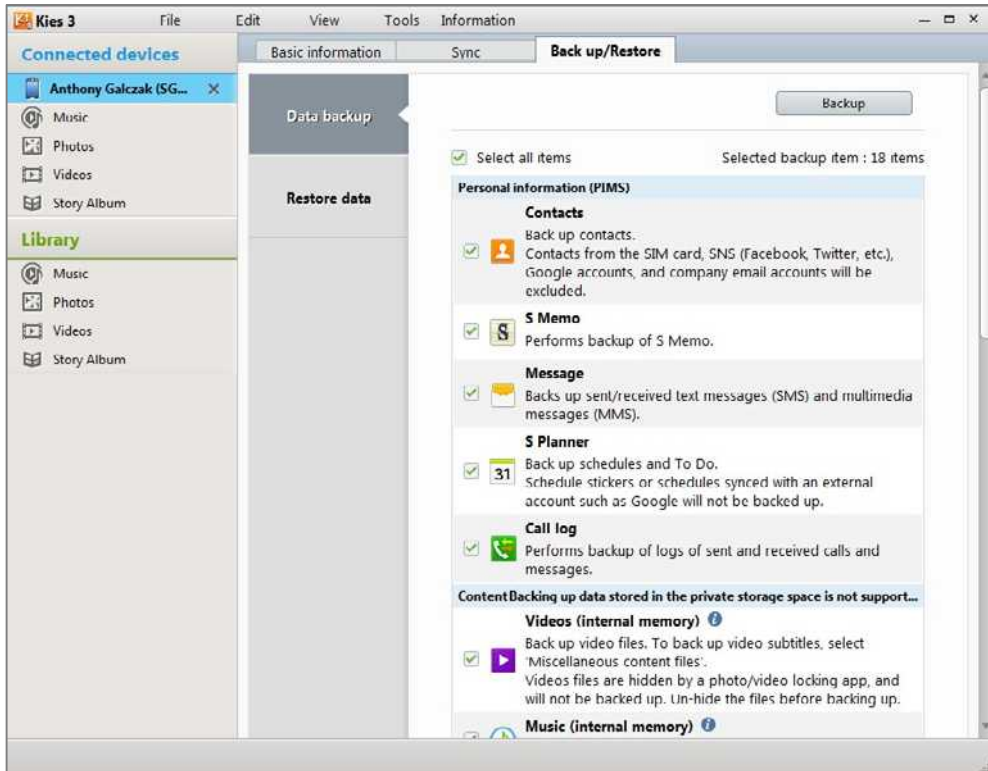
## 1. Vulnerability: Device

14. Run Samsung Kies and connect your device to your computer via USB cable.



## 1. Vulnerability: Device

15. Once your device is successfully connected and synced, click the *Back up/Restore* tab, click the items that you would like to backup and then click *Backup*.



## 1. Vulnerability: Device

16. Select Software update. If you backed up with Kies, select Apps/Applications > More tab > About Device first.



17. Select *OK* to search for and download your update.



18. After waiting for the device to *Check for Updates*, it will prompt you with *A software update is available for your device....* Select *Continue*.

## 1. Vulnerability: Device

19. The device will prompt you once more explaining to keep your device charged and within Wi-Fi/data signal during the download. Select *Continue*.
20. After the update has completed (this will take quite some time) select *Done* to restart your device and complete the update.

Congratulations! Your Android device is now updated and secure from more malware, bugs, and penetration attempts than a few minutes before. But don't rest on that information. It appears evil never sleeps, and it is already working away on new ways to compromise your data.

### **Assignment: Update Apps**

As with the system, apps provide opportunities for bad things to happen to good people. Apps may be poorly coded, unstable, or have unintended weaknesses to compromise. Good app developers are always playing the cat-and-mouse game to be more stable and secure in the face of malicious hackers and errors in previous coding.

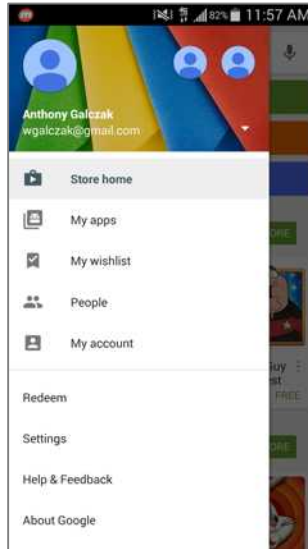
Because of this, it is just as vital to keep apps up to date as it is for the system.

1. From the Home screen, select *Play Store*.

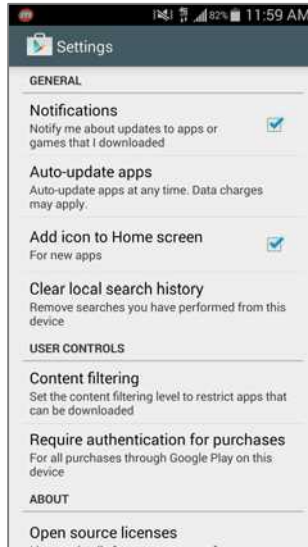


## 1. Vulnerability: Device

2. Select *Menu* in the upper left, and then select *Settings*.



3. Select *Auto-update apps*.



## 1. Vulnerability: Device

4. Select how you would like to Auto-update your apps. If you are on a limited data plan, I'd recommend only on Wi-Fi.



According to the US-CERT <<https://www.us-cert.gov>> (the federal folks in charge of figuring out the best strategies to fight cyber terrorism, malware, and other things that go bump in the ether), one of the top 10 steps to take to harden any system is to ensure updates are applied within 48 hours of release. Allowing your Android device to automatically update is part of this strategy.

That said, there are those who prefer to decide for themselves if and when they will install an update. I'm fairly certain they live their life with hands covering their eyes, ears, and mouth. Should you happen to run into one of these Android users, and they ask you how to disable automatic app updates, you now have the answer for them. Just Select *Play Store* > *Menu* > *Settings* > *Auto-update Apps*.



## 1. Vulnerability: Device

### General Security

There are a few other steps we can take to harden the security of our device fairly easily.

#### Assignment: Enable Screen Timeout

Screen timeout is like the screensaver. After a specified amount of time without use, your Android device will darken its screen, and then require a passcode for access.

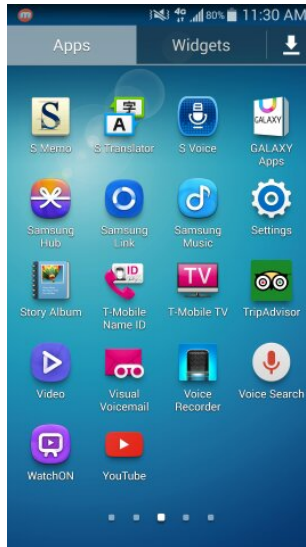
There is no umbrella “right” setting. However, for most people, I recommend setting this to 1 minute. In this way, should you lay your device down unattended, there is only a very slim window of opportunity for someone less ethical than yourself to take advantage of all the juicy data held within.

1. From your Home Screen, select *Apps/Applications*.

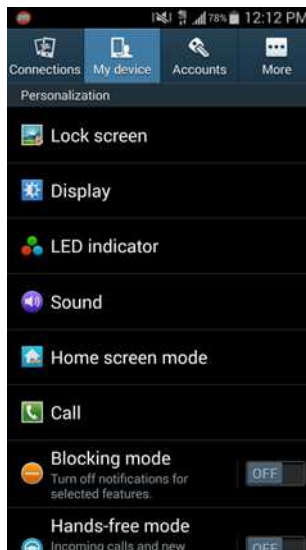


## 1. Vulnerability: Device

2. Select *Settings*.



3. Select My Device > Display.

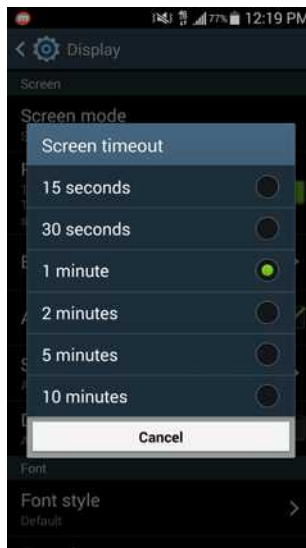


## 1. Vulnerability: Device

4. Scroll down slightly and select *Screen Timeout*.



5. Select the desired time for *Screen Timeout*.



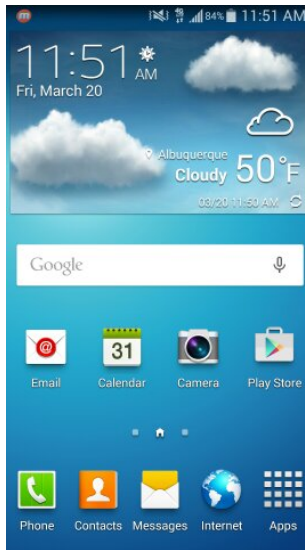
## 1. Vulnerability: Device

6. Press *Home* to exit settings.

### **Assignment: Require Authentication for App Purchases**

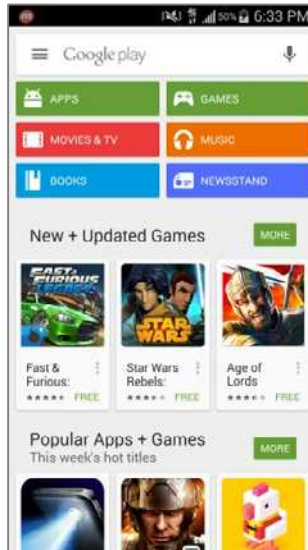
If you allow your children to use your device or have a friend borrow your device, it is important not to just secure your data but also your wallet. For this reason your device must require proper authentication when purchasing apps through the Play Store.

1. From your Home Screen, select *Play Store*.

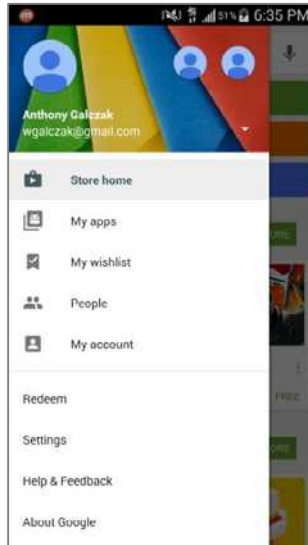


## 1. Vulnerability: Device

2. Select the *Menu* button in the upper left.



3. Select *Settings*.

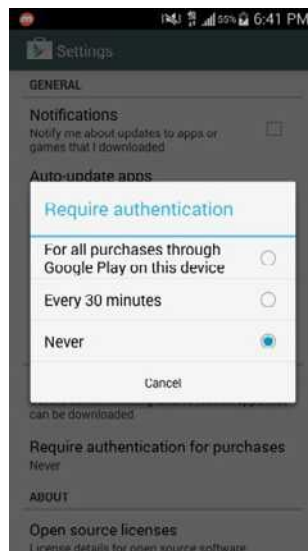


# 1. Vulnerability: Device

4. Select Require authentication for purchases.

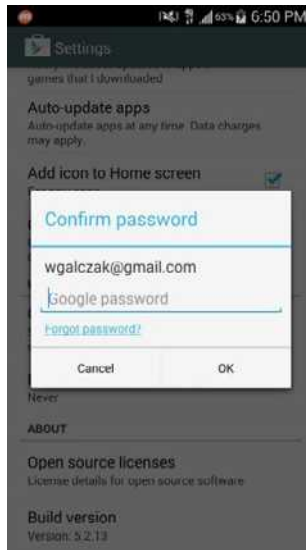


5. Select For all purchases through Google Play on this device.



## 1. Vulnerability: Device

6. Enter the login information for the Google account you use for the Play Store and Select **OK**.



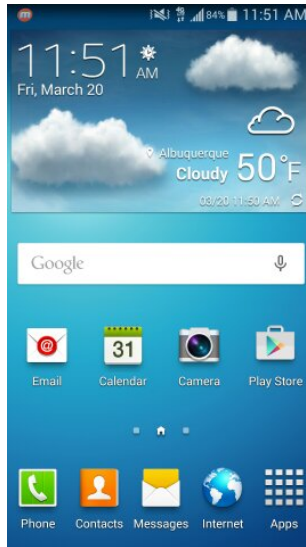
Congratulations! Your children or anyone you let use your device will be blocked from making app purchases and racking up a bill on your dime.

### **Assignment: Secure Play Store from Unauthorized Apps**

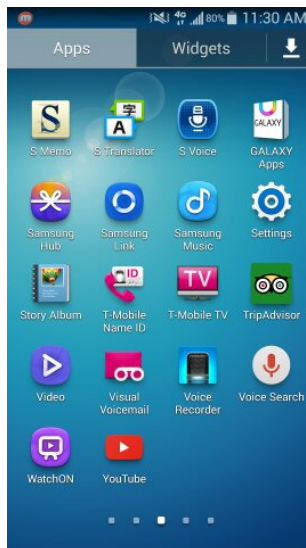
When using the Play Store it is helpful to be aware that Google protects you by default from nefarious applications by refusing a multitude of applications to the Play Store that could be harmful to your device. However, when downloading items from the Play Store or from websites (especially as the raw .apk files) it is important to protect yourself from harmful applications that may be from “unknown sources”. In this assignment, you will set your device prompt whenever it identifies an application trying to run/install that is from an unknown source.

## 1. Vulnerability: Device

1. From your Home Screen, select *Apps/Applications*.



2. Select *Settings*.





## 1. Vulnerability: Device

3. Select More > Security.



4. Scroll down slightly and make sure *Unknown sources* is unchecked and *Verify apps* is checked.



Congratulations! You are now protected from nefarious unknown applications.

## 1. Vulnerability: Device

### Malware

Most people know this category of software as *Antivirus*, but there are so many other nasty critters out there (worms, Trojan horses, phishing attacks, malicious scripts, spyware, etc.) that the overarching term Anti-malware is more accurate.

Depending on how one chooses to measure, there are from 500,000–40,000,000 malware <<http://en.wikipedia.org/wiki/Malware>> in the field that impact Windows. According to Kaspersky <<http://www.kaspersky.com/about/news/virus/2014/Number-of-the-week-list-of-malicious-Android-apps-hits-10-million>> there may be 10,000,000 impacting Android.

The primary way to download apps on an Android device is through the Google Play Store. Google does check and validate the integrity of the applications on the App Store however there is more that you can do to protect your device from malicious attacks. In addition a major risk to your device is visiting a malicious or compromised website.

One particular security flaw in the Android universe is if you have rooted your device <[http://en.wikipedia.org/wiki/Rooting\\_%28Android\\_OS%29](http://en.wikipedia.org/wiki/Rooting_%28Android_OS%29)>. If this is the case, several security measures on your phone have been effectively disabled as you now have access to the kernel of your device and full administrator (root) privileges.

So should you use anti-malware software on an Android device? If you only install apps from the Google Play Store, the probability of your Android device being penetrated is remote. However, when (not if) an attack is made on Android, how will the system protect itself? For this reason I'd rather err on the side of caution and have anti-malware installed on my own Android devices.

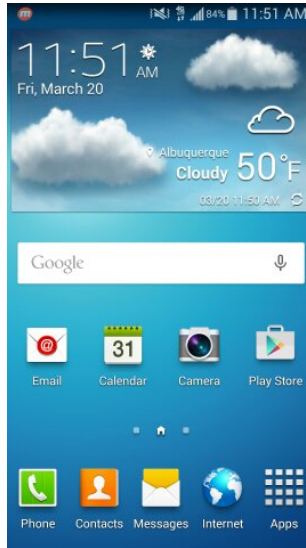
Looking through the Play Store we find the *Bitdefender Mobile Security & Antivirus* <<http://www.Bitdefender.com/solutions/mobile-security-android.html>> is the anti-malware that I recommend over all else.

## 1. Vulnerability: Device

### **Assignment: Install & Configure Bitdefender Mobile Security & Antivirus**

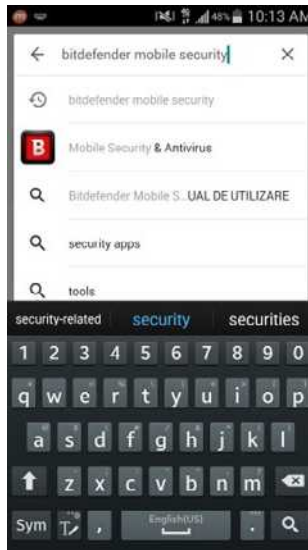
In this assignment, you download, install, and configure *Bitdefender Mobile Security & Antivirus* for your Android device.

1. From your Home Screen, select *Play Store*.



## 1. Vulnerability: Device

2. Type Bitdefender Mobile Security at the top search bar and Select Mobile Security & Antivirus.

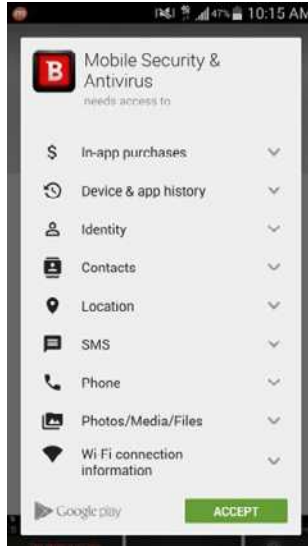


3. Select *Install*.



## 1. Vulnerability: Device

4. *Accept* the access requirements.

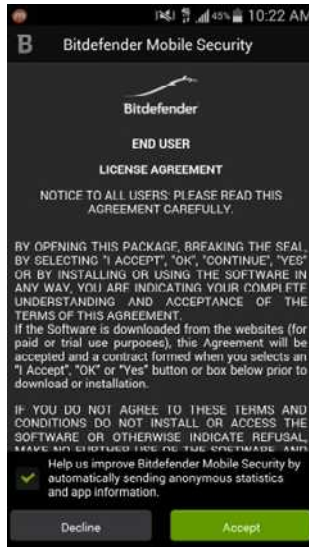


5. Once the download has finished, select *Open*.

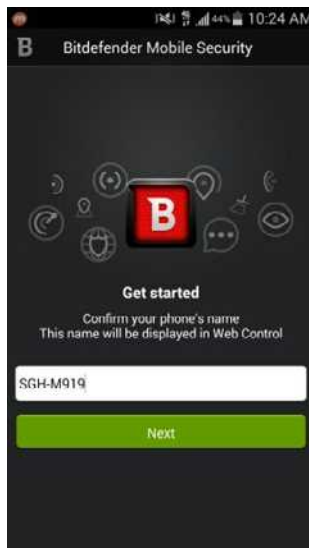


## 1. Vulnerability: Device

6. Select *Accept* to accept the license agreement.

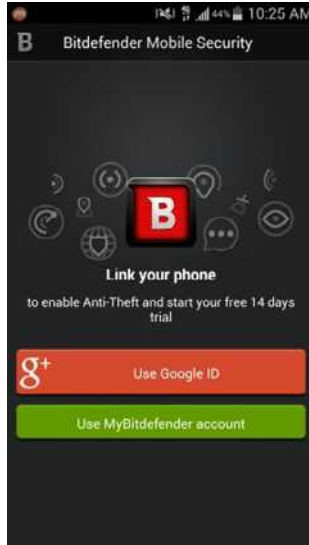


7. Select *Next* to accept your current phone name and use it in *Bitdefender*.

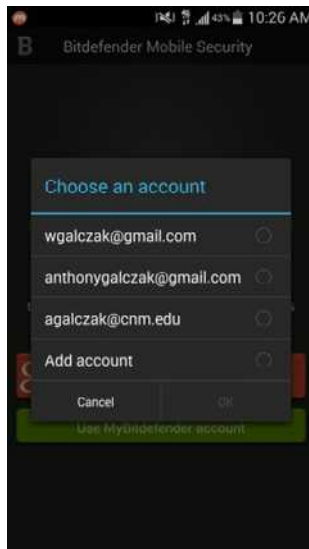


## 1. Vulnerability: Device

8. Link your phone to *Bitdefender* to use anti-theft services. Select *Use Google ID*.



9. Select the Google ID you'd like to use and then select *OK*.



## 1. Vulnerability: Device

10. Select the version of *Bitdefender* you would like to use. If you want to try *Bitdefender* out select *Trial Version* otherwise select *Full Version* or if you have a key already select *I already have a license*.



Congratulations! You have installed and configured *Bitdefender Mobile Security & Antivirus*.

### **Assignment: Scan for Malware with Bitdefender**

Once *Bitdefender Mobile Security & Antivirus* is installed and configured, you are able to perform on-demand scanning of documents.



## 1. Vulnerability: Device

1. From your Home Screen, select *Antivirus*.

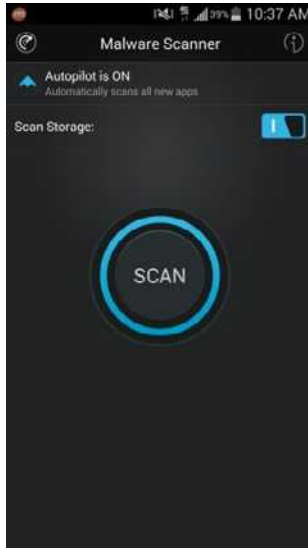


2. Select *Malware Scanner*.

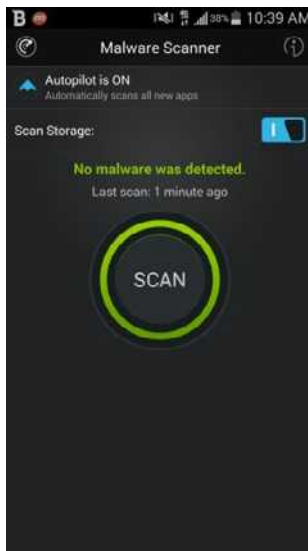


## 1. Vulnerability: Device

3. If you would like to scan your SD card in addition to your phone, leave the *Scan Storage* item lit up blue otherwise select it to turn it off. Select *Scan*.



4. After the scan completes, resolve any found malware. If it displays *No malware was detected*. Congratulations, your device is malware-free!



## 1. Vulnerability: Device

### **Assignment: Restrict Access to Applications using Bitdefender's App Lock**

If you will be loaning your Android device to someone else, or perhaps giving one to a child, give some thought to restricting access to the device. In most situations, only the device owner should have full access—if for no other reason than to prevent unintended and accidental damage.

*Bitdefender* allows the owner to use *App Lock* to restrict access to certain applications.

1. From the Home Screen, select *Antivirus*.

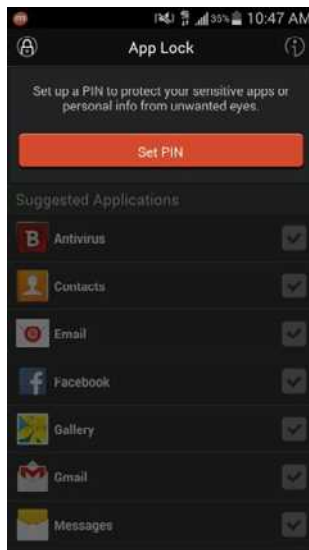


## 1. Vulnerability: Device

2. Select *App Lock*.

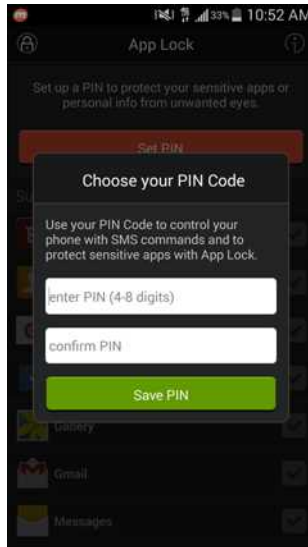


3. Select *Set PIN* to setup a PIN for *App Lock*.

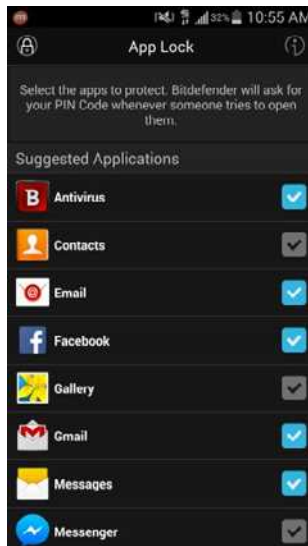


## 1. Vulnerability: Device

4. Enter a secure *PIN* twice and select *Save PIN*.



5. Select the applications you would like to lock. Whenever someone (or yourself) tries to open this app *Bitdefender* will ask for the PIN you've setup.



### Backups

Data loss is a very real fact of life. It is not a matter of *if* you will experience data loss, just a matter of *when*, and how often. Only a small percentage of computer users back up on a regular basis. Far fewer backup their Android devices. I suspect these are the folks who have experienced catastrophic data loss and never want a repeat.

There are many sources of data loss for Android devices. The top contenders include:

- Device theft
- Fire
- Water damage. I don't think a month goes by without a call from a client with water damage to a smart phone from reaching to flush a toilet
- Entropy/aging of the device
- Static electricity
- Physical shock to the device (banging, dropping, etc.)

If we were discussing computers, industry Best Practices call for at least one on-site backup and at least one off-site (typically Internet) backup. To date there are no Best Practices developed for smartphone and tablet devices, but when there is, it's sure to mimic their larger brothers.

Fortunately, Google has built-in the ability to perform Internet-based backups. You may use just the cloud-based backup or additionally use your brand's backup software to store a local copy as well.

The local backup is performed through Samsung Kies. The advantage is that it is highly customizable and can back up nearly everything including your text messages. The disadvantage is a high vulnerability to loss of the backup through fire, theft, etc.

The Internet backup is performed with Google. The advantages are minimal vulnerability to loss, and it is backed up by default. The disadvantage is that only data is backed up, not apps. These will need to be downloaded manually again

## 1. Vulnerability: Device

from the Play Store, however your app data for most apps will be saved. Also, many people aren't thrilled with handing their data over to any corporate entity for "safe keeping."

### **Assignment: Backup to Google**

In this assignment we will configure our Android device to backup to Google on a regular basis if it is not configured for Sync.

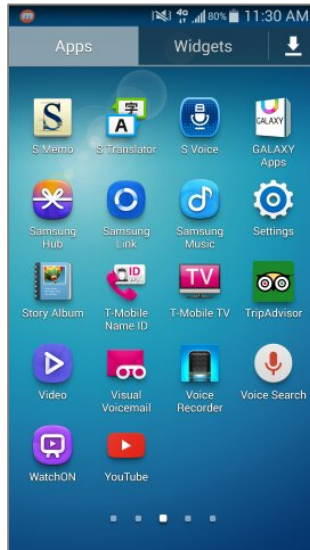
- Note: Backing up to Google will save most App data, however it will not save the device state such as the actual applications, text messages or data on the SD card.

1. From your Home Screen, select *Apps/Applications*.

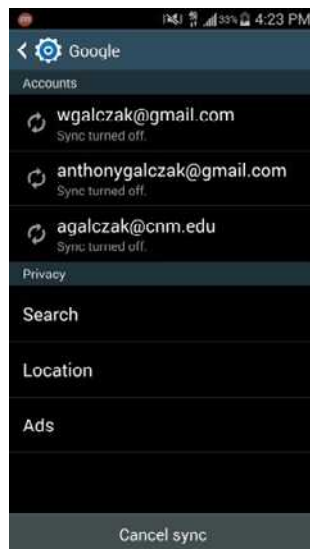


## 1. Vulnerability: Device

2. Select *Settings*.



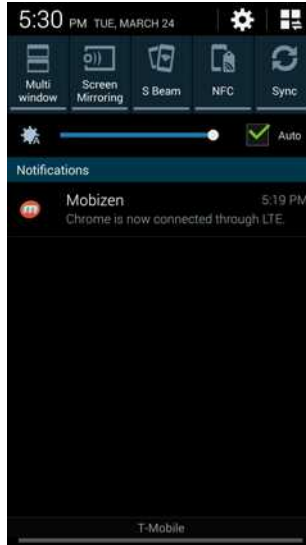
3. Select Accounts > Google.



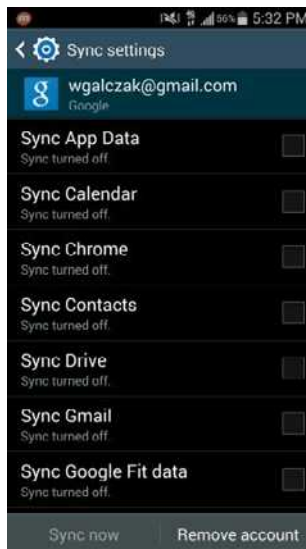


## 1. Vulnerability: Device

4. If you do not have double green arrows, you need to turn on sync. Use the Pull-Down Menu to select *Sync*. If the green arrows are present, congratulations you're already backed up!

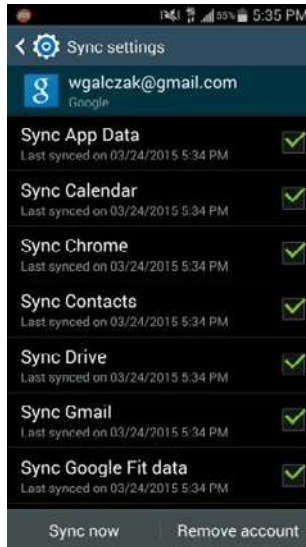


5. Remove the Pull-Down Menu, and then select each box you'd like to back up.

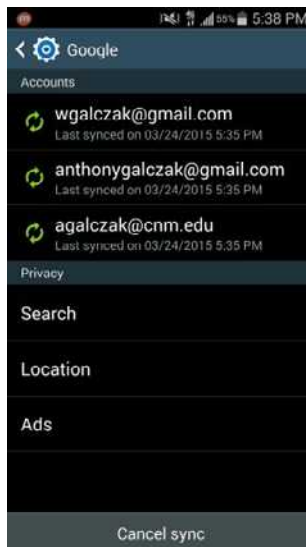


## 1. Vulnerability: Device

6. After your device has synced, verify it is current with today's date and time.



7. Press the *Back* button and verify you now have double green arrows on the email address you'd like your backup to be on.



Congratulations, you are now backed up to your Google account!

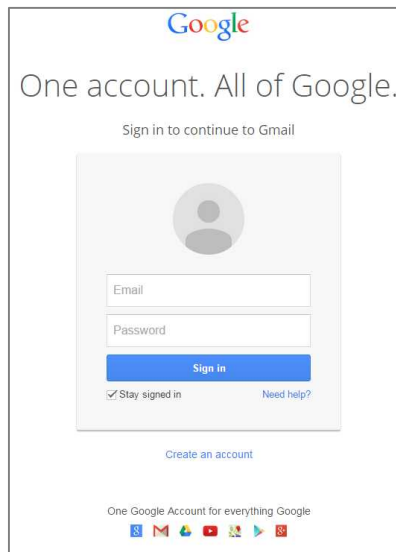
## 1. Vulnerability: Device

### Assignment: Verify the Google Backup via a Computer

All too often my clients *believe* they have done all that is necessary to have working backups, only to discover something went bad. It's important to verify your backup occasionally. You are already able to verify the time in which your backup was done in the Google accounts screen, however when addressing the most important types of data you can never be too cautious.

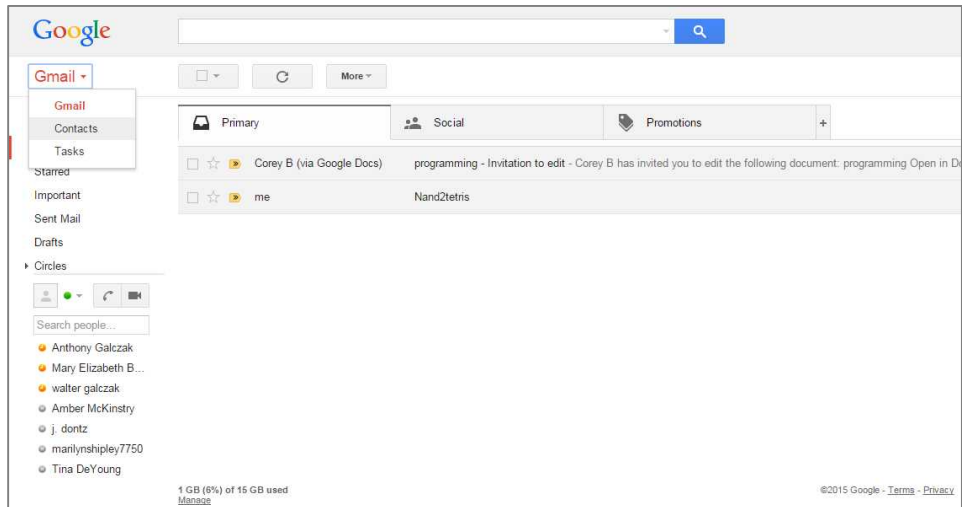
In this assignment, we will verify our Google backup via a PC to verify the most important types of data such as contacts and calendar items.

1. Log into your computer and open a browser. Navigate to gmail.com, and then click *Sign in*.



## 1. Vulnerability: Device

2. Click on Gmail in the upper left, and then select *Contacts* or browse to [www.contacts.google.com](http://www.contacts.google.com).



3. Verify your contacts are all listed in this area.
4. Now we are going to verify calendar items. Browse to [www.calendar.google.com](http://www.calendar.google.com). Make sure all your items are listed under your Calendar.

Congratulations! Your most essential data is backed up and available in the Google cloud.

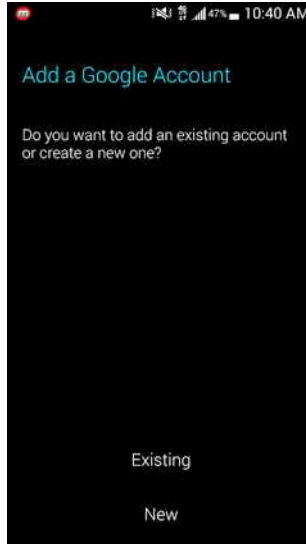
## Assignment: Data Recovery from Google

It is also possible to use a Google backup of an Android device to restore all data to another device.

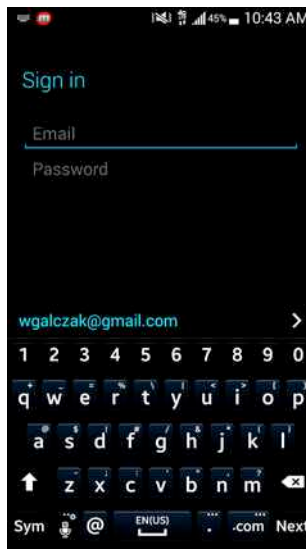
In this assignment we will see how to restore your data from a Google backup.

## 1. Vulnerability: Device

1. On a new Android device, or one that has no Google account you will be prompted to restore data to your device after entering your existing Google account information. Select *Existing* to use your existing Google account.

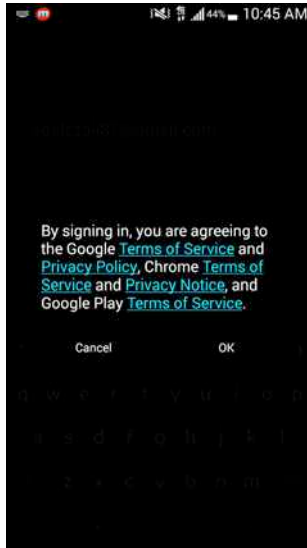


2. Enter your Google username and password and select the *right arrow* to continue.

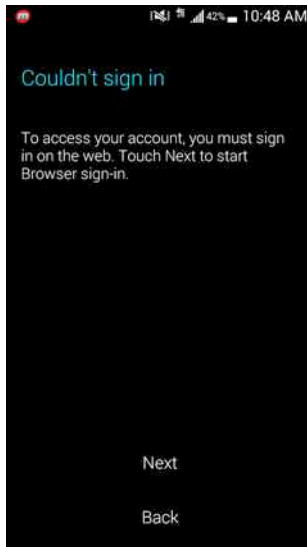


## 1. Vulnerability: Device

3. Gather your legal team in order to decipher the contract and then select *OK* to accept the Terms of Service and Privacy Notice.

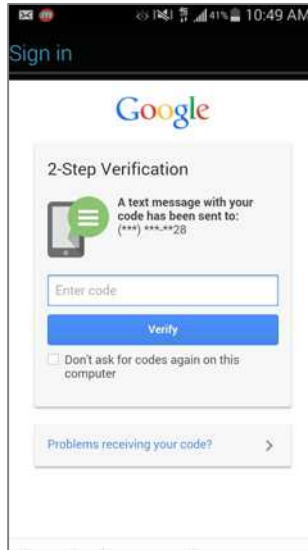


4. If you have not enabled *Google 2-Step Authentication*, skip to step 6. If you have configured *Google 2-Step Authentication*, you will be prompted to sign in on the web to authenticate your account. Select *Next*.

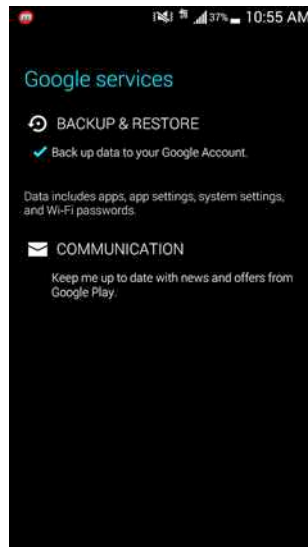


## 1. Vulnerability: Device

5. A web browser will open and a code will be generated and sent to you. Enter the code and select *Verify*.



6. Check the box under *Backup & Restore* and then select the *right arrow* to continue.



## 1. Vulnerability: Device

Your account is now setup on your device and will begin to sync. Depending on how much data you are bringing over this can take a few minutes up to an hour.



## Bitdefender Anti-Theft

On occasion an Android device is stolen. Ok, on *millions* of occasions they are stolen. Using *Bitdefender's Anti-Theft* feature you can remotely wipe your device data should it become lost or stolen.

But it would be nice to be able to get your device back.

*Anti-Theft* is a feature inside the Anti-Malware utility *Bitdefender* that we installed in an earlier activity. This utility locates your Android device on web map, often within a few feet. By passing this information along to your local police or sheriff, they will be able to get a search warrant to the address and recover your property.

For *Bitdefender Anti-Theft* to function, the following must happen:

- A *Bitdefender* account has been activated.
- *Anti-Theft* has been enabled for the device.
- The device is connected to the Internet via Wi-Fi or cellular.

### **Assignment: Activate and Configure Bitdefender Anti-Theft**

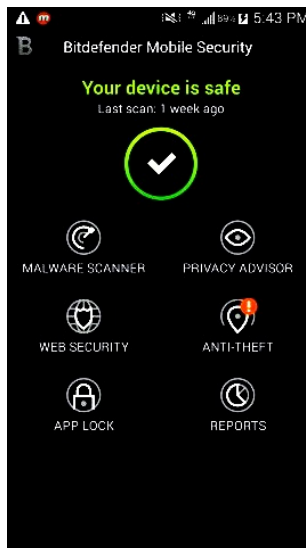
In this assignment we will activate and configure the anti-theft component within Bitdefender, which was installed in an earlier assignment.

## 1. Vulnerability: Device

1. From your Home Screen, select *Antivirus*.

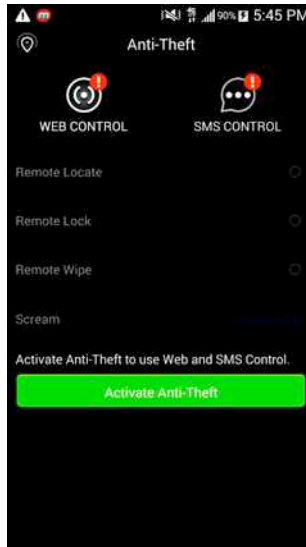


2. Select *Anti-Theft*.



## 1. Vulnerability: Device

3. Select *Activate Anti-Theft*.

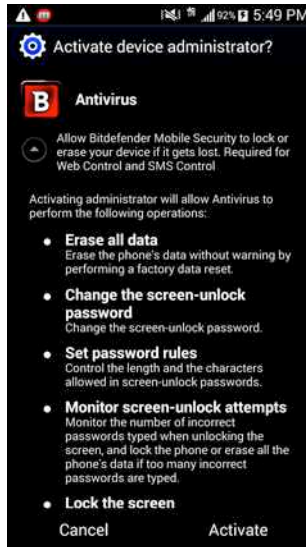


4. Select *OK, I understand*. If for whatever reason you need to uninstall *Bitdefender*, you will also have to revoke device administrator privileges.

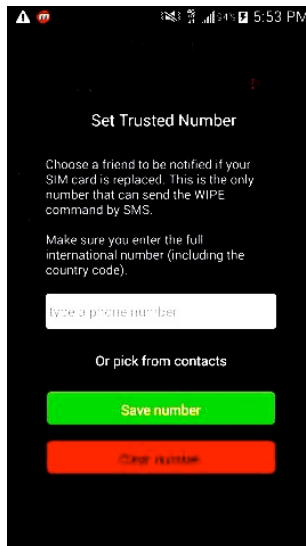


## 1. Vulnerability: Device

5. Select Activate.



6. Enter a trusted number for usage of the *Remote wipe* feature just in case your SIM card is replaced in your device. Select *Save number*.



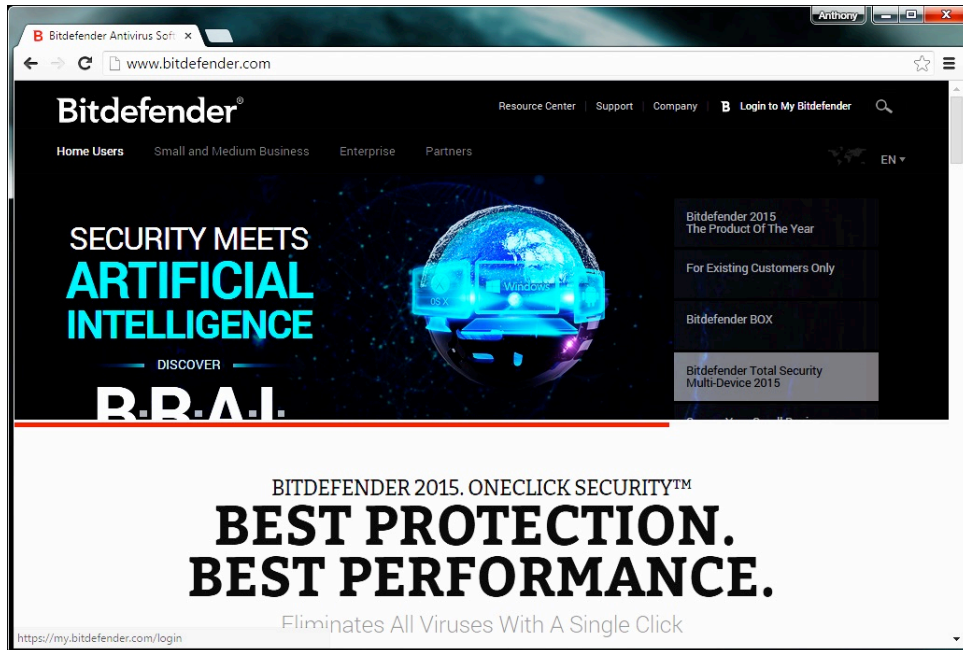
Your Android device is now continuously broadcasting to its GPS coordinates to your Bitdefender account.

## 1. Vulnerability: Device

### Assignment: Use Bitdefender to Find Your Device from a Computer

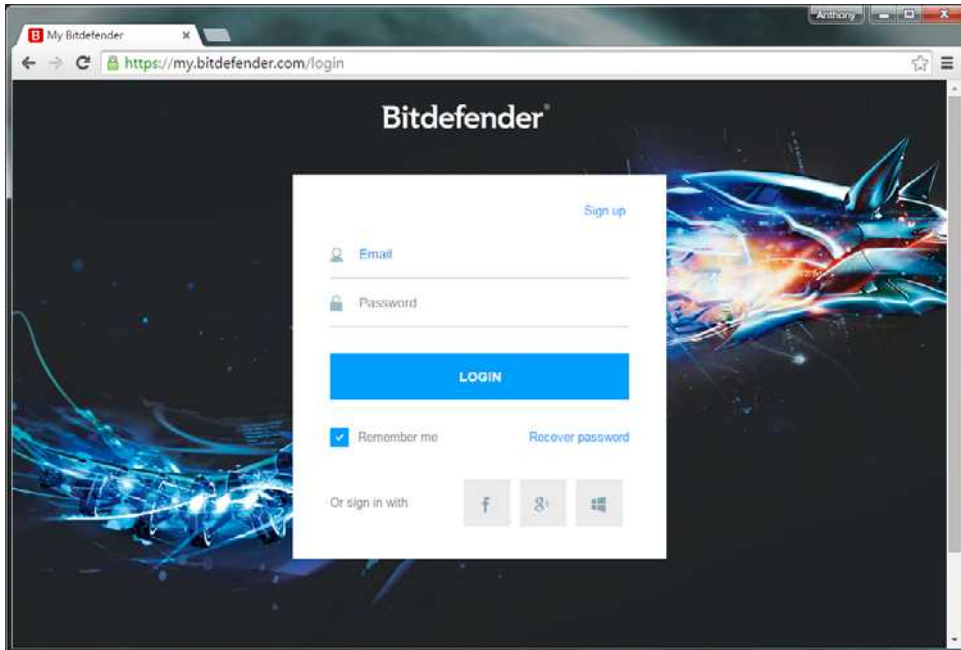
For the purposes of this assignment, let's assume someone has taken your Android device, and we will use *Bitdefender Anti-Theft* to locate it.

1. From any computer, open a browser and go to <http://www.Bitdefender.com>, and then click on *Login to My Bitdefender* at the upper right.



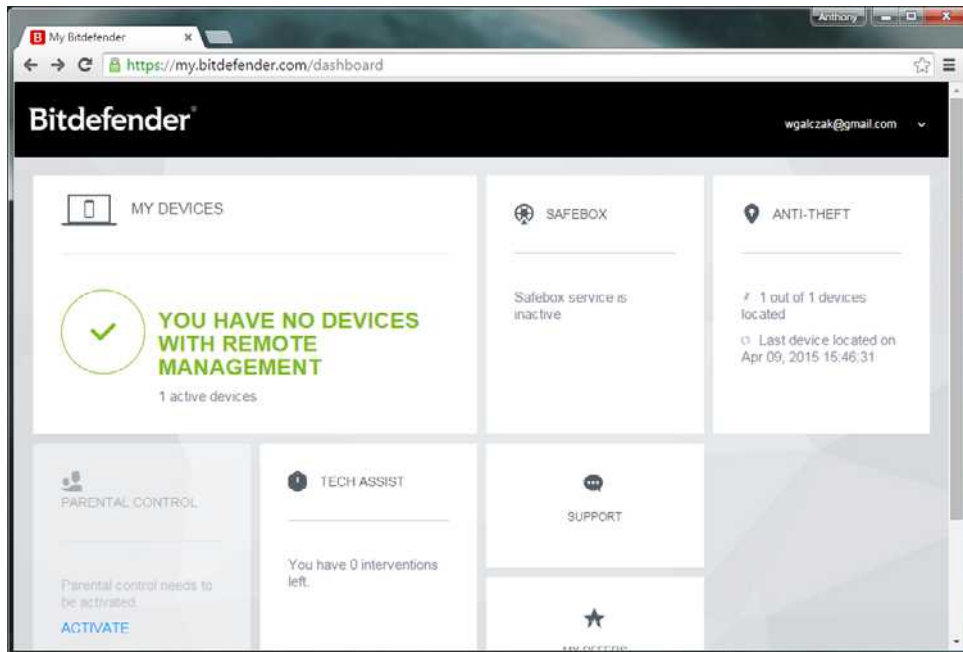
## 1. Vulnerability: Device

2. Enter your *Email* and *Password*, and then click *Login*.



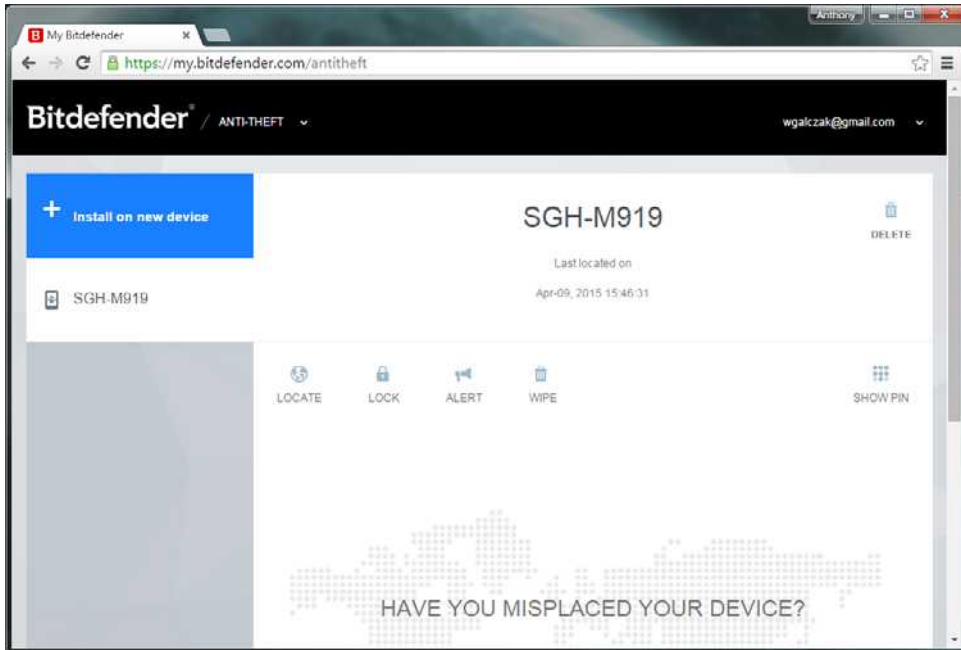
## 1. Vulnerability: Device

3. The Bitdefender dashboard appears. Click *Anti-Theft*.



## 1. Vulnerability: Device

4. On this screen you will see the different options you can do with your device.



- *Locate*. This will locate your device and put a “pin” on Google Maps showing exactly where your device is
  - *Lock*. This will lock your device and request a passcode you set to be entered in order to access your phone.
  - *Alert*. This will sound a buzzer on your device for you to locate and also display a custom message when you unlock the phone.
  - *Wipe*. This will wipe the entire contents of your device.
5. After making your selections, save your work and close out of the page.



## 1. Vulnerability: Device

### Preparing an Android Device for Sale

The time comes when all good things must come to an end. This is just as true for your beloved Android device. But, your device holds all of your documents, passwords, pictures, web browsing history, etc. Not the items you would like someone else to see. Even if you are tossing your device into the trash, there is the very real probability that someone will find it and harvest your data.

So before selling, giving away, or trashing your device, all data must be made inaccessible.

### Assignment: Securely Erase an Android Device

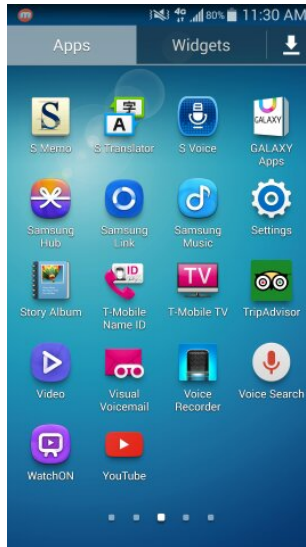
When performing a factory reset on an Android device, the device will delete the /data, /cache folders, but will leave your system files (your phone updates/OS) and your SD card info. If you do sell your device, make sure to secure your SD card by removing it or separately formatting it, as a factory reset will not by default erase the SD card which is where your most precious data may be stored.

1. From your Home screen, select *Apps/Applications*.

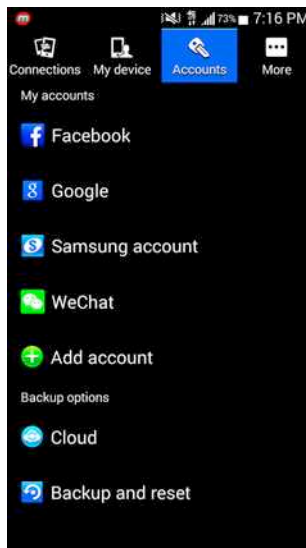


## 1. Vulnerability: Device

2. Select *Settings*.

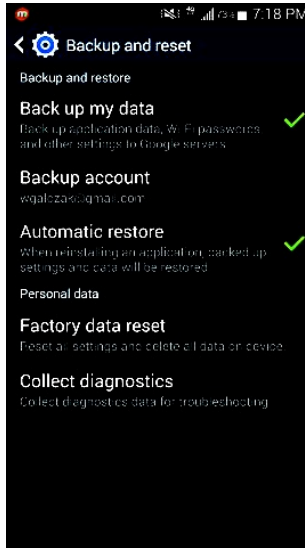


3. Select *Accounts > Backup* and reset.

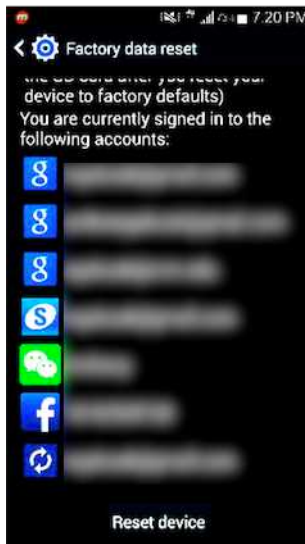


## 1. Vulnerability: Device

4. Make sure your *Back Up* information is valid and checked if you will use another Android device. Select *Factory data reset*.

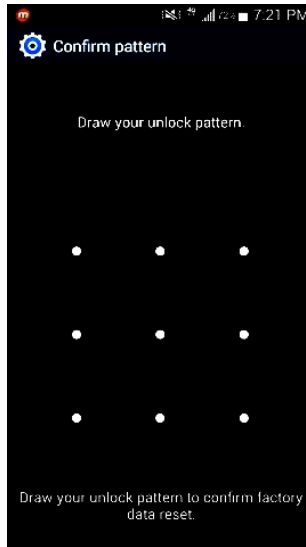


5. Scroll to the bottom of your listed accounts, and then select *Reset device*.

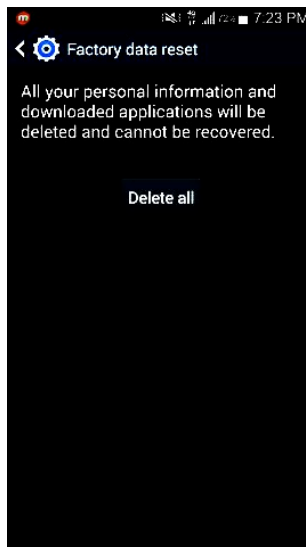


## 1. Vulnerability: Device

6. To confirm a factory reset, enter your authentication (PIN, Password, Pattern).



7. To continue with the factory reset, Select *Delete all*.
  - o Note: There is no going back, this will delete the data on your device.



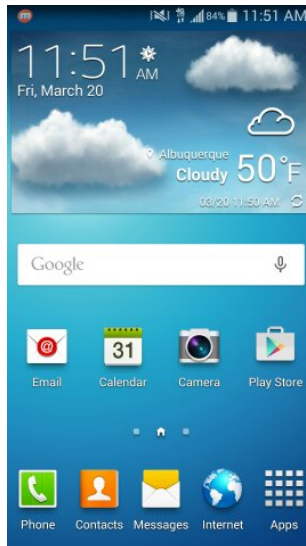
## 1. Vulnerability: Device

Depending on the model, speed and amount of data on the device, the process will take between a few minutes to an hour or more. Once complete, your device will restart bringing you to a Welcome screen. If you have an SD card that you are leaving in the device, then you will need to follow the steps for formatting an SD card (next).

### **Assignment: Format an SD Card**

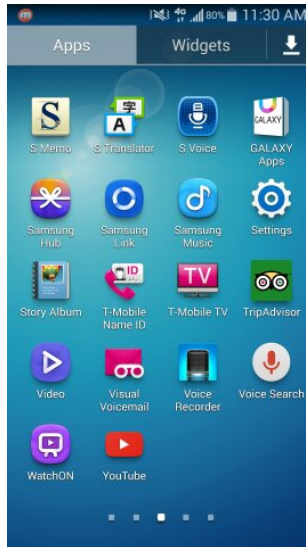
When securing a device for resale or just to clear sensitive data off from your device it is important to format your SD card. Your SD card will by default hold your music, pictures, videos and most personal data.

1. From your Home Screen, select *Apps/Applications*.

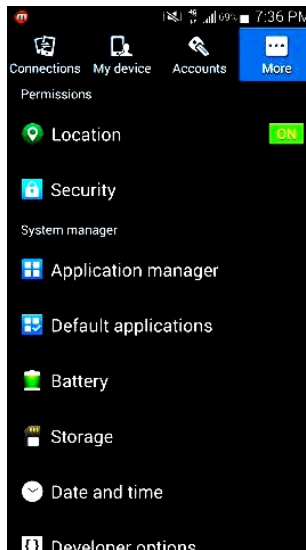


## 1. Vulnerability: Device

2. Select *Settings*.

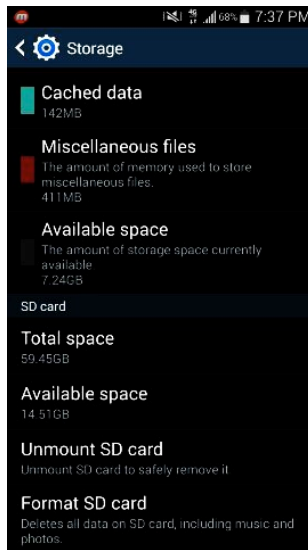


3. Select *More > Storage*.

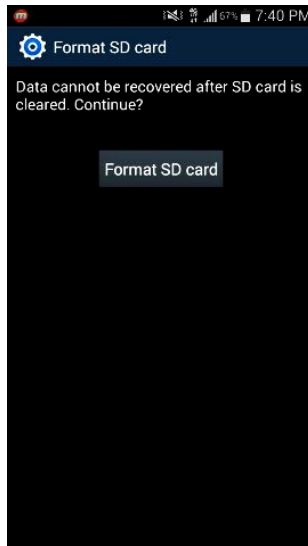


## 1. Vulnerability: Device

4. Scroll all the way down and select *Format SD card*.



5. Select *Format SD card*.



Congratulations! You have formatted your SD card and are now ready to factory reset your device.

## 1. Vulnerability: Device



## 2. Vulnerability: Network

*I am concerned for the security of our great Nation; not so much because of any threat from without, but because of the insidious forces working from within.*

–General Douglas MacArthur

### Wi-Fi Encryption Protocols

Right out of the box almost all Wi-Fi base stations are insecure. Anyone that can pick up the signal can connect. This allows them to see all of the other data—such as usernames and passwords—that are travelling on that network. When connecting to a Wi-Fi network with your Android device, it may be possible that the network is not encrypted, allowing all of your usernames, passwords, email, texting, and other data to be intercepted.

Although cellular networks do use encryption, the protocol in use has been broken for many years, making it easy for a novice hacker to see all the data passing on it. In addition, it is common practice for police and other government law enforcement agencies to set up their own cellular “towers” with the purpose of harvesting data.

In order to prevent your data from being seen while on a cellular network or an unencrypted Wi-Fi network, it is necessary to use VPN (Virtual Private Network) encryption (more on that later.) If the Wi-Fi network is properly encrypted, you should have little concern over the security and privacy of your data.

Below you will find the brief on each of the Wi-Fi encryption protocols.

**WEP** <[http://en.wikipedia.org/wiki/Wired\\_Equivalent\\_Privacy](http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy)> (Wired Equivalency Protocol) was the first encryption protocol for Wi-Fi. Introduced in 1999, it was quickly broken, and by 2003 was replaced by WPA and WPA2 (Wi-Fi Protected Access). Any Wi-Fi base station manufactured in the past 5 years will offer WPA and WPA2, in addition to WEP.

There is only one reason to ever use WEP—you simply have no other option. Kids driving by your home can likely break into your WEP network before leaving the block.

**WPA** <[http://en.wikipedia.org/wiki/Wi-Fi\\_Protected\\_Access](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access)> (Wi-Fi Protected Access) superseded WEP in 2003. Although it is a great advancement, it too has been broken. As with WEP, the only reason to use WPA is that you have no other option.

**WPA2** is the only protocol considered secure. WPA2 <[http://en.wikipedia.org/wiki/Wi-Fi\\_Protected\\_Access](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access)> superseded WPA in

## 2. Vulnerability: Local Network

2004. Although in the past year WPA2 has been broken, it is very difficult to do, and with strong passwords or with 802.1x still provides military-grade protection for your wireless networks.

There are two encryption algorithms that can be used—*TKIP* and *AES* (technically known as *CCMP*, but virtually all vendors refer to it as *AES*.) *TKIP* has been compromised and is no longer recommended. If your Wi-Fi device allows the option of *AES*, use only that. If it only allows for *TKIP*, trash the unit and purchase a more modern device.

### Firewall

If you have ever used a Windows PC and had to deal with any security issues, one of the biggest questions that come up is “Is your firewall on?” This question is valuable and a firewall is a mandatory step of security in your arsenal of tools against the bad guys. When using applications or browsing on any device, it will use “ports” in order to connect to certain services throughout the connection. Think of these ports like either open or closed doors on your device along with all of the good or bad things that come along with doors. In a Windows PC, the ports are generally open or listening depending on your configuration and this poses all kinds of risks, which can generally be fixed by using a firewall.

The good news is that on an Android device the ports are closed by default. Another potential security risk that is resolved by a firewall is un-allowed access on applications that are already installed on your device. Not only does a firewall close all your ports (or doors) for you, it will alert as to whom or what is coming out of those ports and also allow you to grant or deny access to the outside world.

One generally bad part about using a firewall on an Android device is that it commonly requires you to “root” your device. Rooting your device from a security standpoint is a very risky and inadvisable thing to do,. One way around this is to create a virtual network or a pseudo-VPN that routes your traffic for you and then allow or disallow traffic from there. There is such an application, called *NoRoot Firewall*. As the name suggests, it does not require a root and uses a rather ingenious way to create a firewall on your Android device. In addition, you are able to create custom filters on this application that will allow you to automatically set what can and cannot enter or leave your device making this application an invaluable tool for security.

## 2. Vulnerability: Local Network

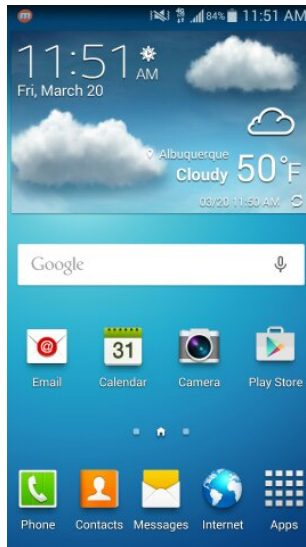
### NoRoot Firewall

NoRoot Firewall is our pick for best application to successfully limit incoming and outgoing traffic on your Android device. The best part about this particular application is that it is not necessary to root your device thereby not opening yourself up to a whole bevy of security risks. In these assignments, you will install the application, set up the configuration of the application, and then set filters for proper firewall use.

### Assignment: Install and Configure NoRoot Firewall for Android

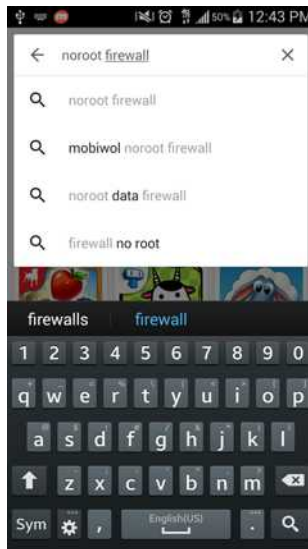
In this assignment we will install NoRoot Firewall from the Play Store.

1. From your Home Screen, select *Play Store*.

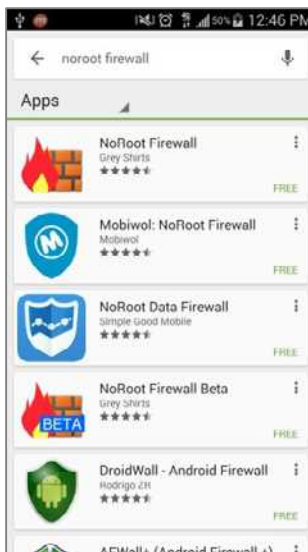


## 2. Vulnerability: Local Network

2. Select the Google Play search bar and search for *NoRoot Firewall*.



3. Select *NoRoot Firewall*.

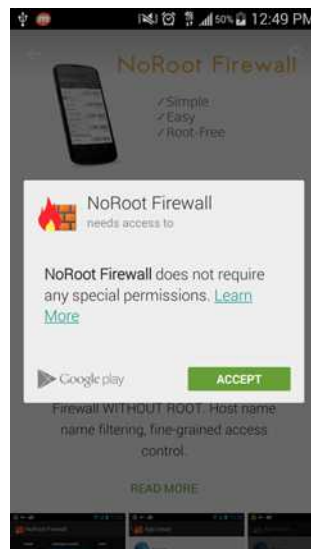


## 2. Vulnerability: Local Network

4. Select Install.

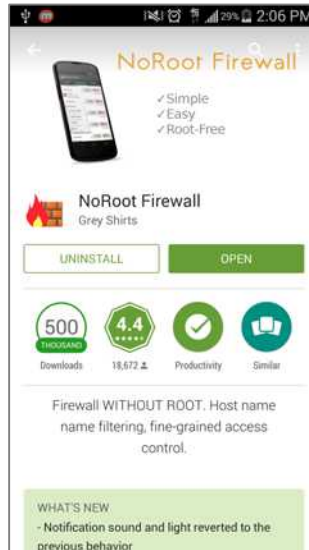


5. *Accept* the access requirements.

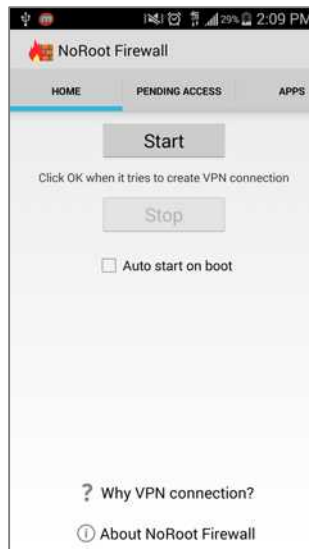


## 2. Vulnerability: Local Network

6. Select *Open*.



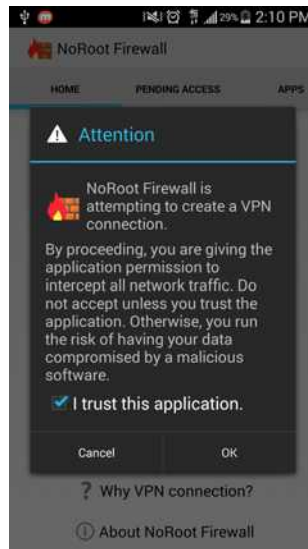
7. In order to use NoRoot Firewall you will have to create a pseudo-VPN connection. Select *Start* to enable this connection.



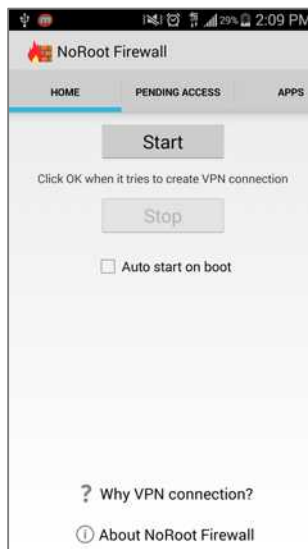


## 2. Vulnerability: Local Network

8. Enable the check box for *I trust this application*, and then select *OK*.



9. When using a firewall, it is most effective if it is always on. Check the box for *Auto start on boot*.

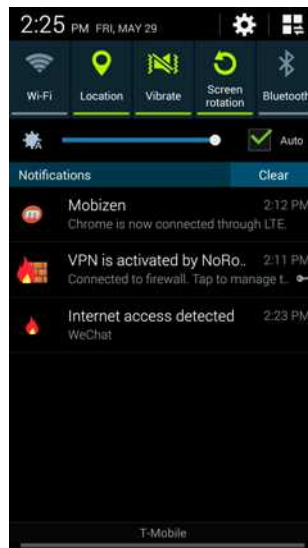


## 2. Vulnerability: Local Network

### **Assignment: Allow an Application Access with NoRoot Firewall**

When using NoRoot firewall one of the things that you will notice is that by default your applications do not have access to use the Internet for incoming or outgoing connections. It is important to be aware of which applications you would like to give access to. There are a few ways to enable access for applications. We will cover all of the different ways to allow your applications to use incoming and outgoing connections.

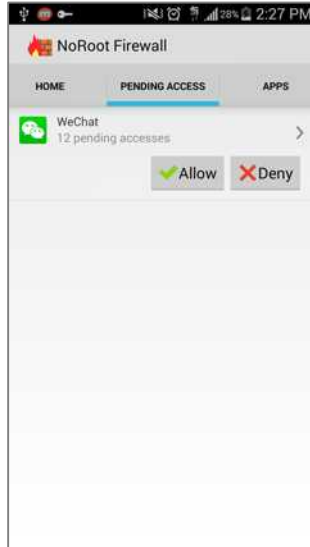
1. If an application has been denied and is requesting access, you will see a little flame in the notification bar. The first way to enable a specific instance of access is by selecting the Pull-Down Menu > *Internet access detected*.



## 2. Vulnerability: Local Network

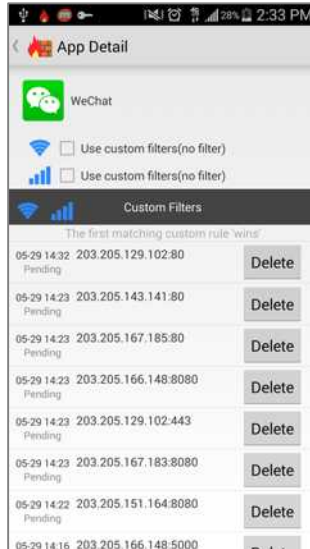
2. This will bring you to the application that has requested access. Select the application's name in order to see what access the app has requested and exactly where it is talking. If acceptable, select *Allow*.

If this is not an application you are familiar with, or is not a pre-included application for your phone brand or Google (Think Samsung Hub or Google Hangouts) then you may want to deny access to this application for your safety.

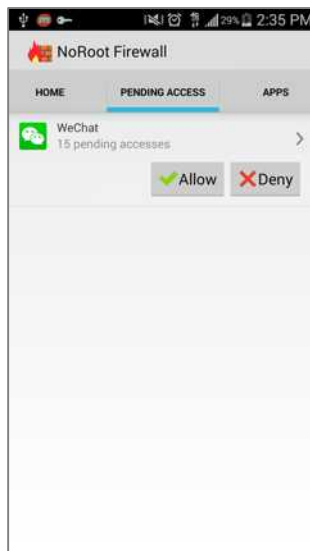


## 2. Vulnerability: Local Network

3. Notice all the IP addresses, port numbers and timestamps listed. This gives you an enormous amount of data regarding what, when, and how your devices connection is being used. Press the *Back* button to go back.



4. If considered safe, select *Allow* to allow that application for Wi-Fi and mobile data.

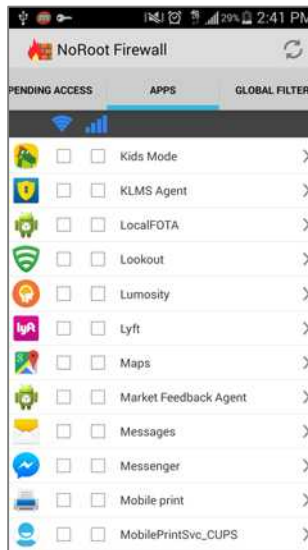


## 2. Vulnerability: Local Network

5. Another way to grant access to an application is to find it in the app list and pre-emptively grant it access. Select the *Apps* tab in the upper right.

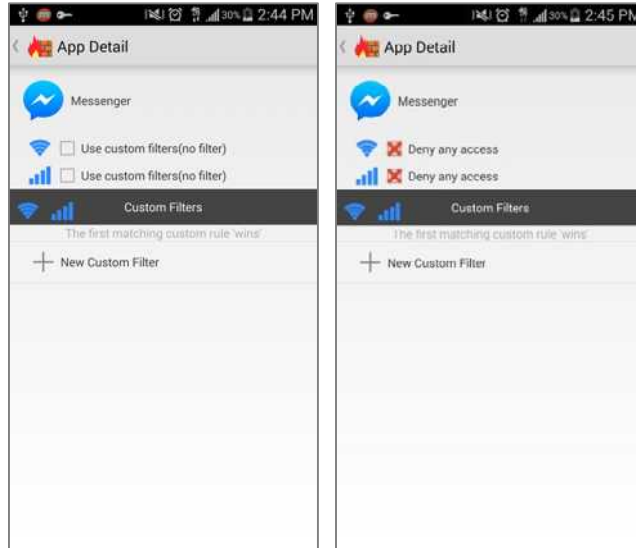


6. Scroll down the list to find the app to be granted access, and then select that application. For this example, I've selected *Messenger*.



## 2. Vulnerability: Local Network

7. Under the application you will see two icons. First is Wi-Fi, second is mobile connection. Check the box once to *allow*, twice to *deny*, or three times to go back to no custom filters for this application. Check both boxes once to *allow*.



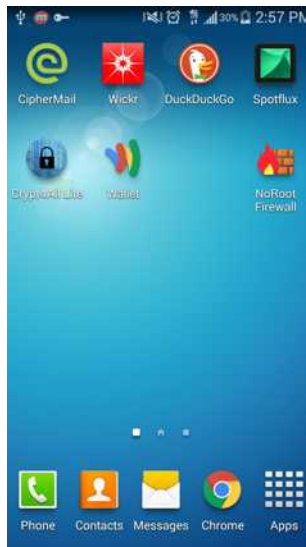
Congratulations! You have given your chosen application rights to access your incoming and outgoing connections.

## 2. Vulnerability: Local Network

### **Assignment: Use Global Filters and Access Log with NoRoot Firewall**

NoRoot Firewall is a very powerful firewall tool that allows you to set IP-level or even domain-level filters for access or denial. It also has a great little section including an access log that can give an in-depth analysis on your network usage. This is not an advanced networking book so I will not delve deeply into the specifics on how to setup filters at a specific level or what port to enable or disable, but I will show you how to access these menus and where you would go to set these filters up if you so choose.

1. From the Home Screen, select *NoRoot Firewall*.

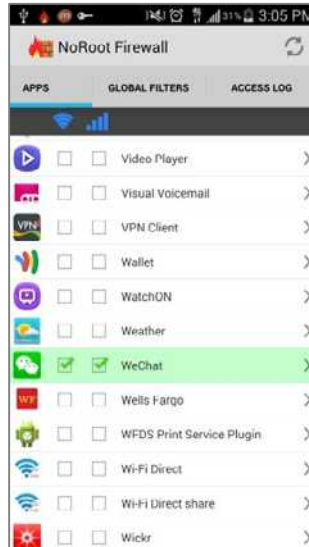


## 2. Vulnerability: Local Network

2. Select *Apps*.



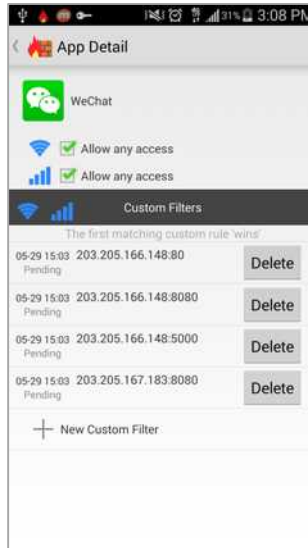
3. Select the application to have a custom filter set.



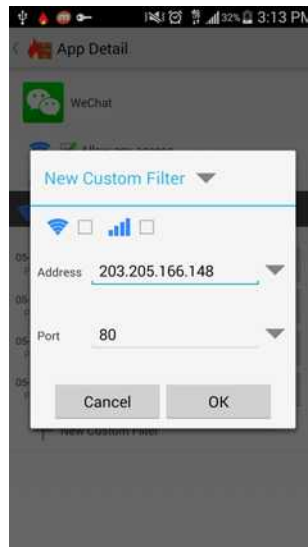


## 2. Vulnerability: Local Network

4. Select one of the IP addresses listed to configure it. You would do this to allow access for this application, but restrict one particular IP address.

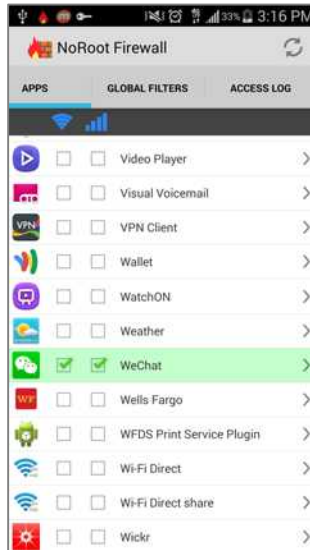


5. From here you can restrict or allow according to Wi-Fi or mobile data, octet level, or port number. Make your changes, and then select OK.

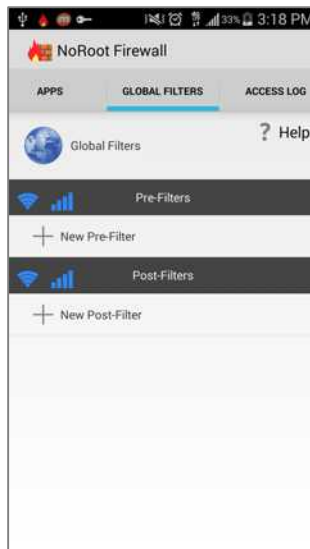


## 2. Vulnerability: Local Network

6. Press the *Back* button and then select *Global Filters*.

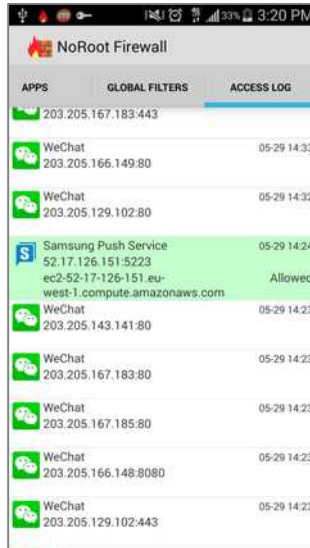


7. In this screen you may configure any pre or post-filters for your device's traffic, and then select *Access Log*.

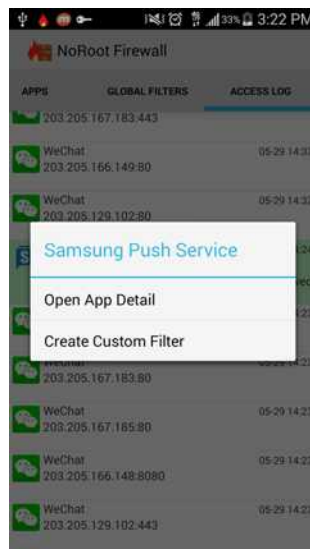


## 2. Vulnerability: Local Network

8. This is my favorite part of this firewall. You can view your individual connections as they are being made. If you see a suspicious connection, select it.

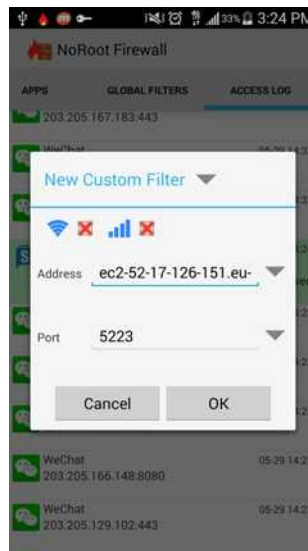


9. When you click on that connection, you have the option to open the app's specific details and filters, or create a custom filter. Select *Create Custom Filter*.



## 2. Vulnerability: Local Network

10. Select the two checkboxes twice in order to *deny* this connection, and then select *OK*.



Congratulations! You have blocked this specific connection from future access. If you have to block a particular application or IP address, NoRoot Firewall is perfect for this task.

Keep in mind when using a firewall that a lot of these concepts can get complicated very quickly. Worry not. Setting up and using a firewall is quite easy. If you are interested in using a firewall—and I do advise it for comprehensive security of your device—all that need be done is to install NoRoot Firewall, start the VPN service and be watchful of anything that requests access. If something unfamiliar asks for access, think before approving. This may be the connection that ruins your week with a data breach.

### 3. Vulnerability: Web Browsing

*Distrust and caution are the parents of security.*

–Benjamin Franklin

Due to an extraordinary marketing campaign, everyone knows the catchphrase: *What happens in Vegas, stays in Vegas*. With few exceptions, web surfers think the same thing about their visits.

Most websites use HTTP (Hypertext Transport Protocol) to relay information and requests between user and website and back again. HTTP sends all data in clear text—anyone snooping on your network connection anywhere between your computer and the web server can easily see everything that you are doing.

Typically, the only exceptions you will come across are financial and medical sites, as they are mandated by law to use HTTPS (Hypertext Transport Protocol Secure). HTTPS uses the SSL (Secure Socket Layer) encryption protocol to ensure that all traffic between the user and server is military-grade encrypted.

Although it is unlikely that you would ever be in the position to enter your password or bank account into an unsecure web page, you are almost guaranteed to enter your identity information, such as full name, address, phone number, and social security number. It is almost effortless for an identity thief to copy this information.

### 3. Vulnerability: Web Browsing

## Browser Security

Due to the extra features and capabilities that come along with it, I recommend that you use *Google Chrome* as opposed to *Internet*. Although Google Chrome is safe, the same can't be said for some websites. The good news is that you are able to protect yourself with the proper configuration.

### Assignment: Configure Google Chrome Settings

In this assignment we will configure *Google Chrome Settings* to provide a safer web browsing experience.

1. From your Home Screen, select *Apps/Applications*.

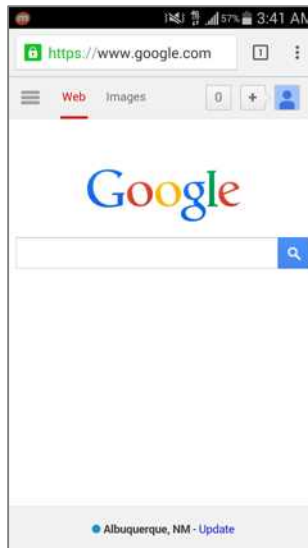


### 3. Vulnerability: Web Browsing

2. Select *Chrome*.

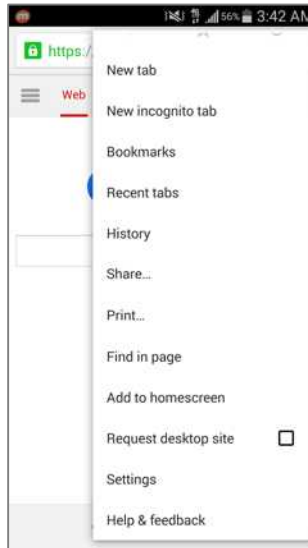


3. Select the *Menu* (3 dots) button in the upper right.

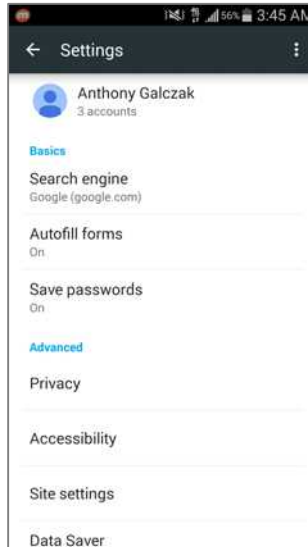


### 3. Vulnerability: Web Browsing

4. Select *Settings*.



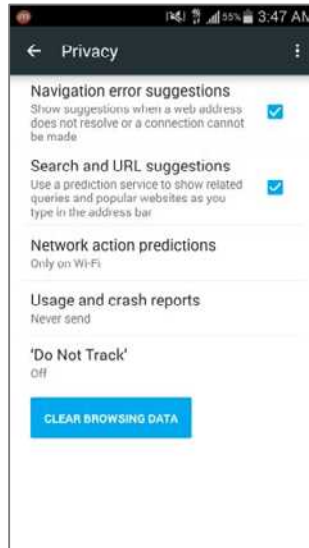
5. Select *Privacy*.



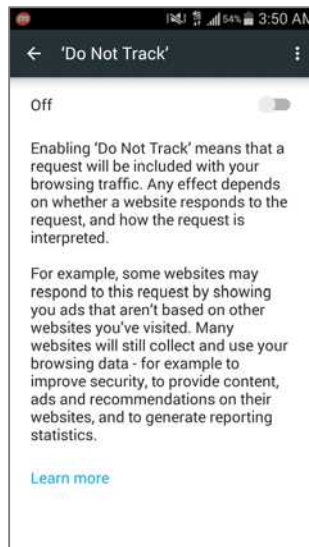


### 3. Vulnerability: Web Browsing

#### 6. Select Do Not Track.

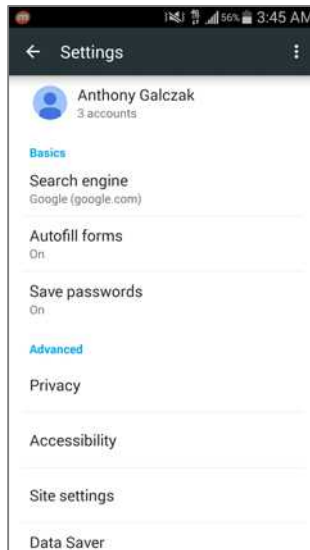


#### 7. Select *Off* or the drag the slider on the upper right to the right to turn *Do Not Track* on..

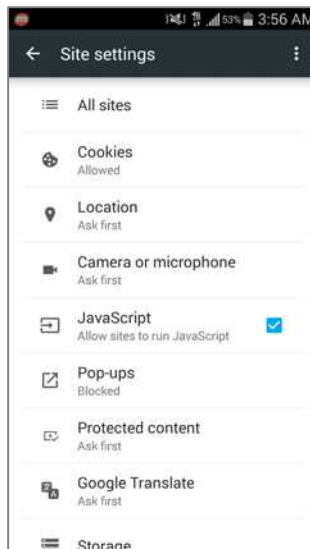


### 3. Vulnerability: Web Browsing

8. Press the *Back* button twice until you return to the *Settings* menu, and then select *Site Settings*.



9. Select Cookies.

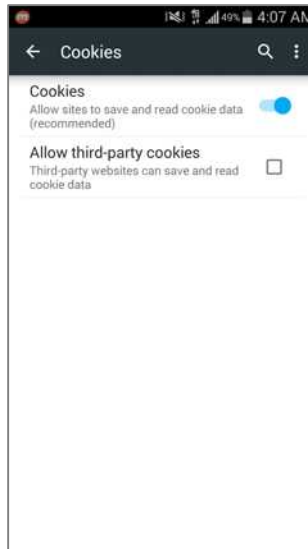


### 3. Vulnerability: Web Browsing

In the *Cookies* screen, you get to decide how cookies will be dealt with. A cookie is a file sent from the web server to the browser. It was originally intended to provide for a more intelligent, welcoming experience. For example, when I visit Amazon.com, the Amazon server sends a cookie to my browser of my likes. On my next visit, it's likely I'll be welcomed to a screen offering the latest in my personal likes.

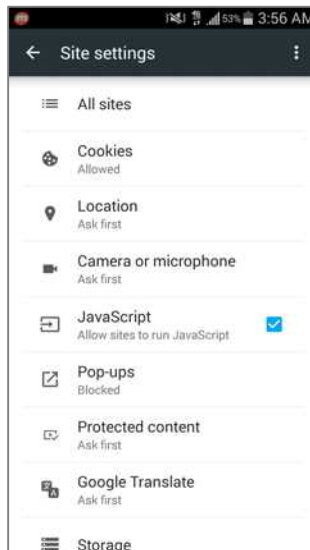
Unfortunately, it is just as likely that this information is passed along to other sites. Eventually, your cookies will be seen by many sites. Some of them adding to the cookie along the way. This can be a significant security concern.

10. Select your choice, and then press *Back* once to go back to *Site Settings*.



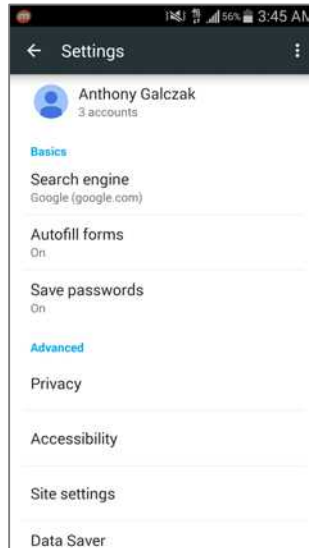
### 3. Vulnerability: Web Browsing

- *Allow sites to save and read cookie data.* This is to allow cookies to be saved and read, but does not affect third-party cookies which I recommend turning off.
  - *Block all sites.* Never allows acceptance of a cookie from any web server. This will prevent sharing of this level of information. However, some sites allow visits only if cookies are allowed.
  - *Allow third-party cookies.* Turning this option off will allow cookies from all the websites that you visit, but will not allow any 3<sup>rd</sup> party sites to get in the action. I recommend that you turn off this setting.
11. Take note of the *JavaScript* checkbox. JavaScript is a popular web development tool used to create forms, animations, interactivity, and occasionally to penetrate a device connected to the Internet. JavaScript presents a potential security hole, but it is also a necessary element for the proper viewing of some websites. You are the best judge of its necessity for you.



### 3. Vulnerability: Web Browsing

12. Select *Privacy*.



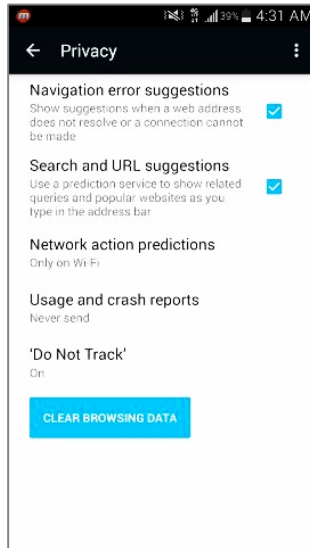
You just realized that: 1) Your mother is coming over, 2) You have been naughty on the web all day, 3) You did not turn on Incognito Browsing mode, 4) Your mom will want to play with your Android device, and will feel insulted if you don't let her: *Oh baby, I only need to check my AOL email. Just let me get on your phone for a minute.*

Is it time to panic? Not yet! You can erase your entire (steamy) Chrome history in one click.

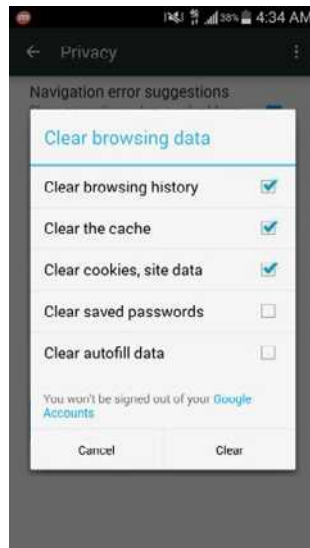
13. Selecting *Clear Browsing Data* will display a dialog box confirming what type of browsing data you'd like to delete.

### 3. Vulnerability: Web Browsing

#### 14. Select Clear Browsing Data.



15. Select the type of browsing data you'd like to delete, and then select *Clear*. You should not have to clear saved passwords or autofill data, but if you'd like you can select those as well.



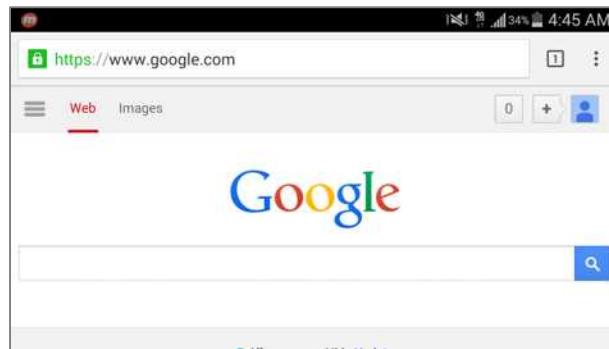
### 3. Vulnerability: Web Browsing

16. Select the *Back arrow* twice in the upper left to return to the browsing window. Whew, saved mom from a stroke.

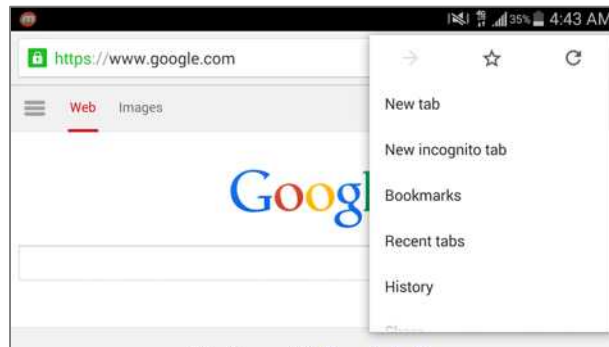
#### **Assignment: Google Incognito Mode**

Before we secure your website travels from roaming eyes out on the Internet, we should first be secure from the roaming eyes on the home front. By enabling the *Google Chrome Incognito* mode, no trace of your browsing history is recorded to your storage device. If you have secured your device to this point, it's unlikely that you also need to implement *Google Chrome Incognito Mode*. But just in case...

1. Open *Google Chrome*, and then visit any page. Note that when *Google Chrome Incognito Mode* is off, the Chrome toolbar at the top is white. Select the *Menu* (3 dots) button in the upper right.

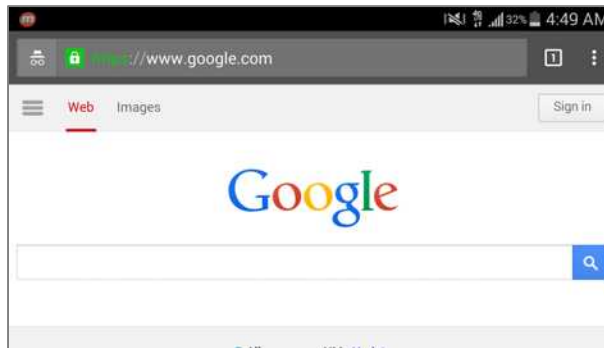


2. Select *New Incognito tab*.



### 3. Vulnerability: Web Browsing

3. *Google Chrome Incognito mode* is now active. The indicator that it's active is that all browser outlines and tabs are a dark grey and a hat with glasses is in the upper left corner.



4. As long as *Google Chrome Incognito mode* is active, Chrome will not keep a record of the pages visited, search history, or AutoFill data, however it will keep any files you download and any bookmarks created.



### 3. Vulnerability: Web Browsing

## Safer Internet Searches with DuckDuckGo

With most search engines, when you perform a search, your search criteria and sites visited are collected and stored by the search engine. Cookies assigned from one site can communicate with other sites and webpages you open. Not so with the *DuckDuckGo* search engine. You can use the *DuckDuckGo Search & Stories* application to open your private search in an external browser.

### Assignment: Install DuckDuckGo Search & Stories

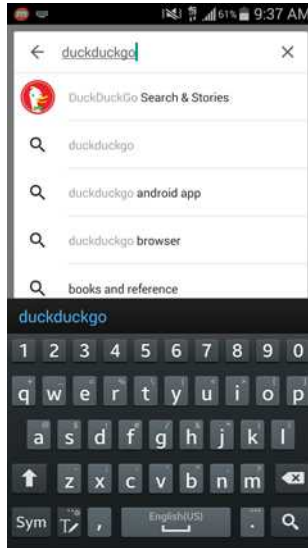
In this assignment, we will install the DuckDuckGo Search & Stories application from the Play Store

1. From your Home Screen, select *Play Store*.



### 3. Vulnerability: Web Browsing

2. Select the Google Play search bar and search for *DuckDuckGo*. Select *DuckDuckGo Search & Stories*.



3. Select *Install*.



### 3. Vulnerability: Web Browsing

4. *Accept* the access requirements.



5. After the download completes you have *DuckDuckGo Search & Stories* installed.

### **Assignment: Use DuckDuckGo to Search and Display in an External Browser**

In this assignment, you will use *DuckDuckGo Search & Stories* to do a private search in an external browser.

### 3. Vulnerability: Web Browsing

1. From your Home Screen, select *DuckDuckGo*.

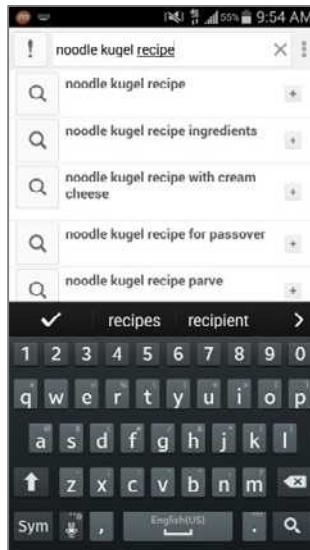


2. Select *Get Started*.



### 3. Vulnerability: Web Browsing

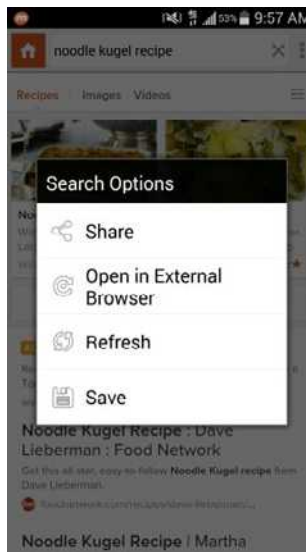
3. Select the *Search DuckDuckGo...* box at the top, type in your search, and then hit the *Search* button on the bottom right of the screen.



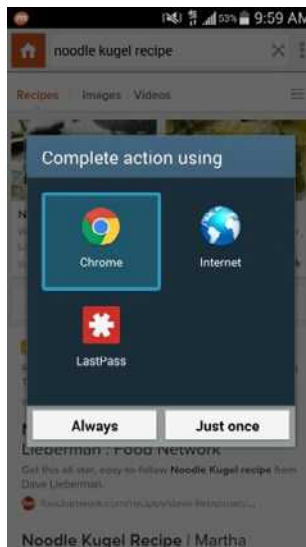
4. At this point you have successfully made a private search in *DuckDuckGo*. However if you'd like to open the search in another browser then continue along.

### 3. Vulnerability: Web Browsing

5. Select the *Menu* (3 dots) key in the upper right, and Select *Open in External Browser*.

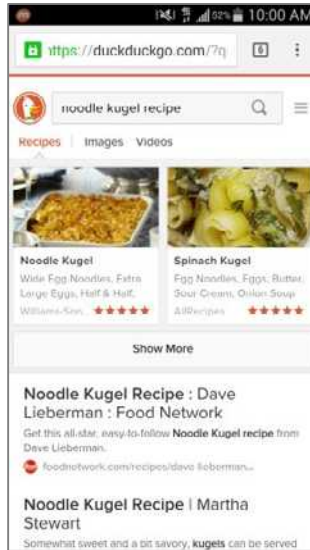


6. Select the browser you would like to use, and then select *Always*.



### 3. Vulnerability: Web Browsing

Congratulations! You have done a private search in *DuckDuckGo* and ported it over to the browser of your choosing.



When performing a search from DuckDuckGo Search & Stories, nobody will ever know how many sites you visited in order to learn my aunts secret recipe for Noodle Koogel.

### 3. Vulnerability: Web Browsing

## HTTPS: How to Know You Are in a Secure Web Page

The typical webpage is not encrypted. Any and all communications between you and the page are transmitted in human-readable format. Under normal conditions this doesn't present an issue.

However, if you are visiting a page where you need to enter sensitive or private information, you must have an encrypted page. Encrypted web pages communicate all data, user names, passwords, credit cards, etc. between itself and the visitor fully encrypted. Currently, almost all such pages use the *HTTPS* protocol. Anytime that you visit a web page that is secured using https, it will be reflected in the URL or address field of your web browser.

In the following example, I visit Wikipedia.org by entering *wikipedia.org* in my browser address field:





### 3. Vulnerability: Web Browsing

In the next example, I visit Wikipedia again, but this time I enter *https://www.wikipedia.org* in the address field. Note how the address field reflects that I'm now connected securely by displaying the lock icon.



Whenever visiting a page where you will be entering private or sensitive data, always verify that it is an encrypted page. If the page is not encrypted, try replacing the *http://* with *https://* for the URL, and revisit the page. If the browser reports an error, or if you are taken back to the *http://* version of the page, do not enter your data.

### 3. Vulnerability: Web Browsing

## TOR

If you are looking for the ultimate security against the NSA or even Billy across the street, then look no further. Tor is a non-profit organization whose main goals and interest is ultimate security for its users. When using Tor you are establishing a connection from one server to one server and so on until you end up hitting your end connection. The reason that this helps immensely with security is that whoever is tracking you will have a very difficult time finding from where the traffic originated.

Tor is a godsend for investigative journalists, those who live in countries with censorship laws, or even just a working professional who needs keep their data locked down. To read more about all of benefits of the Tor network and the Tor browser, visit <<https://www.torproject.org>>.

In order to use Tor on an Android device, an application created by the same developers—called *Orbot* <<https://guardianproject.info/apps/orbot/>>—must be installed. Orbot was developed for a much older Android version and therefore in the newer versions requires a root to work. However, with some new applications and configuring we will have the ability to use Orbot without opening yourself up to the risk of rooting your device.

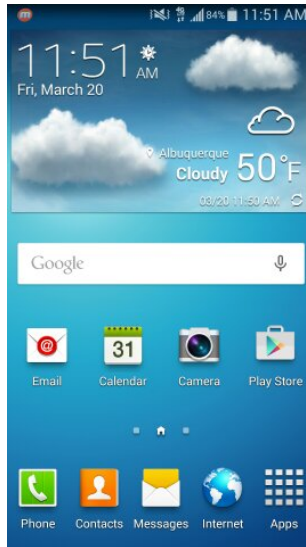
In order to use Orbot, you will need to route your traffic through the proxy settings on your web browser, or an application's proxy settings through Orbot's *Apps*. *Firefox* is the preferred browser for Orbot and therefore is the one that we will install. As Firefox's proxy settings on Android are locked down there is one further step to take—install an add-on called *Proxy Mobile*. In the following assignments we will install Firefox, Orbot and the add-on Proxy Mobile for Firefox. From there it just takes a little bit of configuring and the safest way to browse the web will be at your fingertips.

### **Assignment: Install Firefox**

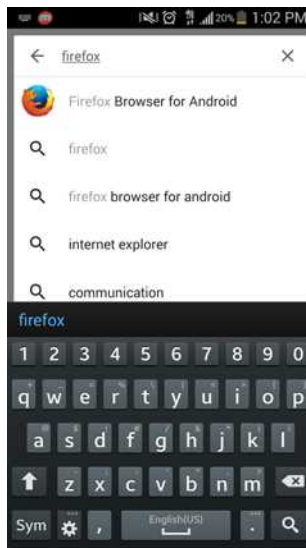
In order to use Tor services, *Firefox for Android* must be installed. It is possible to use Orbot with Google Chrome and a plugin, however Firefox is currently the browser that Orbot is being tested and developed on for without a root.

### 3. Vulnerability: Web Browsing

1. From your Home Screen, select *Play Store*.

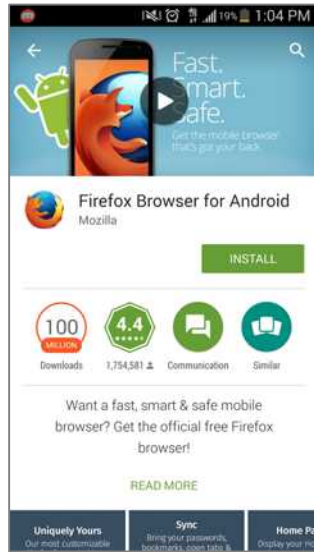


2. Enter *Firefox* into the top search bar and select *Firefox Browser for Android*.

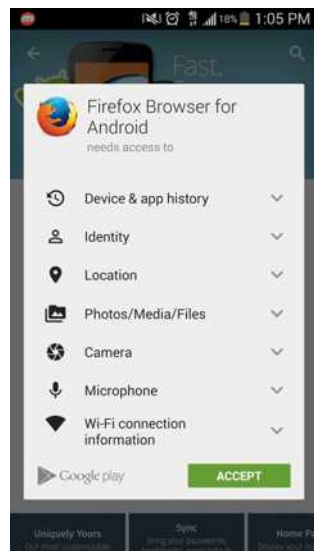


### 3. Vulnerability: Web Browsing

3. Select Install.



4. *Accept* the access requirements.



Great! Firefox is now installed. Next step... Install Orbot.

### 3. Vulnerability: Web Browsing

#### **Assignment: Install and Configure Orbot**

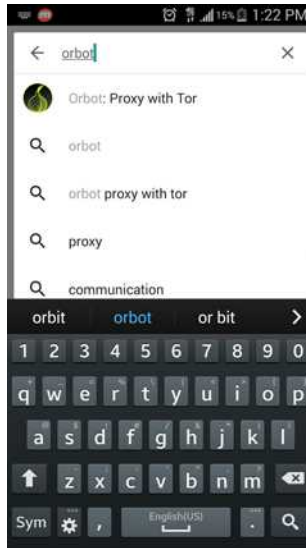
The next step is to install Orbot from the Play Store, and then configure it for proper use with our device.

1. From the Home Screen, select *Play Store*.

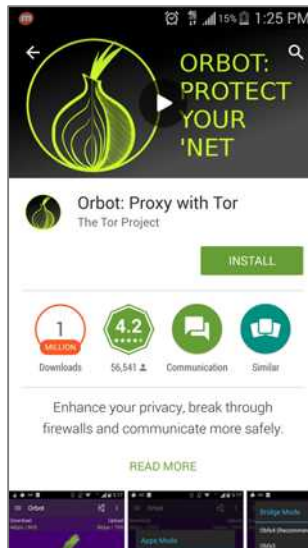


### 3. Vulnerability: Web Browsing

2. Enter *Orbot* into the top search bar, and then select *Orbot: Proxy with Tor*.

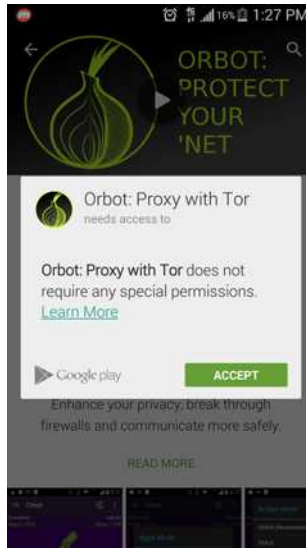


3. Select Install.

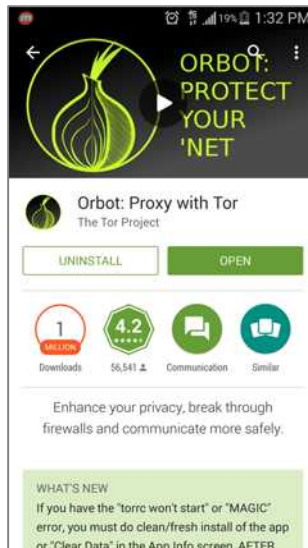


### 3. Vulnerability: Web Browsing

4. *Accept* the access requirements.

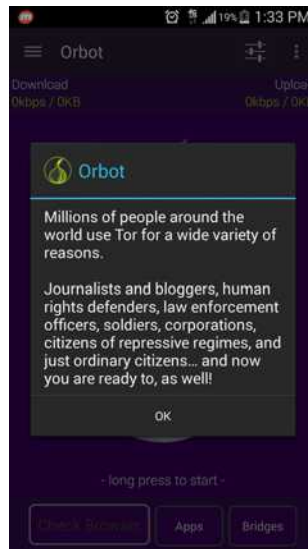


5. *Select Open.*



### 3. Vulnerability: Web Browsing

6. Select *OK*.



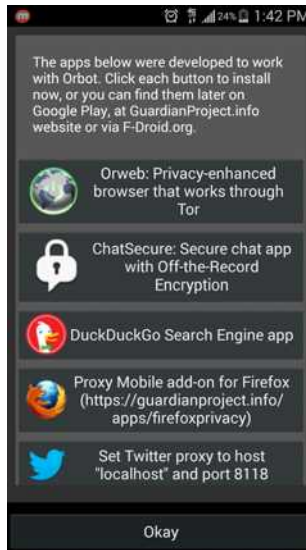
7. Press the *Menu* (3 dots) key in the upper right and select *Wizard*.





### 3. Vulnerability: Web Browsing

8. This screen lists the recommended applications to use with Orbot and how to use them. Select *Okay*.

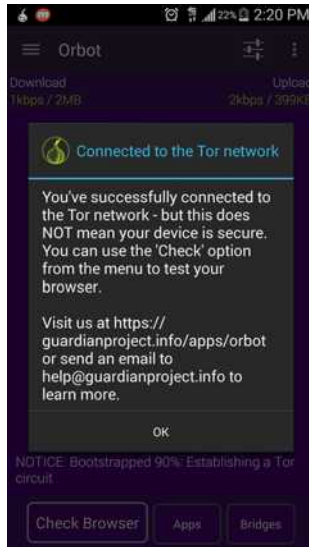


9. Do a long hold on the large ON button in the middle.



### 3. Vulnerability: Web Browsing

10. Select *OK*.



11. You will see that Orbot is connected to Tor, however configuration isn't yet complete. Select *Check Browser*.

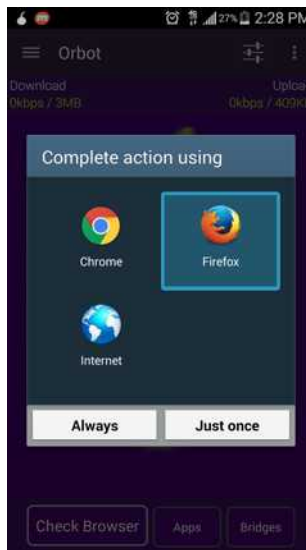


### 3. Vulnerability: Web Browsing

12. Select Standard Browser.

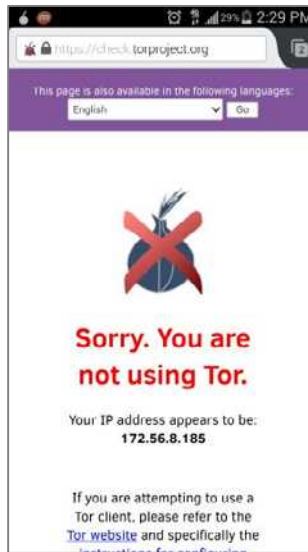


13. Select *Firefox* and then select *Always* and *OK*.



### 3. Vulnerability: Web Browsing

14. Notice the alert *Sorry. You are not using Tor.* To resolve this, the *Proxy Mobile* must be set up, and then finish the setup of Orbot for Tor.

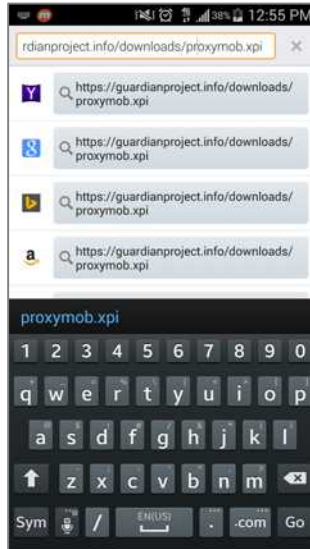


15. Press the *Home* button, and then select *Firefox*.

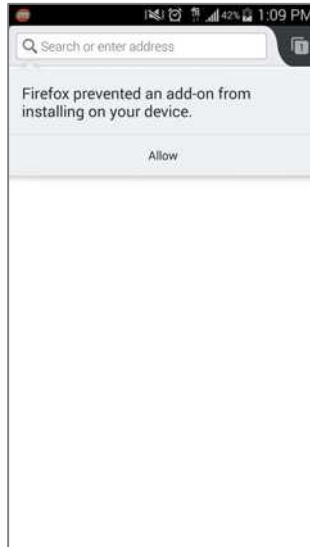


### 3. Vulnerability: Web Browsing

16. Enter *https://guardianproject.info/downloads/proxymob.xpi*, and then select *Go*.

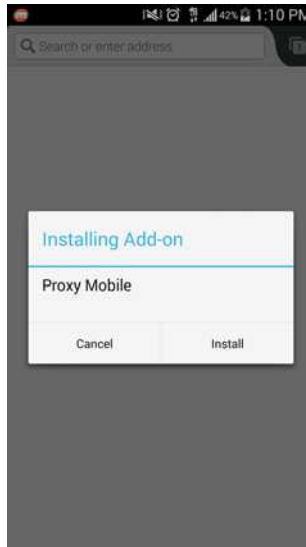


17. Select *Allow* to allow the add-on to install.



### 3. Vulnerability: Web Browsing

18. Select *Install* to have Proxy Mobile install.



19. Select *Restart* to have the browser restart and finish the installation of Proxy Mobile.



### 3. Vulnerability: Web Browsing

20. Enter *https://check.torproject.org*, and then select *Go*. This will check and verify that Tor is indeed up and running.



21. This screen will confirm that the browser is confirmed to use Tor and Tor is currently running through Orbot.



### 3. Vulnerability: Web Browsing

Congratulations! You have successfully setup Tor and now have the ultimate security against surveillance and the bad guys. Keep in mind when you do want to use the Tor network that you will need to have Orbot turned on and lit up green inside the application as well as browsing using Firefox.



## 4. Vulnerability: Email

*Human beings the world over need freedom and security that they may be able to realize their full potential.*

–Aung San Suu Kyi

It can be rightfully argued that email is the killer app that brought the Internet out of the geek world of university and military usage and into our homes (that is, if you can ignore the overwhelming impact of Internet pornography.) Most email users live in some foggy surreal world with the belief they have a God or constitutionally given right to privacy in their email communications.

No such right exists. Google, Yahoo!, Microsoft, Comcast, or whoever hosts your email service will turn over all records of your email whenever a government agency asks for that data. If that isn't bad enough, in most cases email is sent and received in clear text. This means that not only can anyone along the dozens of routers and servers between you and the other person clearly read your messages, but the kids and criminals snooping on your network can as well. Add to this knowledge the recent revelations about PRISM <[https://en.wikipedia.org/wiki/PRISM\\_\(surveillance\\_program\)](https://en.wikipedia.org/wiki/PRISM_(surveillance_program))>, where the government doesn't have to ask the provider for records, the government simply *has* your records.

If you find this as distasteful as I do, then let's put an end to it!

### Email Encryption Protocols

There are three common protocols that provide encryption of email between the computer and the email server:

- **TLS** <[http://en.wikipedia.org/wiki/Secure\\_Sockets\\_Layer](http://en.wikipedia.org/wiki/Secure_Sockets_Layer)> (Transport Layer Security),
- Its predecessor, **SSL** <[http://en.wikipedia.org/wiki/Secure\\_Sockets\\_Layer](http://en.wikipedia.org/wiki/Secure_Sockets_Layer)> (Secure Socket Layer), and
- **HTTPS** <<http://en.wikipedia.org/wiki/Https>> (Hypertext Transport Layer Secure)

Understand that these protocols only encrypt the message as it travels between your computer and your email server and back. Unless you are communicating with only yourself (sadly, as most geeks are prone), this does little good. Once your encrypted mail passes from your computer to your email server, it becomes clear text from your email server, through dozens of Internet routers, to the recipient email server, and finally onto the recipient's computer.

In order to use TLS or SSL, the following criteria must be met:

- Your email provider offers a TLS or SSL option. Many do not. If your provider does not offer this, *run*, don't walk, to another provider. If you are not sure which to select, I'm a fan of Google mail.
- You are using an email application as opposed to using a web browser to access your email.
- Your email application supports TLS or SSL.
- Your email provider has configured your email service to use TLS or SSL.
- You have configured the email application to use TLS or SSL
- Lastly, although not a requirement for TLS or SSL, a requirement to stall off breaking your password is that your email provider allows for strong passwords, and you have assigned a strong password to your email (many providers still are limited to a maximum of 8 character passwords.)

#### 4. Vulnerability: Email

### **Assignment: Configure the Email Application to Use TLS or SSL**

If you use a web browser for email, you may skip this assignment and move on to the next where we configure browser-based email to use https.

In this assignment we will verify if your email currently uses TLS or SSL.

1. From the Home Screen, select *Email*.



## 4. Vulnerability: Email

2. Press the *Menu* button, and then select *Settings*.

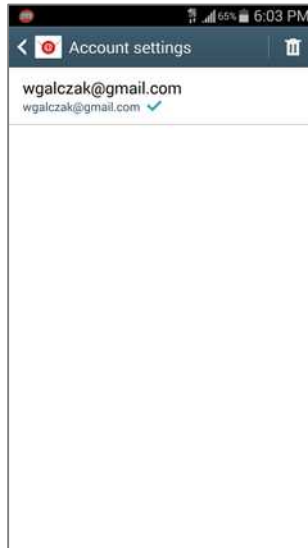


3. Select *Account settings*.

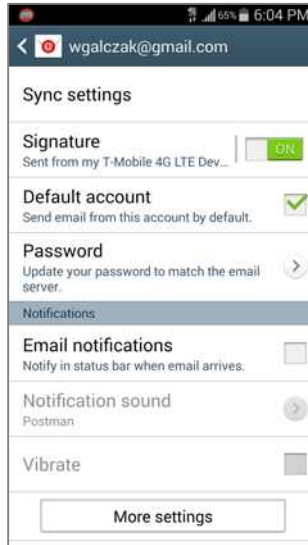


## 4. Vulnerability: Email

4. Select the account to check.

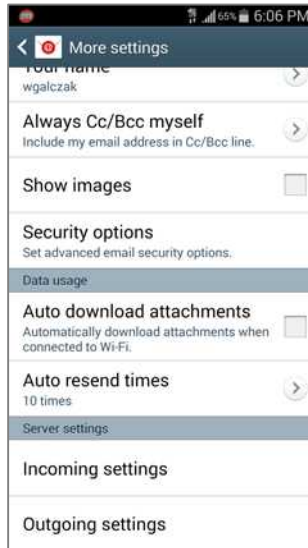


5. Select *More settings*.



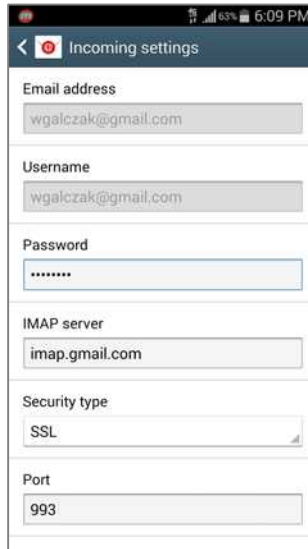
## 4. Vulnerability: Email

6. Scroll down to the bottom, and then select *Incoming settings*.



#### 4. Vulnerability: Email

7. Verify that *Security type* is set to either *SSL* or *TLS*. If it is off, don't activate the option yet. We first need to find out if your email provider supports SSL or TLS. If they do, then you will need to ask them what changes (if any) will need to be made to the email settings to use this encryption, and then make those changes.
  - In most cases there is nothing to do beyond selecting the SSL security type. If the provider doesn't support SSL or TLS, *run* to another provider.



8. Press *Back* and select *Outgoing settings* and make sure the same security type has either *SSL* or *TLS* listed.

**HTTPS.** We discussed HTTPS in the previous chapter. It is an encryption protocol used with web pages. It also can be used to secure email that is accessed via a web browser. When using HTTPS the user name and password are fully encrypted between the website and the computer, as are the contents of all email that you create or open.

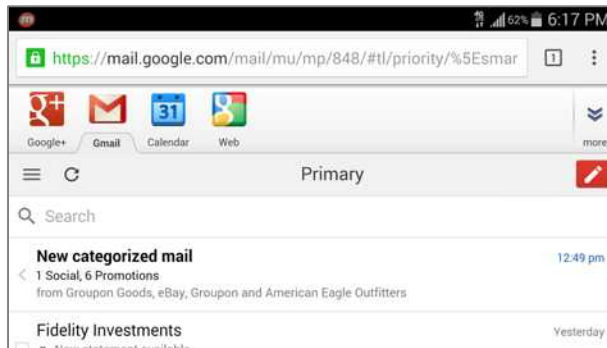
When using a web browser to access email, it is vital that the email site use the HTTPS encryption protocol to help ensure data and personal security.

## 4. Vulnerability: Email

### Assignment: Configure Browser Email to Use HTTPS

If you use a web browser to access email, it is critical that the web connection use HTTPS. In this assignment we will verify that your browser-based email uses HTTPS.

1. Open *Chrome*, and then go to your email login page. In this example we will be using *Google Mail* (Gmail).
2. As in the screen shot below, make sure that the URL field shows either the lock to the left of the URL, or `https://` and not `http://`. This indicates you are communicating over a secure, encrypted pathway. If instead the browser shows the URL to be `http://` or there is no lock, try revisiting the email login page, but this time manually enter `https://...`



3. If you get to the login page, all is good. Just bookmark the `https://` URL and use it instead of the previous non-secure URL.
4. If you cannot get to the log in page, change your email provider NOW!



### End-To-End Secure Email With SendInc

Using TLS/SSL or HTTPS for email is a good start. Unfortunately, unless you are certain that the other end of the communication chain also is using *the same email system as yourself*, this is much like locking your front door when leaving for vacation, while leaving the back door open. The reason is that even if the other user has TLS/SSL or HTTPS, this only ensures security between their computer and their server. When the two of you exchange email, there is no guarantee that the email is not in plain text once it hits either server, or when being transmitted from sender to recipient servers.

If you are serious about email security, then you need to use an end-to-end secure email solution.

There are two ways to approach this:

- Use an email encryption utility. This works well as long as the other end of the communication also is using the same encryption utility. Later in this chapter will cover this strategy using *GNU Privacy Guard* and *S/MIME*.
- Use a cloud-based option. This method makes it every bit as simple to send and receive email as the user is accustomed to. The downside is that instead of using an email client, a website is used to send and receive mail.

We will be discussing the email encryption later in this chapter. Here we will focus on the cloud-based option.

Our recommendation is to use *SendInc* <<https://SendInc.com>>. SendInc has several advantages for the typical user. These include:

- Both a free and pro service is offered.
- The pro service is only \$5/month.
- Military-grade end-to-end encryption of username and password, email, and attachments are included.
- The free version automatically self-destructs the email after 7 days. The pro version allows the user to determine the destruction date and includes unlimited retention.

#### 4. Vulnerability: Email

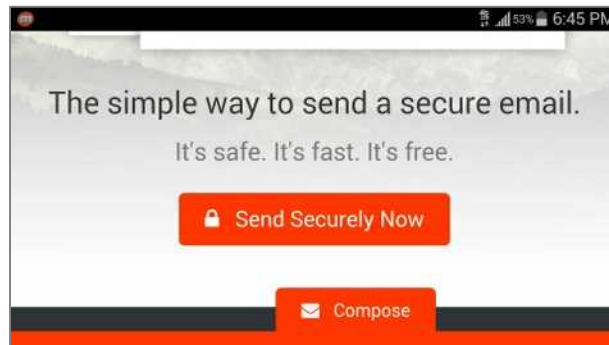
- The free version allows up to 20 recipients/day. The pro version allows 200.
- The pro version allows retraction of a sent email (if it has not yet been opened).
- The pro version allows for rich text email. The free version is text-only.

When sending from SendInc, you log into an HTTPS home page that also serves as the email composition page. Once the message is sent (fully encrypted), the recipient receives an email stating that a secure message is waiting. The recipient clicks the link, taking the recipient to an authentication page. Upon entering the password (which is automated if this is other than a first visit), the recipient then sees the message. The recipient can directly reply securely to the message, and you then receive an email informing you a secure message is waiting.

Although not quite as convenient as using your own email software, when security, convenience, and cost are taken into consideration against the impacts of violating HIPAA requirements, or the potential drama of confidential communications being intercepted, we find SendInc to be an easy choice.

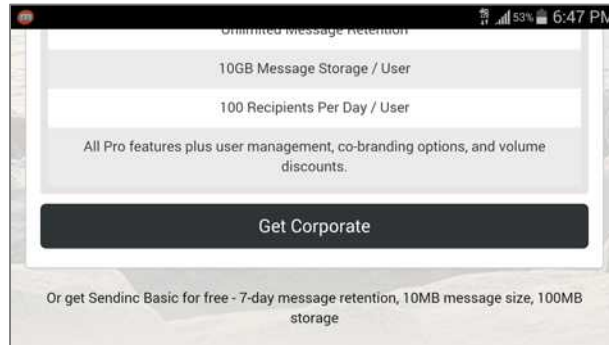
#### **Assignment: Create a SendInc Account**

1. Using *Chrome*, visit SendInc <<http://SendInc.com>>. Scroll down and select the *Send Securely Now* button.



#### 4. Vulnerability: Email

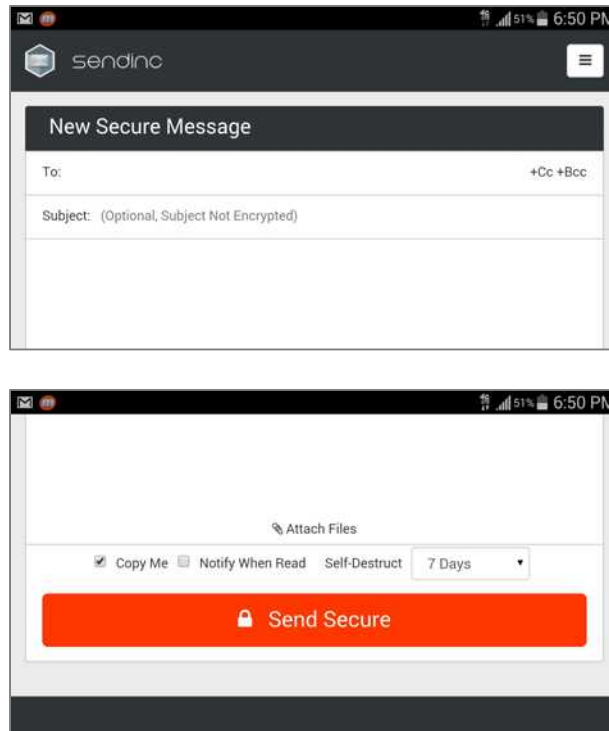
2. Scroll down the screen, and select *Or get SendInc Basic for free*.



3. On the *Create Your Account* screen, enter your email address, and then tap the *Continue* button.
4. Check email for a message from SendInc. Note the *Activation Code*. It will be needed in the next step.
5. On the *Account Information* screen, enter your full name, password, the *Activation Code* received in your email, enable the *I have read...* checkbox, and then tap *Create Account*.

#### 4. Vulnerability: Email

6. And here you are... Your first *New Secure Message* screen, waiting for you to conspire for world domination.



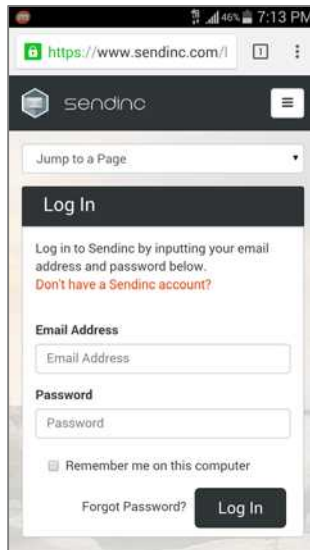
#### **Assignment: Create an Encrypted SendInc Email**

Once you have a *SendInc* account, you can send and receive limited numbers of fully encrypted emails daily for free. Should your needs exceed the free account, SendInc is happy to take a few dollars per month in exchange for a *Pro* account.

In this assignment, we will send our first fully encrypted email through SendInc.

## 4. Vulnerability: Email

1. Open *Chrome*, and go to <<http://www.sendinc.com>>, enter your email address and password, and then select *Log In*.

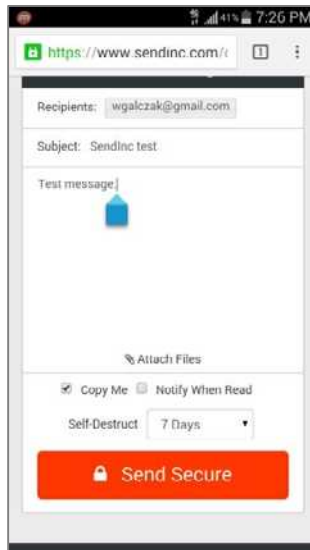


2. At the *New Secure Message* screen, enter the recipient email address and subject.



#### 4. Vulnerability: Email

3. Scroll down the screen, configure the *Copy Me*, *Notify When Read*, and *Self-Destruct* to taste, and then tap *Send Secure*.



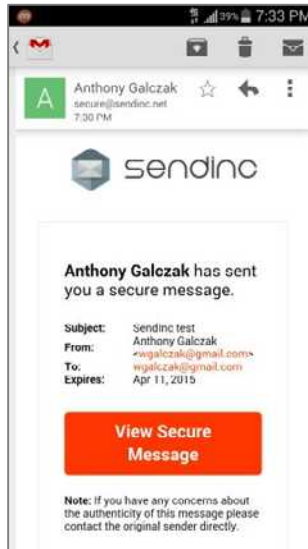
Your fully encrypted email is on its way!

#### **Assignment: Receive and Respond to a SendInc Secure Email**

In this assignment we reply to our first SendInc secure email. The previous two assignments must first be completed.

#### 4. Vulnerability: Email

1. The recipient will receive the email just as they would ordinary email. They will see the sender and subject line. However, in order for them to read the body of the message or any attachments, they will need to scroll down and select *View Secure Message*.



2. If the recipient has an existing *SendInc* account, they will be prompted to login. If they don't have an account, they will be prompted to create an account—the same process you went through.

The document and any attachments will now open for viewing and reply.

### End-To-End Secure Email With S/MIME

*S/MIME* (Secure/Multipurpose Internet Mail Extensions)

<<http://en.wikipedia.org/wiki/S/MIME>>, uses a strategy of employing both Public and Private Keys to secure email. Each person has a Private Key to decrypt a received email, and a Public Key that others may use to encrypt email to send out. An advantage of S/MIME over other Public/Private Key services is that there is no need to manually retrieve the other person's Public Key. Simply by signing an email and sending it to the other person, that person now has your Public Key. When the other person has done the same for you, the two of you may exchange encrypted email. Another benefit is that S/MIME is built right into almost all email clients, including the Android Email.app. No need to install another application. Note that S/MIME will not work with browser-based email.

Unlike other Public/Private Key services, you will need to acquire an *email certificate* from a *Certificate Authority (CA)*. There are many Certificate Authorities available. Your Internet Provider or Web Host may be able to do this for you. Free certificates for personal use (which are valid for one year) are available, but using these can become tedious, as you will need to repeat all the steps below every year. Purchasing a commercial certificate will set you back \$10 to \$100 per year, but you will only have to go through the process once.

S/MIME offers three certificate classes:

- **Class 1:** This level of certificate is acquired without any background check or verification that the person requesting it has anything to do with the email address it will be assigned to. In fact, it is even possible to roll your own certificate! That said, it will verify that the email address in the *From* field is actually the address that sent the email, and do the job of encrypting email so that only the intended recipient can decrypt and read it.
- **Class 2:** This level takes it a step further, validating that not only is the email address in the *From* field the one that actually sent the email, but that the name in the *From* field is tied to that email address.



#### 4. Vulnerability: Email

- **Class 3:** This is the highest-level validation, with a background check performed to verify not only the name of the individual or company, but physical address as well. **This is the only class suitable for healthcare (HIPAA), legal, and corporate use.**

Any level certificate for use with Android will require using a computer to acquire the certificate and then transfer it to your device. In the next exercise we will create a Class 1 (free) certificate. Full step-by-step details to create a Class 3 certificate are available in *Practical Paranoia: OS X Security Essentials*, and *Practical Paranoia: Windows Security Essentials*.

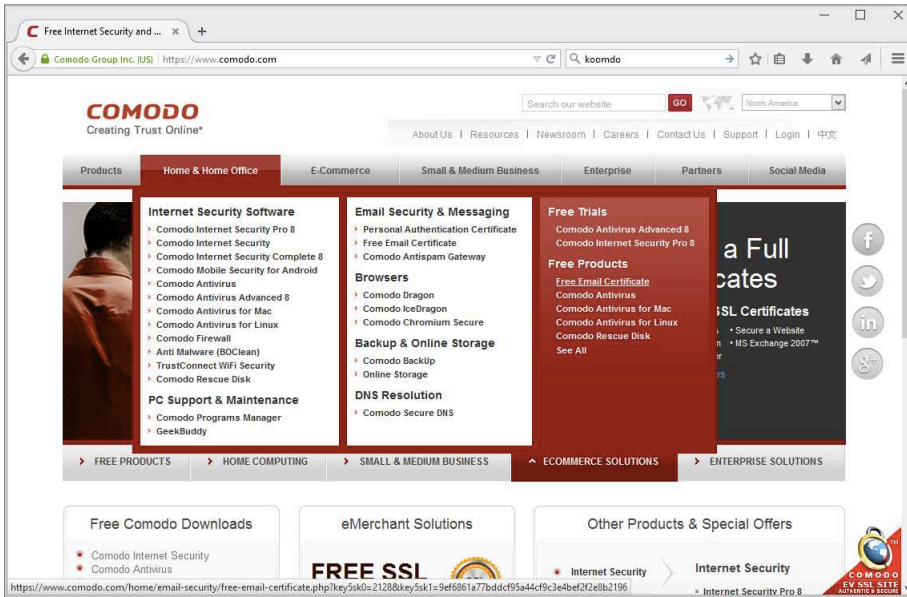
#### **Assignment: (Windows) Acquire a Free Class 1 S/MIME Certificate for Personal Use**

In this assignment you will sign-up for a free 1-year free S/MIME certificate for personal use from a leading Certificate Authority, Comodo, in Windows 10. This can be converted into a long-term commercial certificate. If you are using OS X, skip to the next assignment, *Assignment: (OS X) Acquire a Free Class 1 S/MIME Certificate for Personal Use*.

1. Open a web browser and surf to *Comodo* at <<https://comodo.com>>.

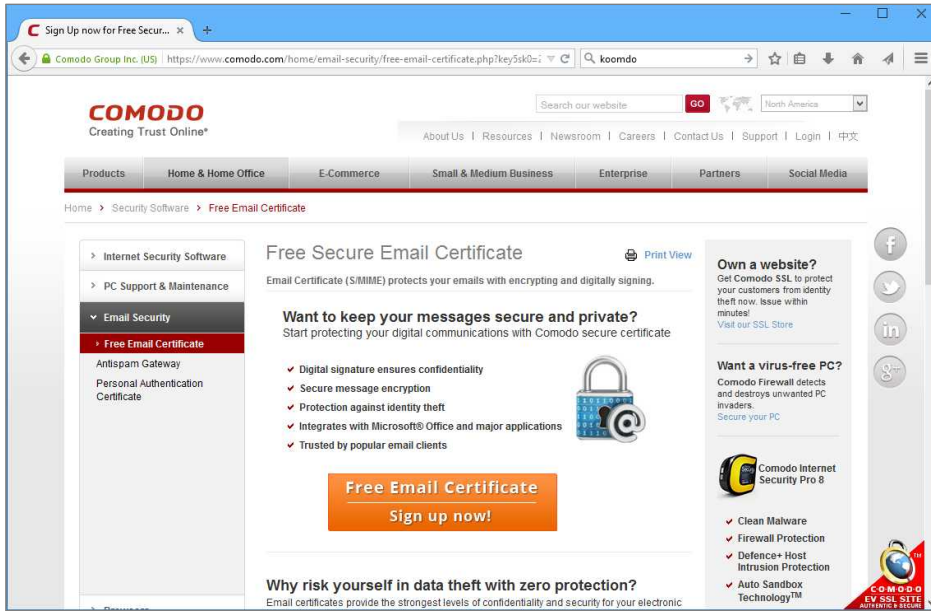
## 4. Vulnerability: Email

2. From the navigation bar, select *Home* & *Home Office* > *Free Email Certificate*.



## 4. Vulnerability: Email

3. This takes you to the Free Secure Email Certificate page. Select the Free Email Certificate button.



The screenshot shows a web browser window displaying the Comodo website. The browser's address bar shows the URL: <https://www.comodo.com/home/email-security/free-email-certificate.php?key5sk0z;>. The page title is "Sign Up now for Free Secur...". The Comodo logo is at the top left, with the tagline "Creating Trust Online®". A search bar and a "GO" button are at the top right. Below the logo is a navigation menu with links: "About Us", "Resources", "Newsroom", "Careers", "Contact Us", "Support", "Login", and "中文". A secondary menu below that lists "Products", "Home & Home Office", "E-Commerce", "Small & Medium Business", "Enterprise", "Partners", and "Social Media". The breadcrumb trail reads "Home > Security Software > Free Email Certificate".

The main content area is titled "Free Secure Email Certificate" and includes a "Print View" link. Below the title, it states: "Email Certificate (S/MIME) protects your emails with encrypting and digitally signing." A sub-heading asks, "Want to keep your messages secure and private?" followed by "Start protecting your digital communications with Comodo secure certificate". A list of benefits is provided:

- ✓ Digital signature ensures confidentiality
- ✓ Secure message encryption
- ✓ Protection against identity theft
- ✓ Integrates with Microsoft® Office and major applications
- ✓ Trusted by popular email clients

An image of a padlock with a Comodo logo is shown. Below the list is a large orange button that says "Free Email Certificate Sign up now!".

At the bottom of the main content area, a section titled "Why risk yourself in data theft with zero protection?" states: "Email certificates provide the strongest levels of confidentiality and security for your electronic".

On the right side of the page, there are three promotional boxes:

- Own a website?** "Get Comodo SSL to protect your customers from identity theft now. Issue within minutes! Visit our SSL Store"
- Want a virus-free PC?** "Comodo Firewall detects and destroys unwanted PC invaders. Secure your PC"
- Comodo Internet Security Pro 8** with a list of features:
  - ✓ Clean Malware
  - ✓ Firewall Protection
  - ✓ Defence+ Host Intrusion Protection
  - ✓ Auto Sandbox Technology™

At the bottom right, there is a "COMODO EV SSL SITE AUTHENTIC & SECURE" logo.

## 4. Vulnerability: Email

4. The *Application for Secure Email Certificate* page opens. Complete the form, specifying *High Grade* for your *Key Size*, and then select the *Next* button.

The screenshot shows a web browser window with the URL `https://secure.comodo.com/products/frontpage?area=SecureEmailCertificate&currency=l`. The page title is "COMODO Creating Trust Online" and the main heading is "Application for Secure Email Certificate".

**Your Details**

First Name   
Last Name   
Email Address   
Country

**Private Key Options**

Key Size (bits):

**Note:** Backup your private key! We do not get a copy of your private key at any time so, after completing this application procedure, we strongly advise you create a backup. Your certificate is useless without it. [More info](#)

**Revocation Password**

If you believe the security of your certificate has been compromised, it may be revoked. A revocation password is required to ensure that only you may revoke your certificate.

Revocation Password   
Comodo Newsletter  Opt in?

**Subscriber Agreement**

Please read this Subscriber Agreement before applying for, accepting, or using a digital certificate. If you do not agree to the terms of this Subscriber Agreement, do not apply for, accept, or use the digital certificate.

Email Certificate Subscriber Agreement

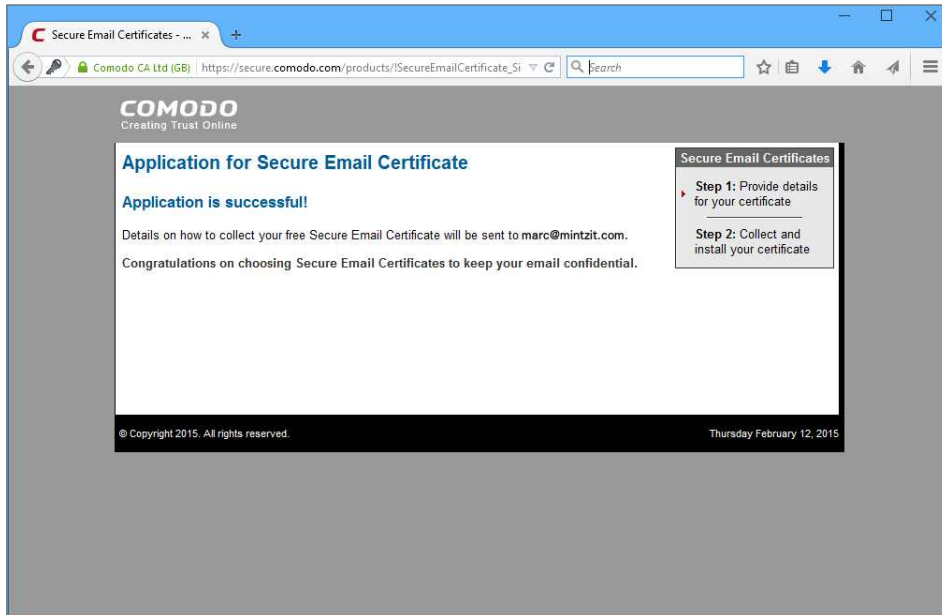
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING THE TERMS AND CONDITIONS.

IMPORTANT - PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING A COMODO EMAIL CERTIFICATE. BY USING, APPLYING FOR, OR ACCEPTING A COMODO EMAIL CERTIFICATE OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT THAT YOU

A progress indicator on the right side of the page shows "Secure Email Certificates" with two steps: "Step 1: Provide details for your certificate" (active) and "Step 2: Collect and install your certificate".

#### 4. Vulnerability: Email

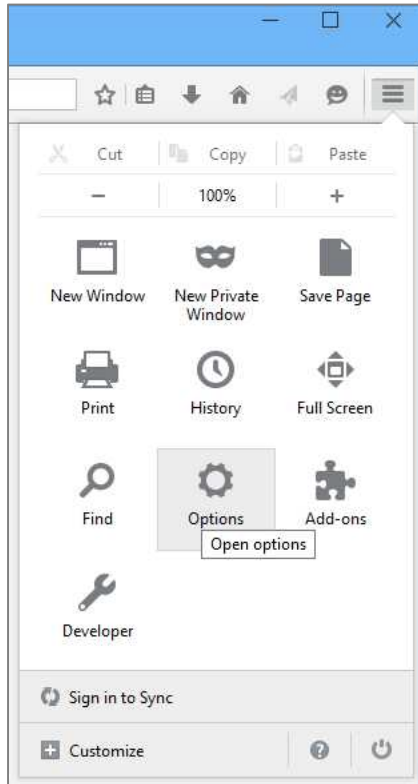
5. If all was completed correctly, you will see the *Application is Successful* page!



6. The certificate will be sent to the email address you specified.
7. Open your email to find the mail from Comodo, and then select the *Click & Install Comodo Email Certificate* button. You will be taken to the Comodo website to install the certificate on your computer
8. Assuming you are using Firefox, upon visiting the Comodo page, the Comodo certificate will automatically install in the browser. If using a different browser, you may be prompted to *install* or *download the certificate* manually.
9. Once installed in the browser, it's time to export the certificate and the associated private key to your email application. For this example we will be using Mozilla Thunderbird.

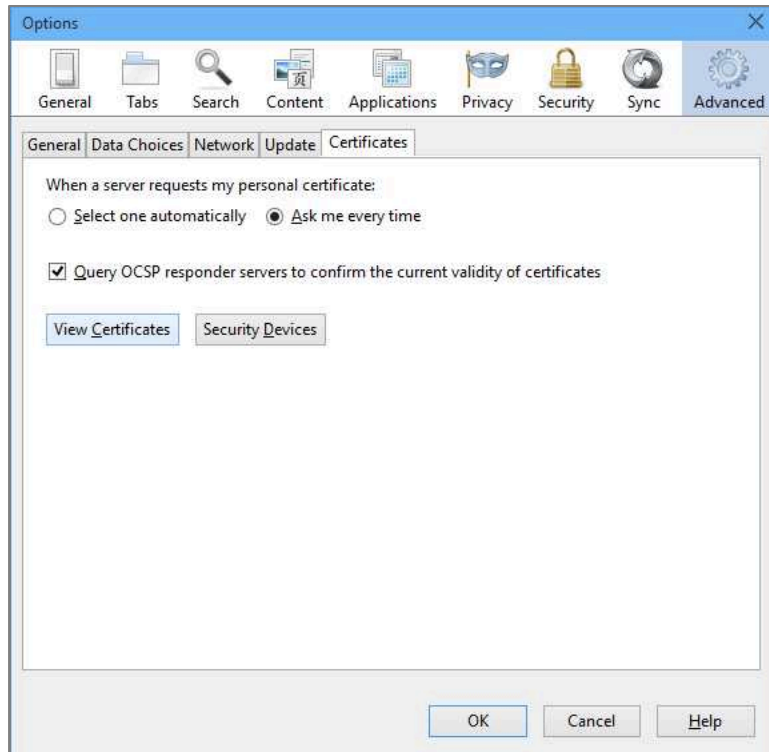
#### 4. Vulnerability: Email

10. Go to the Firefox Menu and select the *Options* button.



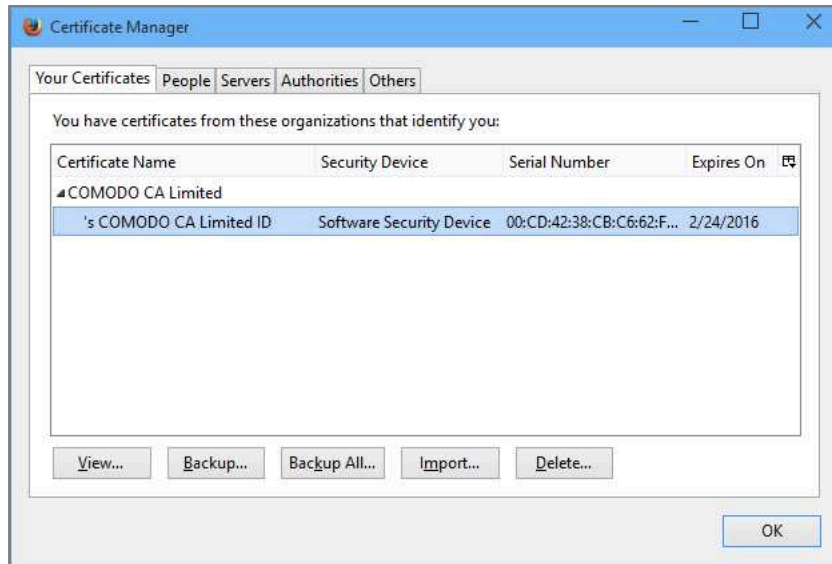
#### 4. Vulnerability: Email

11. In the *Options* pane, select the *Advanced* tab, and then the *View Certificates* button.

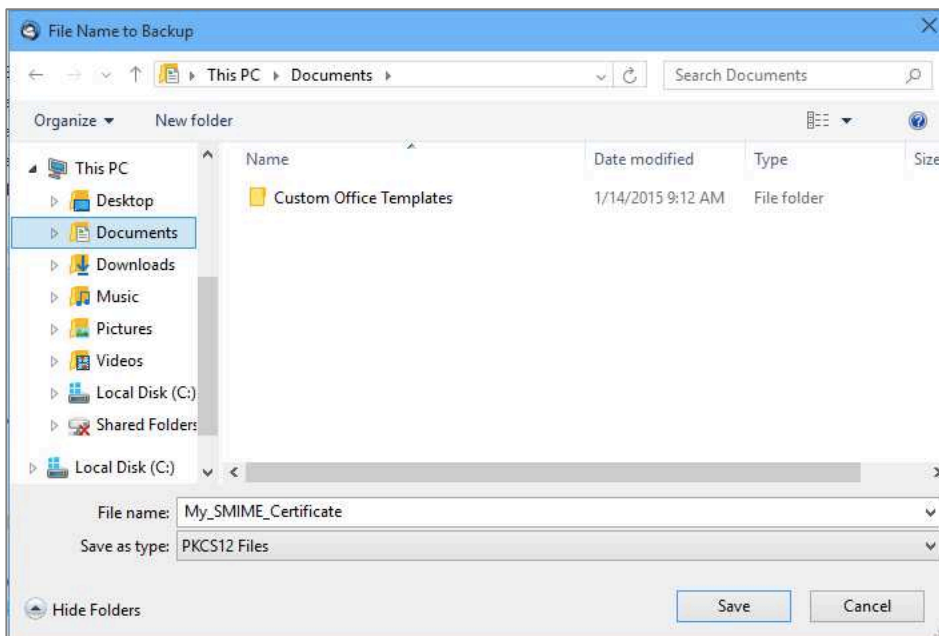


## 4. Vulnerability: Email

12. Once *View Certificates* opens, click the *Your Certificates* tab at the top. Select the certificate that was just installed, and then select the *Backup* button.



13. Select the *Save* button.



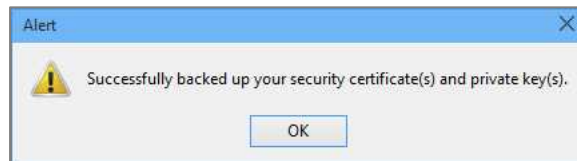


## 4. Vulnerability: Email

14. Name the personal certificate, and then click the *Save* button.
15. In the *Choose a Certificate Backup Password* window, enter a secure password, so that the exported Certificates will be secured with strong encryption, and then select the *OK* button.



16. A dialog box will appear confirming that your new E-mail certificate has been successfully exported. Select the *OK* button.



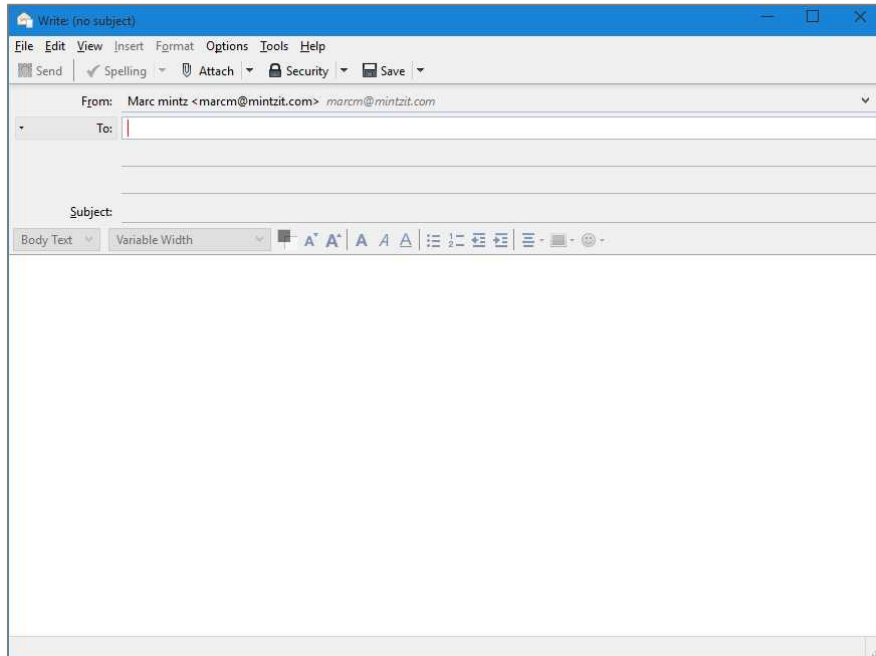
Wahoo! The hard part is over. Next step is to start using your new powers in your Android device!

### **Assignment: Export S/MIME Certificate from Windows for Import to Android**

To enable S/MIME on your Android devices to receive encrypted emails, it is necessary to email your Private Keys (your S/MIME certificate) from your Windows computer to your Android device. From here we can import the Private Keys into your Android device.

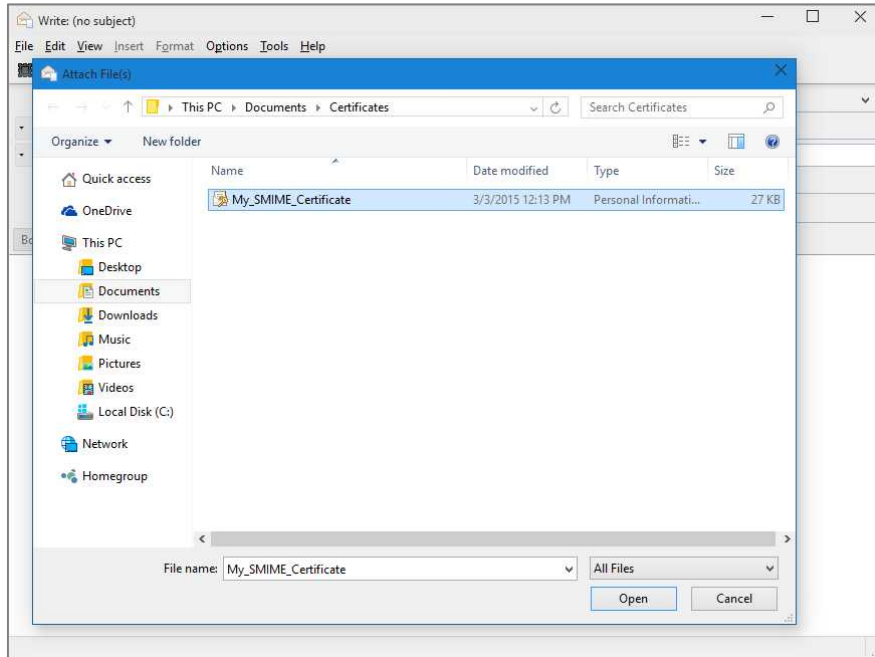
## 4. Vulnerability: Email

1. If you have not yet done so, complete the *Assignment: Acquire an Email Certificate* in the previous section. You should have your certificates that were exported out of Firefox to complete the next lesson.
2. Open Mozilla Thunderbird and compose an email to your own address.



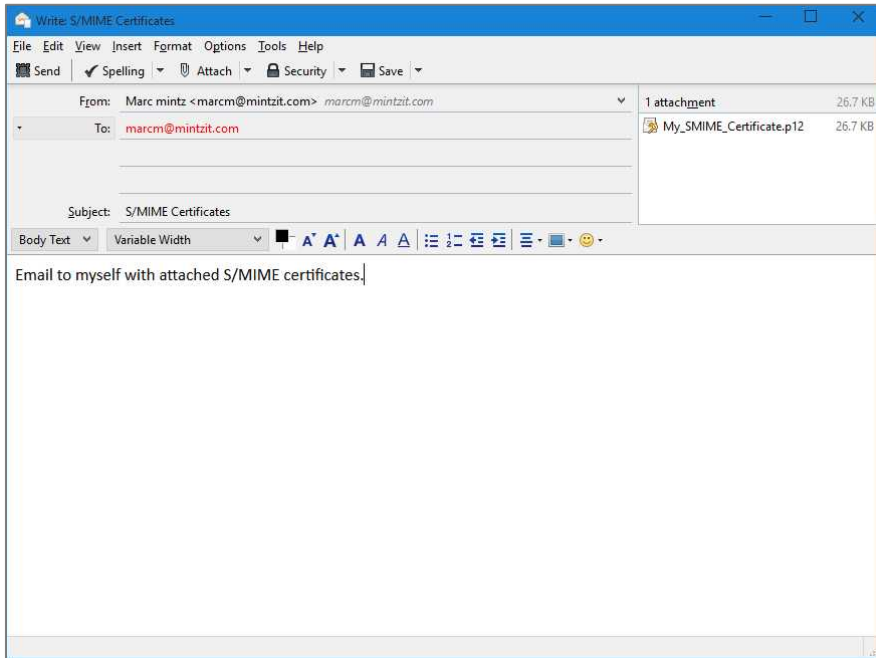
#### 4. Vulnerability: Email

3. From the top toolbar click the *Attach* button, and browse to the location where your S/MIME certificate was saved from Firefox. Select the certificate, and then click *Open*.



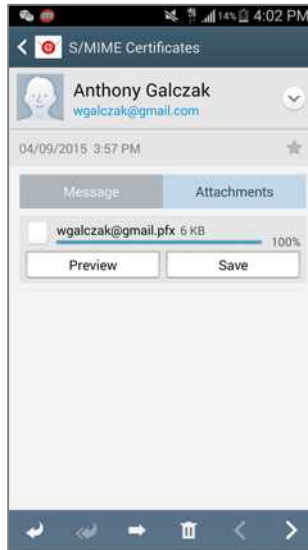
## 4. Vulnerability: Email

4. With your S/MIME certificate now attached, click the *Send* button.  
IMPORTANT: As you will be opening this message on your Android device—which does not yet have your certificate, and therefore doesn't have the ability to decrypt your messages—do *sign*, but don't *encrypt* this message!

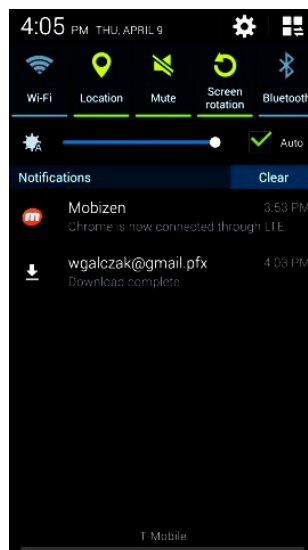


#### 4. Vulnerability: Email

5. On your device, open your *EMail* app, and then open the message you just sent to yourself. It will contain the attached .pfx/.p12 certificate.
  - o Note: .pfx and .p12 are the same file type. Select *Attachments*, and then select *Save*.

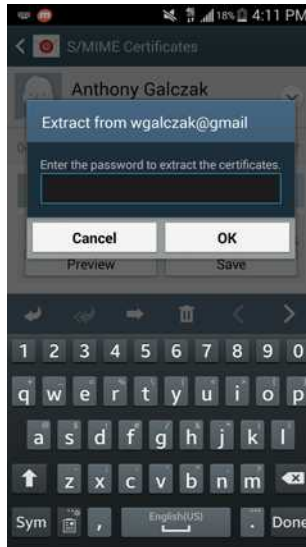


6. Use the pull-down menu at the top to select your attachment.



#### 4. Vulnerability: Email

7. Enter the secure password you used for the certificate earlier, and then select **OK**.

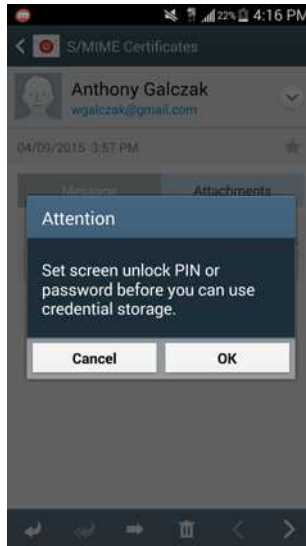


8. Name your certificate for use on your Android device. I recommend you leave it as the default, which is your email address. Select **OK**.

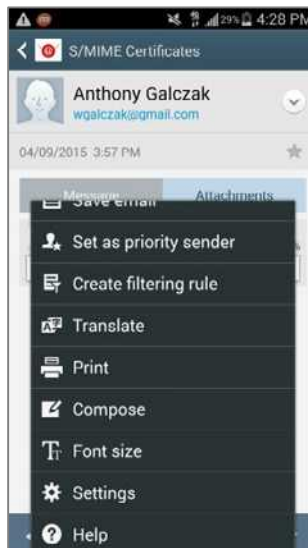


#### 4. Vulnerability: Email

9. If you do not have a PIN or password set, you will be prompted to setup one. Select *OK*. Enter whatever method of security you have, and then setup either a PIN or Password. Reference *Activity: Creating a Screen Lock using a Password*.

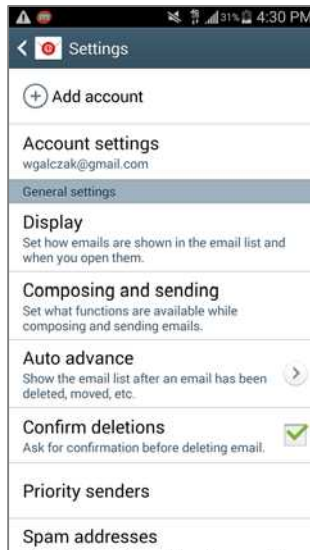


10. Your email client will confirm your certificate has been installed. We now need to sign all messages. Press *Menu*, scroll down, and then select *Settings*.



## 4. Vulnerability: Email

11. Select *Account settings* for the email address you are using, and then select your email address again.



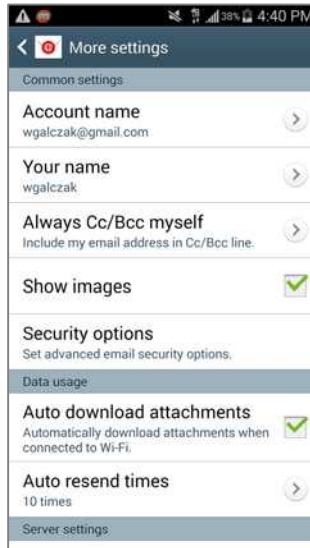
12. Select More settings.





## 4. Vulnerability: Email

13. Select Security options.



14. Enable the *Sign all* and *Encrypt all* check boxes. This will not allow you to use S/MIME yet, as you will need an additional app to interface with your email application to do this.



## 4. Vulnerability: Email

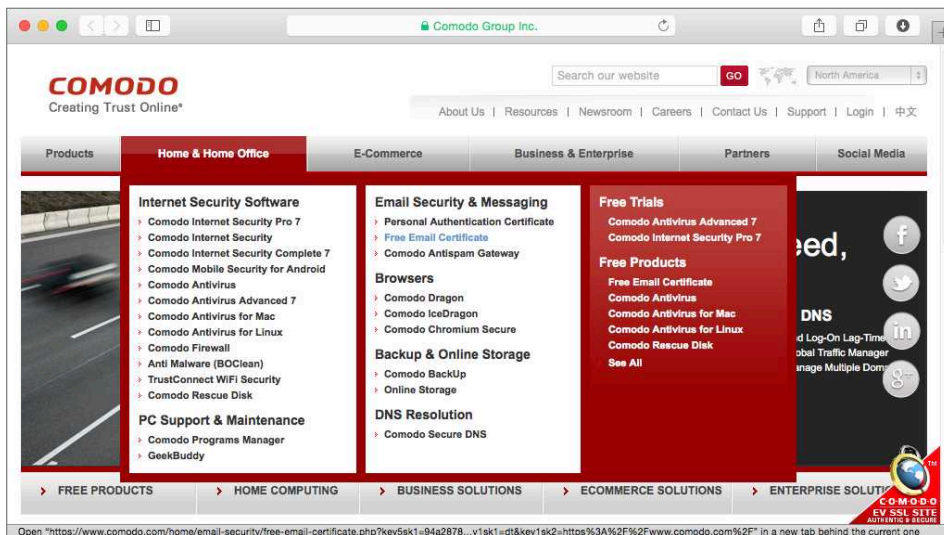
15. Press *Home* to exit.

Your Android device is now fully configured to both send and receive secure, encrypted S/MIME email.

### Assignment: (OS X) Acquire a Free Class 1 S/MIME Certificate for Personal Use

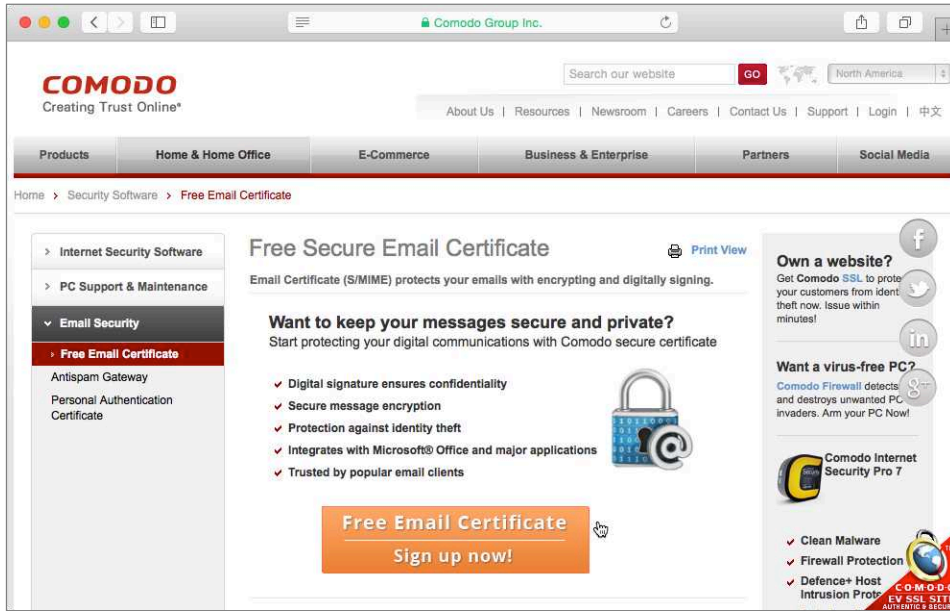
In this assignment you will sign-up for a free 1-year free S/MIME certificate for personal use from a leading Certificate Authority, Comodo. This can be converted into a long-term commercial certificate.

1. Open your web browser and surf to *Comodo* at <<http://comodo.com>>.
2. From the navigation bar, select *Home* & *Home Office* > *Free Email Certificate*.



## 4. Vulnerability: Email

3. This takes you to the *Free Secure Email Certificate* page. Select the Free Email Certificate button.



The screenshot shows a web browser window displaying the Comodo Group Inc. website. The page is titled "Free Secure Email Certificate" and features a navigation menu with categories like "Products", "Home & Home Office", "E-Commerce", "Business & Enterprise", "Partners", and "Social Media". The main content area includes a sidebar with "Email Security" options, a central section with a list of benefits (Digital signature ensures confidentiality, Secure message encryption, Protection against identity theft, Integrates with Microsoft Office and major applications, Trusted by popular email clients), and a prominent orange button labeled "Free Email Certificate Sign up now!". The right sidebar contains promotional text for "Own a website?", "Want a virus-free PC?", and "Comodo Internet Security Pro 7", along with social media icons and a "COMODO EV SSL SITE AUTHENTIC & SECURE" badge.

## 4. Vulnerability: Email

4. The *Application for Secure Email Certificate* page opens. Complete the form, specifying 2048 (High Grade) for your Key Size, and then select the Next button.

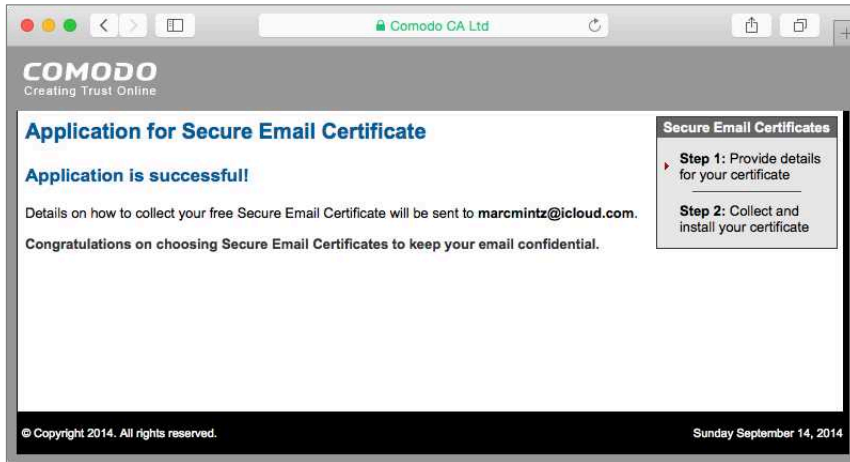
The screenshot shows a web browser window with the address bar displaying 'Comodo CA Ltd'. The page title is 'COMODO Creating Trust Online' and the main heading is 'Application for Secure Email Certificate'. The form is divided into several sections:

- Your Details:** Includes input fields for First Name, Last Name, and Email Address, and a dropdown menu for Country (currently set to 'United States').
- Private Key Options:** A dropdown menu for Key Size (bits) is set to '2048 (High Grade)'. Below this is a red note: 'Note: Backup your private key! We do not get a copy of your private key at any time so, after completing this application procedure, we strongly advise you create a backup. Your certificate is useless without it. [More info](#)'.
- Revocation Password:** A text input field for the password and a checkbox for 'Comodo Newsletter' which is checked.
- Subscriber Agreement:** A large text area containing the terms of the agreement, including a binding arbitration clause and a list of terms. The first term is '1. Application of Terms'. Below the text area is a checkbox labeled 'I ACCEPT the terms of this Subscriber Agreement.' which is currently unchecked.

At the bottom of the form is a 'Next >' button. The footer of the page contains the copyright notice '© Copyright 2014. All rights reserved.' and the date 'Sunday September 14, 2014'.

#### 4. Vulnerability: Email


5. If all was completed correctly, you will see the *Application is Successful* page!



6. The certificate will be sent to the email address you specified.

## 4. Vulnerability: Email


7. Open your Mail.app to find the email, and then select the *Click & Install Comodo Email Certificate* button.

☆ Certificate Customer Services  September 14, 2014 7:25 PM  
To: Marc Mintz  
Your certificate is ready for collection! [Hide Details](#)

**COMODO**

Tel Sales : +1 888 266 6361  
Fax Sales : +1.201.963.9003

**Your Comodo FREE Personal Email Certificate is now ready for collection!**



Dear Marc Mintz,

**Congratulations** - your Comodo FREE Personal Secure Email Certificate is now ready for collection! You are almost able to send secure email!

Simply click on the button below to collect your certificate.

**Click & Install Comodo Email Certificate**

**Note:-** If the above button does not work, please navigate to [https://secure.comodo.com/products/SecureEmailCertificate\\_Collect2](https://secure.comodo.com/products/SecureEmailCertificate_Collect2) Enter your email address and the Collection Password which is: pMJNalysGvxFcux

Your Comodo FREE Personal Secure Email Certificate will then be automatically placed into the Certificate store on your computer.

Click "Yes" if you see a "Potential Scripting Violation" window asking "Do you want this Program to add Certificates now?"

Please visit [http://www.comodogroup.com/support/products/email\\_certs/index.html](http://www.comodogroup.com/support/products/email_certs/index.html) for guidance on configuring your email client to use your certificate to secure email.

**Note:-** We strongly recommend that you export your certificate to a safe place in case you need to reload it later. For details, please see [http://www.instantssl.com/ssl-certificate-support/server\\_faq/ssl-email-certificate-faq.html](http://www.instantssl.com/ssl-certificate-support/server_faq/ssl-email-certificate-faq.html).

You can revoke your certificate by clicking on the button below.

**Revoke Comodo Email Certificate**

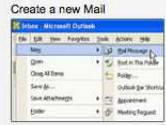
If you need to revoke your Comodo FREE Personal Secure Email Certificate then please navigate to [https://secure.comodo.com/products/SecureEmailCertificate\\_Revoke](https://secure.comodo.com/products/SecureEmailCertificate_Revoke) You will need to enter your email address and revocation code. Thank you for your interest in Comodo.

Comodo Certificate Services Team  
[secureemail@comodogroup.com](mailto:secureemail@comodogroup.com)

### How to encrypt mail

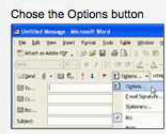
**Step 1**

Create a new Mail



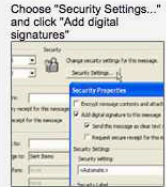
**Step 2**

Choose the Options button




**Step 3**

Choose "Security Settings..." and click "Add digital signatures"



**Step 4**

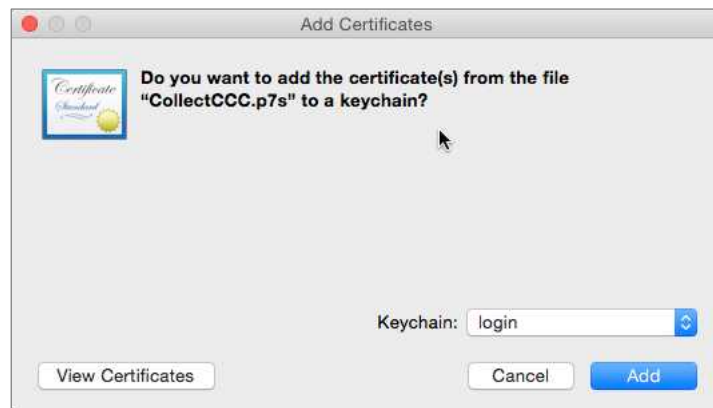
You can digitally sign "all" your e-mails by enabling it in the main "options" setting in outlook



**Tip :-** "Encrypt contents" will only work if you have added a digitally signed email to your address book from the person you want to encrypt the email with on the RHS screenshot.

#### 4. Vulnerability: Email

8. Although the button says *Click & Install Comodo Email Certificate*, all it really does is download the certificate. You will need to manually install the certificate.
9. Once downloaded, the certificate will be found in your *Downloads* folder, named something like *CollectCCC.p7s*. Navigate in the Finder to your *Downloads* folder to find this certificate file.
10. Double-click the *CollectCCC.p7s* certificate. An *Add Certificates* window will open asking if you want to add the certificate to your keychain. From the *Keychain* pop-up menu, select *Login*. This will add the certificate to your own default Keychain database, and then select the *Add* button.



11. Quit the Keychain Access application.
12. Repeat steps 1-10 for each of your email addresses for which you need secure communications.

Wahoo! The hard part is over. Next step is to start using your new powers with your Android device!

## 4. Vulnerability: Email

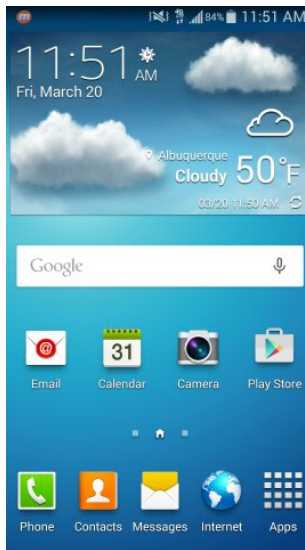
### Using S/MIME

In order to use S/MIME on Android we first have to install an additional app that has support for the S/MIME protocol. The application I recommend is *CipherMail* <<https://www.ciphermail.com>>. This application does not have to serve as your main email client; it is just a shell that goes on top of your existing email client and it will be only necessary to use this when sending or receiving S/MIME emails.

### Assignment: Install and Configure CipherMail

Now that your S/MIME certificate is installed on your Android device, we will install a front-end application that can send and receive S/MIME certificates.

1. From your Home Screen, select *Play Store*.





#### 4. Vulnerability: Email

2. Enter *Ciphermail* into the top search bar. Select the *Search* button in the bottom right and select *CipherMail*.

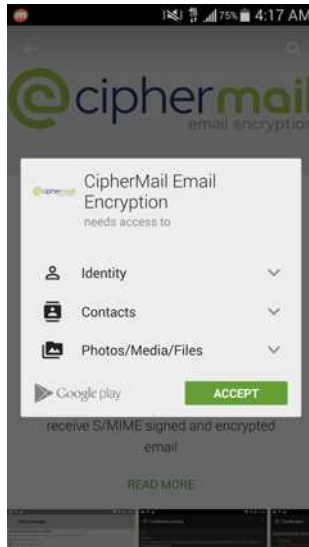


3. Select Install.



## 4. Vulnerability: Email

4. *Accept* the access requirements.

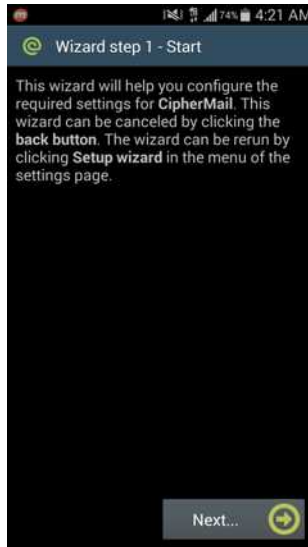


5. Select *Open*.

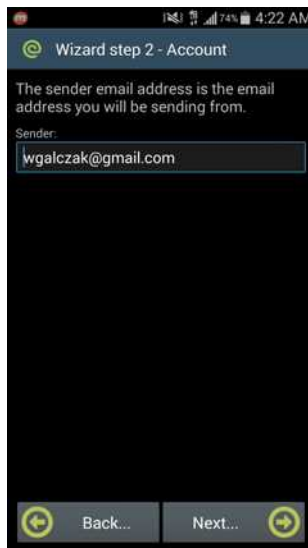


#### 4. Vulnerability: Email

6. Opening CipherMail will start the setup wizard. Select *Next* to continue.

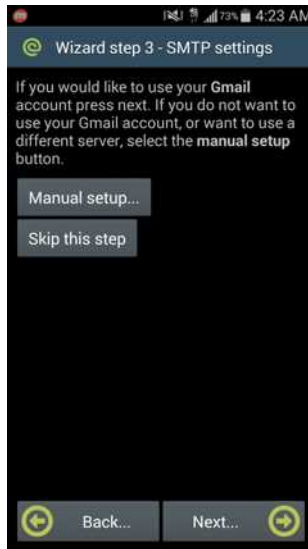


7. Enter the email address for which you are using S/MIME, and then select *Next*.

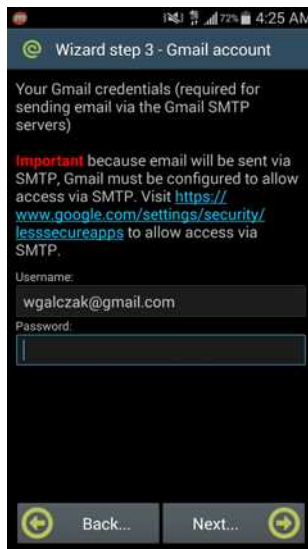


#### 4. Vulnerability: Email

8. If you are using a non-web-based email service this is where you would setup your SMTP settings. For all other accounts select *Next*.

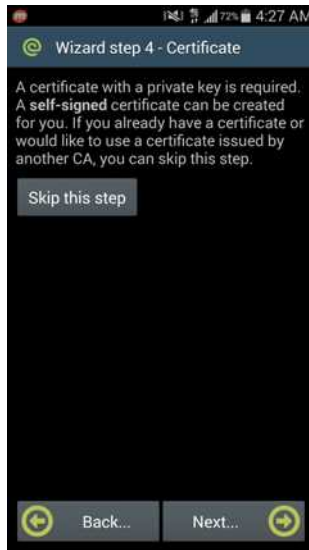


9. Because CipherMail will be interfacing with your email account, it will need your login credentials to send and receive. Enter your password, and then select *Next*.

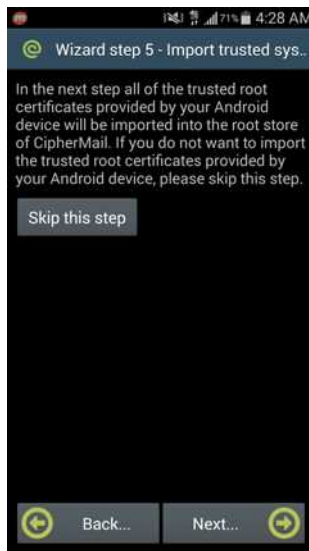


#### 4. Vulnerability: Email

10. I recommend skipping the *Wizard step 4–Certificate* step, as we want to use the S/MIME certificate we have already created. Select *Skip this step*.

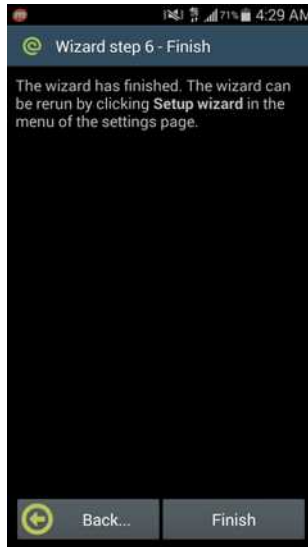


11. *Wizard step 5* will import all the default Android root certificates. I recommend doing this. Select *Next* to continue.



#### 4. Vulnerability: Email

12. Select *Finish*.



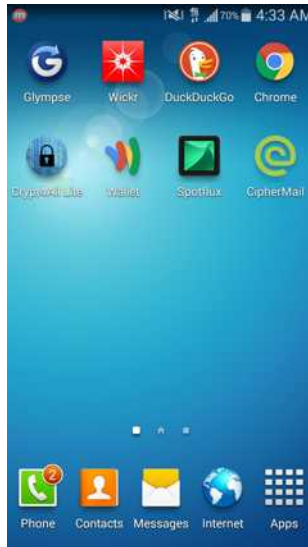
Congratulations! You have installed and configured CipherMail. It is now ready to import private keys including your new S/MIME certificate.

#### **Assignment: Add a Private Key to CipherMail**

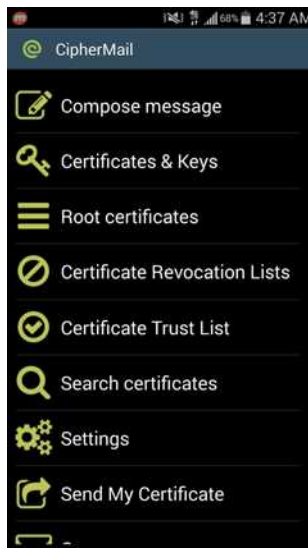
In order to use our brand new S/MIME certificate we will now need to import the key into Ciphermail.

## 4. Vulnerability: Email

1. From your Home Screen, select *CipherMail*.

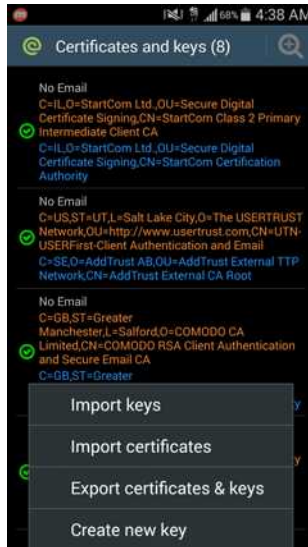


2. Select Certificates & Keys.

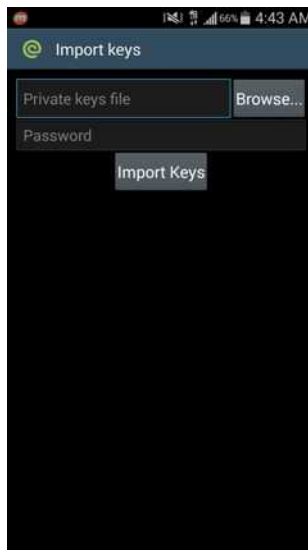


## 4. Vulnerability: Email

3. Press the *Menu* button and select *Import keys*.



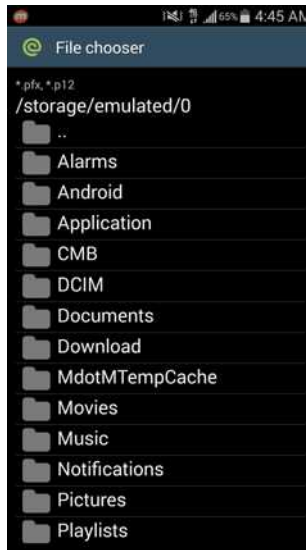
4. Select *Browse* to locate the certificate file.



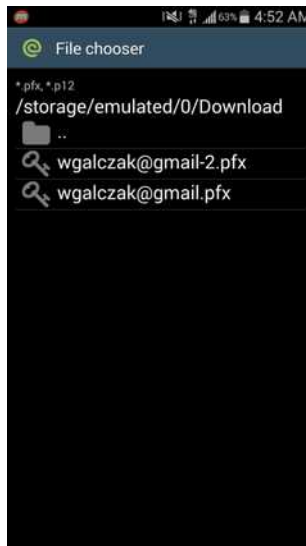


#### 4. Vulnerability: Email

5. If you downloaded the file like the previous assignments, your certificate should be in your *Download* folder. Select *Download*.

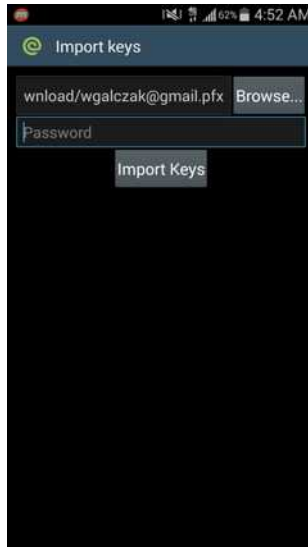


6. Select your certificate file.

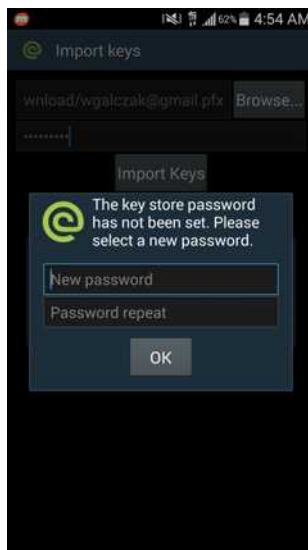


#### 4. Vulnerability: Email

7. Enter your password and then select *Import Keys*.

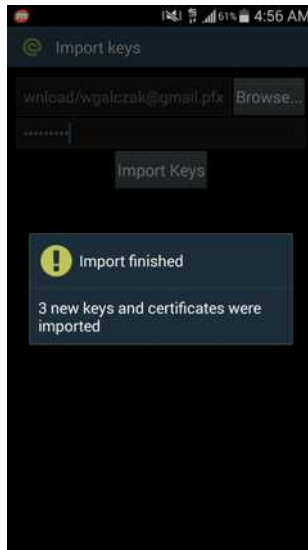


8. Now we need to setup the *key store password*. This is your default password for retrieving your keys saved in Ciphermail. Enter a password, repeat it and select *OK*.



#### 4. Vulnerability: Email

9. After entering your key password, set a key store password, and then select OK. A message will display showing your import has finished.



Whew! Now your keys and certificates are imported into CipherMail and we can now compose messages using S/MIME!

#### **Assignment: Compose an S/MIME Encrypted Email with CipherMail**

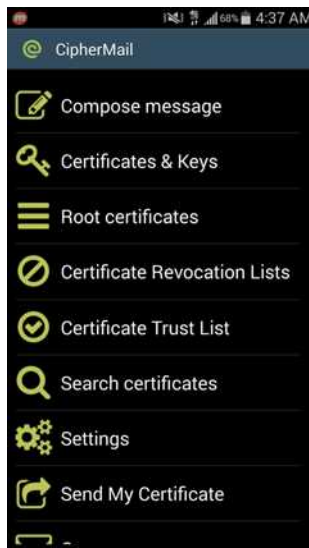
In this assignment we will create and send our first S/MIME encrypted email.

## 4. Vulnerability: Email

1. From your Home Screen, select *CipherMail*.

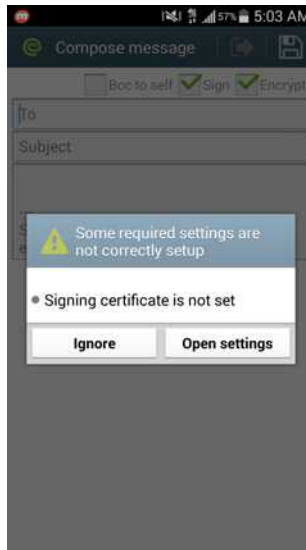


2. Select *Compose message*.



## 4. Vulnerability: Email

3. We will now need to set the certificate we'd like to use for signing our messages. Select *Open settings*.

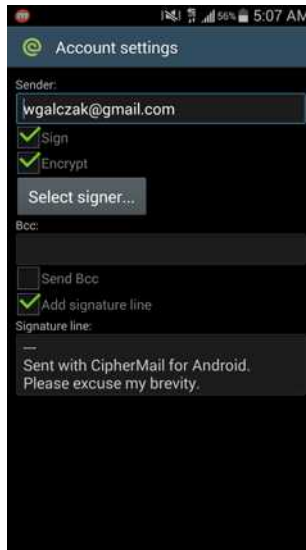


4. Select *Account*.

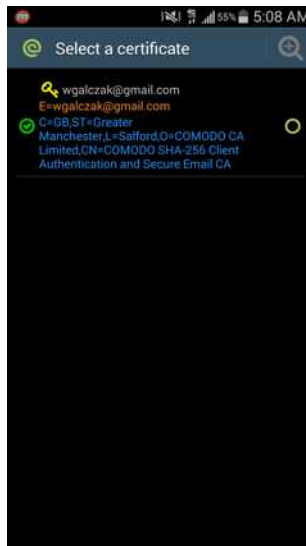


#### 4. Vulnerability: Email

5. Notice the *Sign* and *Encrypt* boxes are checked, leave those checked to sign and encrypt your email. All we need do is select *Select signer...*

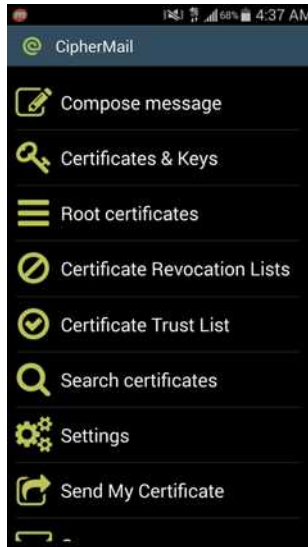


6. Select your *Comodo CA* certificate that we have imported.

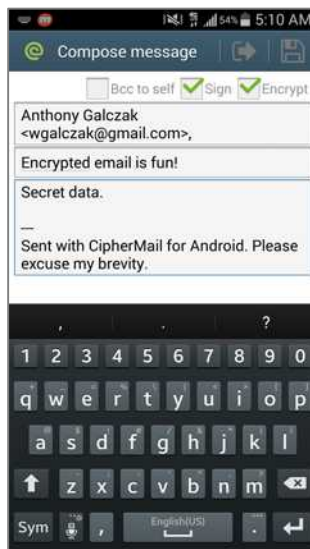


#### 4. Vulnerability: Email

7. Press the *Back* button twice and then select *Compose message* again.

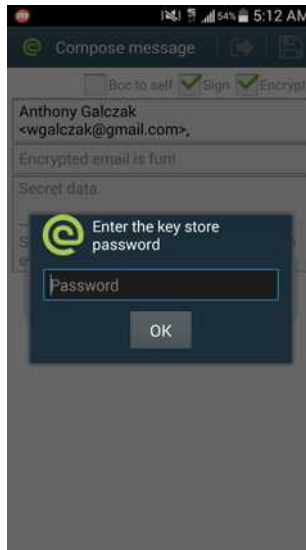


8. Enter your recipient, subject line and message in your email and then select the *Send arrow* in the upper right.

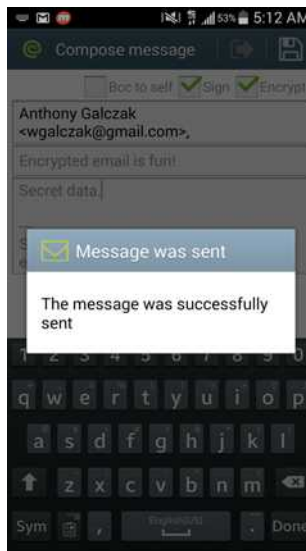


#### 4. Vulnerability: Email

9. You are sending an encrypted email, so you will need to confirm your CipherMail *key store password*. Enter the password and select *OK*.



10. A message will display when the message has been successfully sent. Press the *Back* button to compose another message or exit this notification.





#### 4. Vulnerability: Email

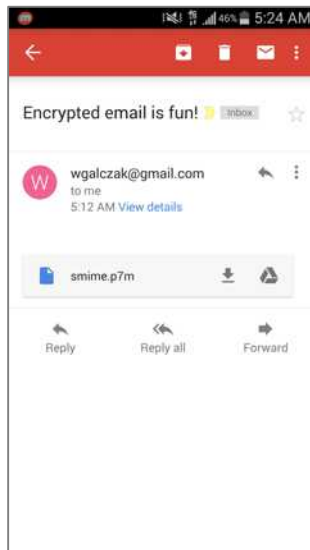
Congratulations! You have composed your first S/MIME signed and encrypted email. This is a huge step for the security of your email.

### **Assignment: Receive and Read S/MIME Encrypted Emails in CipherMail**

In order to read the encrypted emails that you have received in either the Email or Gmail app, it is necessary to open the S/MIME file in your email app, which will then prompt CipherMail to attempt to decrypt the message.

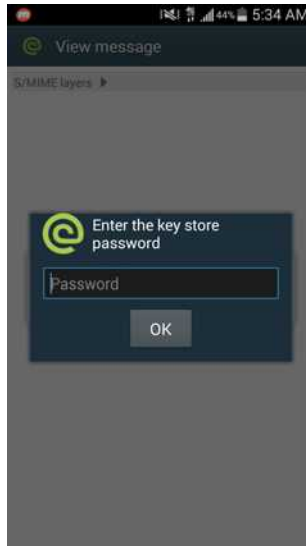
If you do not have the certificate to decrypt this message, skip ahead to *Assignment: Importing a Certificate in CipherMail* to first import the certificate.

1. Open your Email app and browse to your received S/MIME encrypted email. Notice that in your default email client that the body/message field is blank. We will have to decrypt this message in CipherMail.

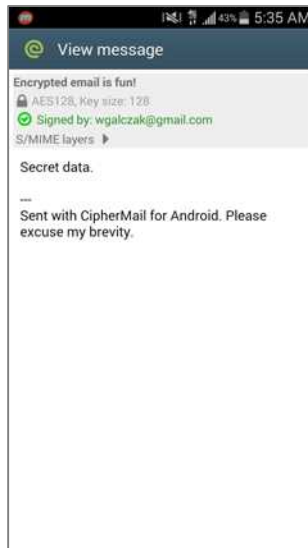


#### 4. Vulnerability: Email

2. Select the smime.p7m file. CipherMail will automatically open and request your key store password to use the keys you already have to try to decrypt the message. Enter your password and select *OK*.



3. If you have the key for the email, it will display the message.

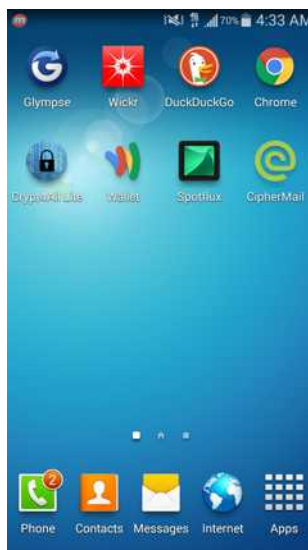


#### 4. Vulnerability: Email

### **Assignment: Send your S/MIME Certificate to Recipients in CipherMail**

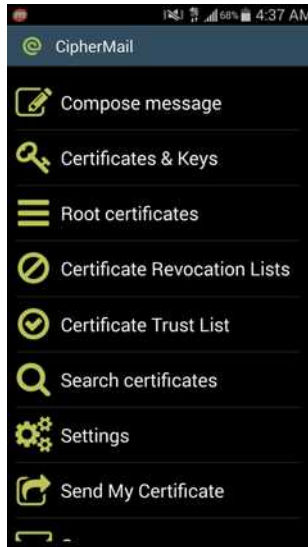
In order for recipients of your encrypted email to decrypt and read the message of your email they will need your certificate. Luckily, CipherMail comes with a nifty feature to send a .cer file, which will send your certificate to them. This will allow that recipient to be able to read any further emails that you have encrypted and sent to them.

1. From your Home Screen, select *CipherMail*.

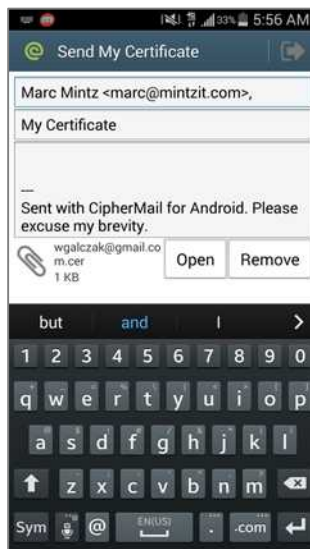


## 4. Vulnerability: Email

2. Select *Send My Certificate*.



3. Enter the recipient you would like to send your S/MIME certificate to and select the *Send arrow* in the upper right.

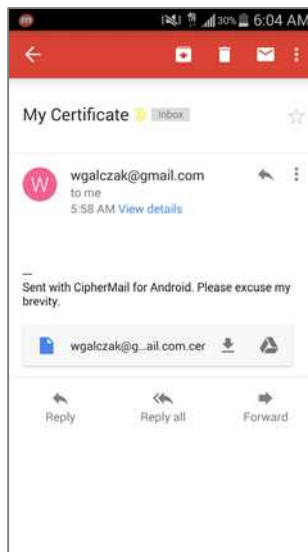


## 4. Vulnerability: Email

### Assignment: Import a Certificate to CipherMail

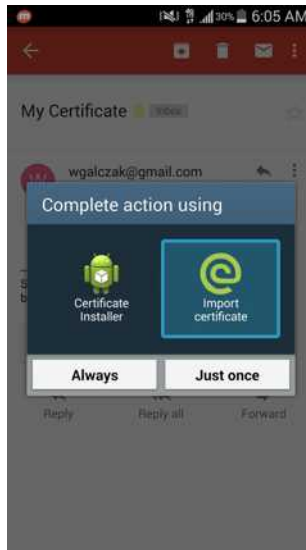
In order for you to read someone else's S/MIME encrypted email you will first need their certificate to decrypt the message. If when attempting to decrypt a message CipherMail alerts you that you do not have the certificate to decrypt the message you have been sent then follow these steps.

1. Request that the sender of the email send you their certificate (usually a .cer or .crt) in another email.
2. Open the email in your email app. Select the .cer file.

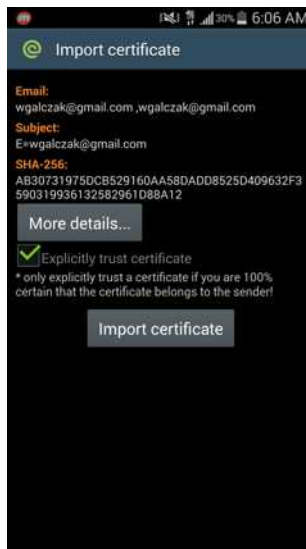


#### 4. Vulnerability: Email

3. When prompted to select an application to use to install the certificate, select the icon for CipherMail and select *Always*.

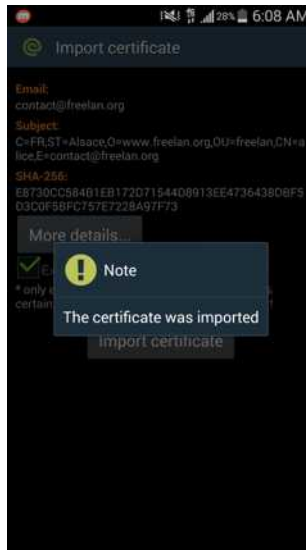


4. Verify that the email address matches the sender's email address at the top and if it indeed does, select *Import certificate*.



#### 4. Vulnerability: Email

5. When the certificate is successfully imported, the *The certificate was imported* alert will appear.



Congratulations! You can now view and decrypt messages from this sender.

## **Closing Comments on Encryption and the NSA**

Using S/MIME or secure email hosts will give 100% protection against your communications being intercepted or eavesdropped by pranksters, criminals, master criminals, and virtually all government personnel (my apology for being redundant.) The bad news is that the NSA may have the ability to bypass virtually any security system should the NSA take a strong enough interest. The question then becomes: *Am I someone of such strong interest to the NSA that they will focus their full legal (and illegal) powers upon me?* If so, you may want to consider a change of career or lifestyle.



## 5. Vulnerability: Google Account

*Even in the common affairs of life, in love, friendship, and marriage, how little security we have when we trust our happiness in the hands of others!*

–William Hazlitt

### Google Account

Every single day a Google account is hacked, allowing the hacker full access to the victim's Google account, including access to their calendar, contacts, and email. This is normally accomplished not by traditional black hat hacking, but with a bit of social engineering. All the hacker needed was to discover the victim's birthdate and email address associated with his Google account. With a quick email to Google saying something like, *I've forgotten my Google password and would like to reset it. Here is my birthdate and my email address*, the hacker was able to reset the Google password. With this, he could access the victim's data as if he were the victim himself.

Luckily, Google has implemented an optional Two-Step Verification (also referred to as a 2-Factor Authentication) process to harden your Google security. Adding this additional security layer makes it extremely difficult for anyone to hijack your Google account and make fraudulent purchases. This is a step I strongly recommend for all Google users.

Remember that every password can be broken. Your defense is to make it so difficult and time consuming to break that the hacker moves on to an easier target. The vast majority of security questions can be accurately guessed or broken through social engineering (*What is your birthday? In what city did your parents marry? What is the name of your first pet?* etc.) Both of these types of security are based on what you know. And if there is something that you know, someone else can know it as well. Unfortunately, even those you love and trust may occasionally use this information against you.

Google has implemented Two-Step Verification so that whenever you (or anyone else) sign in to your Google account to manage your account or purchase something from the Play Store from a new (unknown) device, a code is sent to your previously verified device. You are prompted to provide this code before the purchase or support can be made.

In the event that your Android device has been stolen or lost, you can log in to your Google account via a web browser to remove the device from the *Trusted* list.

## 5. Vulnerability: Google Account

### **Assignment: Create a Google Account**

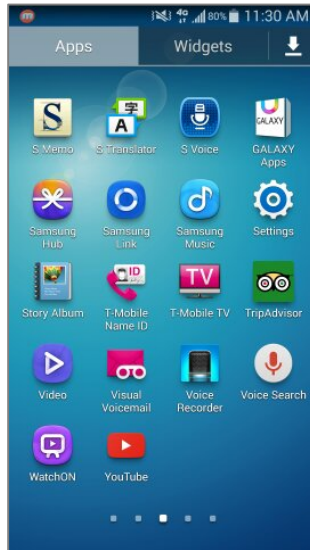
If you already have a Google Account, skip this assignment. If you do not already have a Google Account, no better time than the present to create one!

1. Select Apps/Applications.

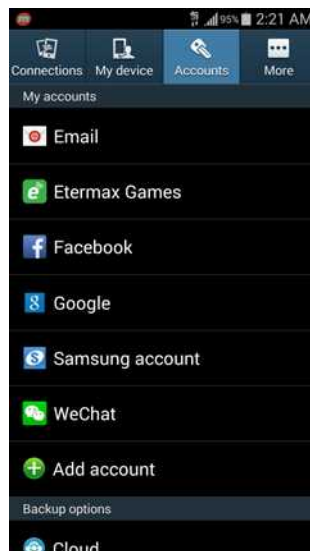


## 5. Vulnerability: Google Account

2. Select *Settings*.

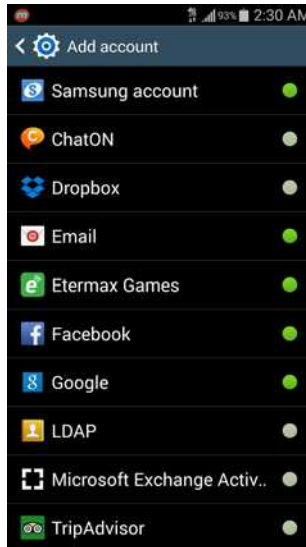


3. Select *Accounts > Add account*.

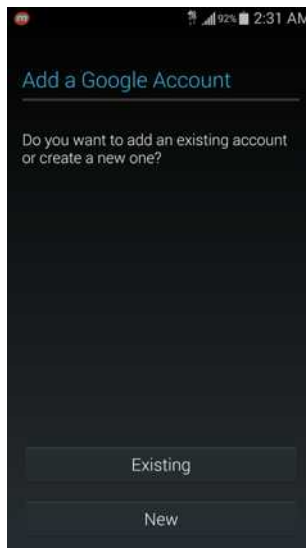


## 5. Vulnerability: Google Account

4. Select *Google*.



5. Select *New*.

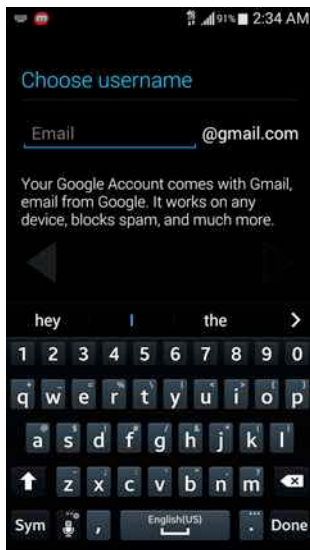


## 5. Vulnerability: Google Account

6. Enter your name, and then select *Next/Done*.

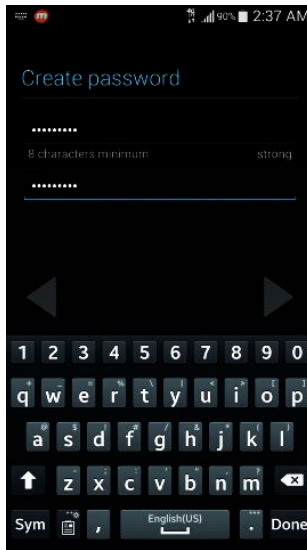


7. Enter a username, and then select *Next/Done*.

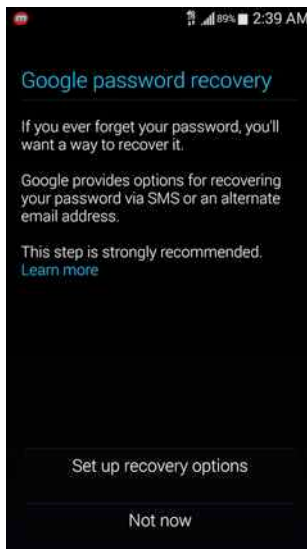


## 5. Vulnerability: Google Account

8. After Google checks your username for availability, enter a strong password and select *Next/Done*.

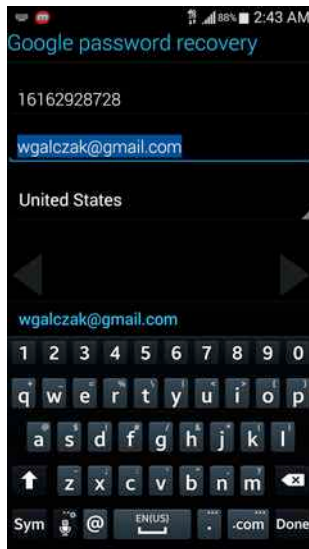


9. It is a very good idea to setup a recovery phone number or email address in case you forget your account information. Select *Set up recovery options*.

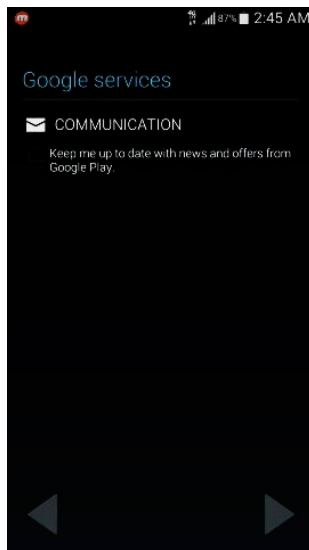


## 5. Vulnerability: Google Account

10. Enter your phone number and recovery email address, and then select *Next/Done*.



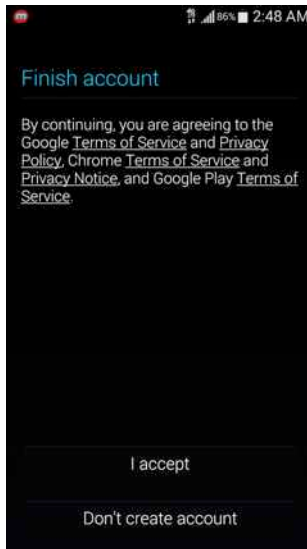
11. Select the *right arrow* to continue.



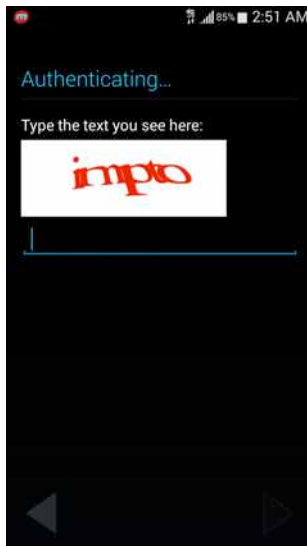


## 5. Vulnerability: Google Account

12. Gather your legal team to review the *Terms of Service* and then regardless of what they say, select *I accept*.



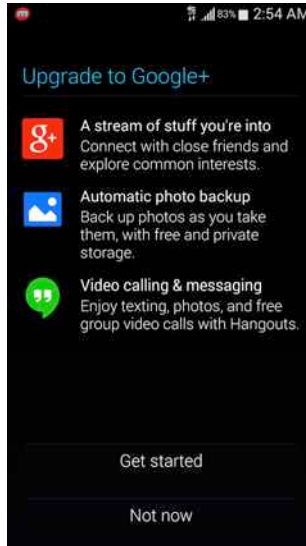
13. Enter the captcha and select the *right arrow* to continue.



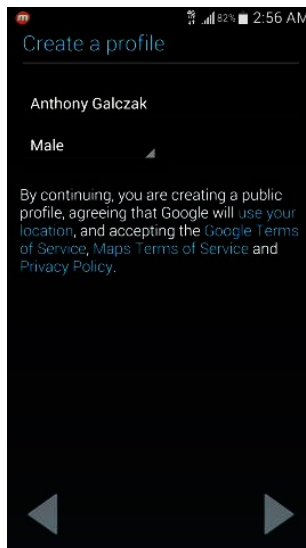
## 5. Vulnerability: Google Account

Congratulations, you have made a Google account! From this point I would recommend creating a Google+ account as well while you're at it. Google+ is the social network that runs across all of Google's services.

14. Select Get started.

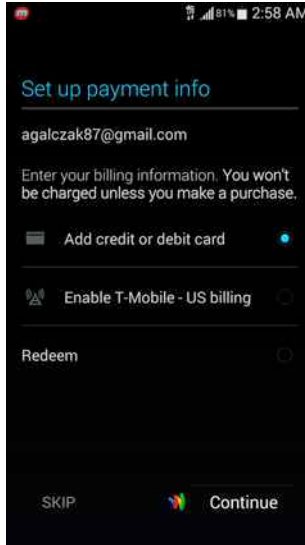


15. Select your gender and select the *right arrow* to continue.

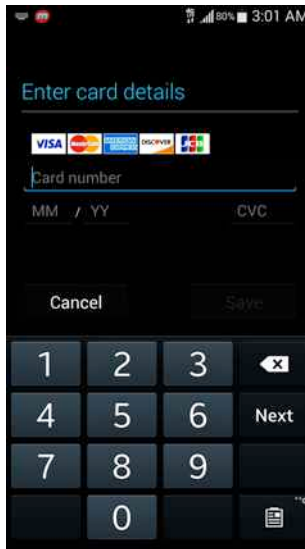


## 5. Vulnerability: Google Account

16. Now we'll setup an account for use in the Google Play Store. If you're able to use carrier billing, click that. Otherwise select *Add credit or debit card* and select *continue*.

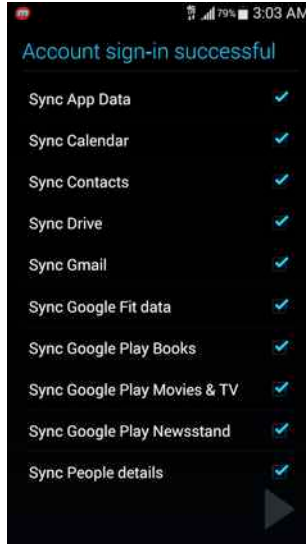


17. Enter your card information and zip code, and then select *Save*.



## 5. Vulnerability: Google Account

18. Select all the sync settings you would like to use. I recommend using all of them in case your phone is lost or stolen you will not lose any data. Select *right arrow* to continue.



Congratulations! You have successfully created a new Google ID with a Google+ account.

### **Assignment: Implement Two-Step Verification for Your Google Account**

If you have performed the previous assignment, you now have an active Google account. However, it's important to implement two-step authentication to prevent anyone from impersonating you to gain access to your Google account.

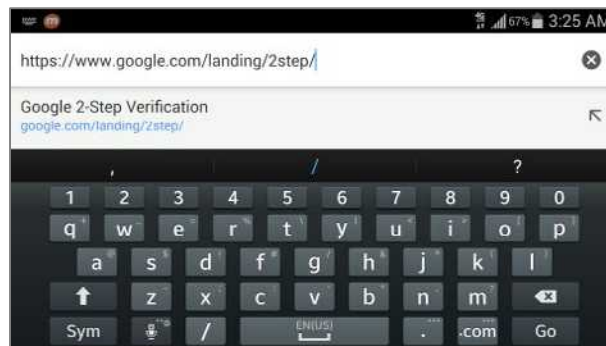
Two-step verification, also called two-factor authentication, helps to prevent someone else from pretending to be you to reset your Google account settings. Anytime significant settings are modified, you will receive an alert on your mobile phone. If you made the changes, ignore the alert. If you did not make the changes, the alert will provide a link to take security actions.

## 5. Vulnerability: Google Account

1. From your Home Screen, select *Chrome*.

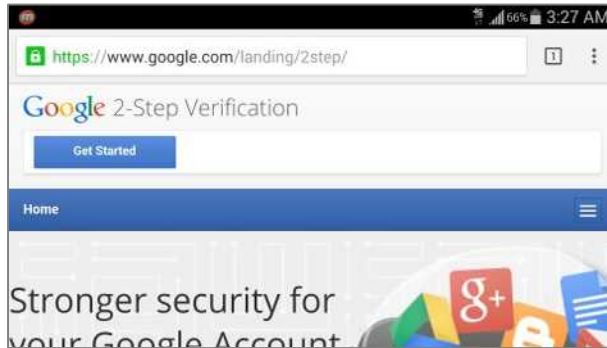


2. Type *https://www.google.com/landing/2step*, and then select *Go*.

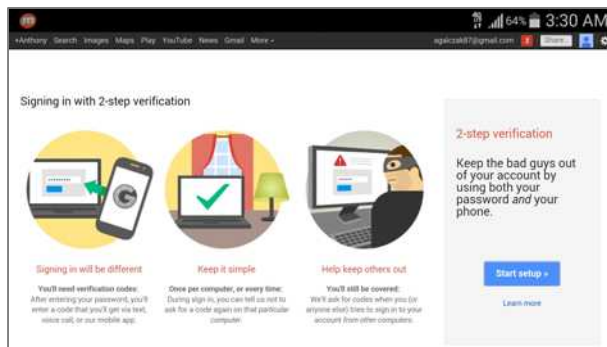


## 5. Vulnerability: Google Account

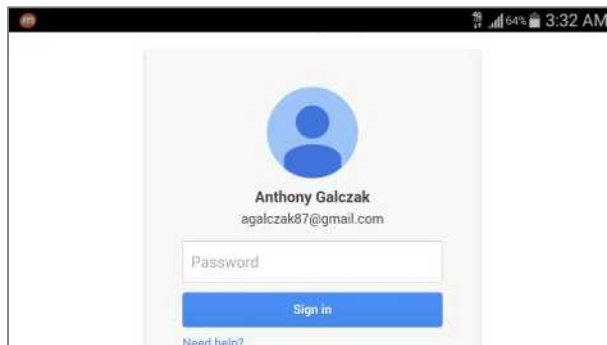
3. Select *Get Started*.



4. Select *Start setup*.

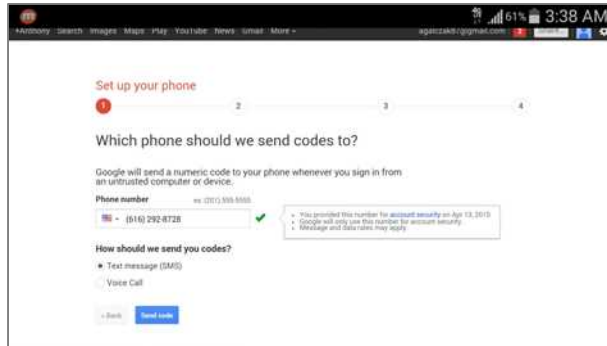


5. At the login screen, enter your password and select *Sign in*.

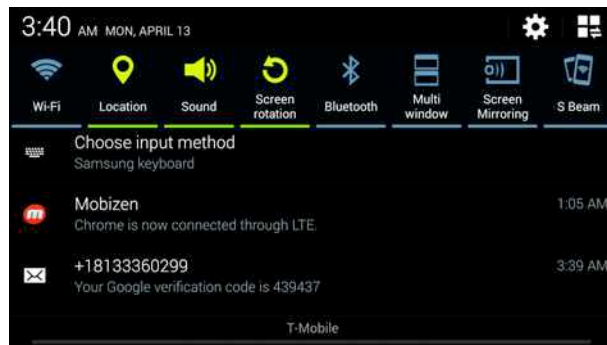


## 5. Vulnerability: Google Account

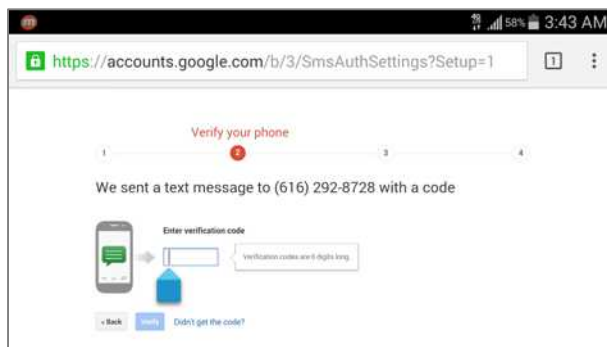
6. Confirm the phone number to send your authentication code to and select *Send code*.



7. You will receive a text message from Google with an verification code. Use the pull-down menu and write down the code.

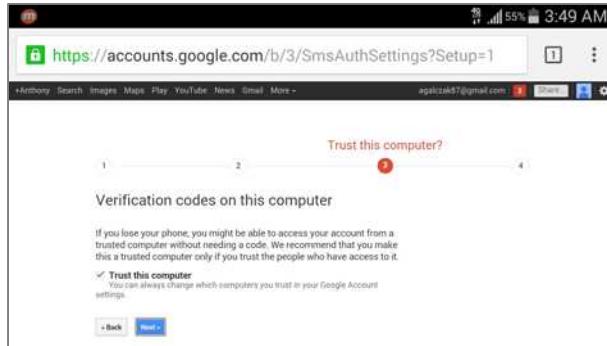


8. Pull the menu back up to reveal your browser, enter your verification code and select *Verify*.

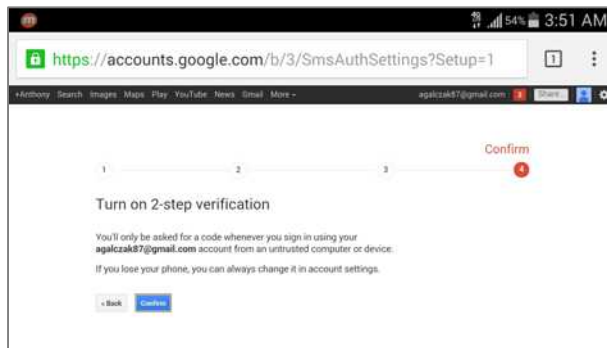


## 5. Vulnerability: Google Account

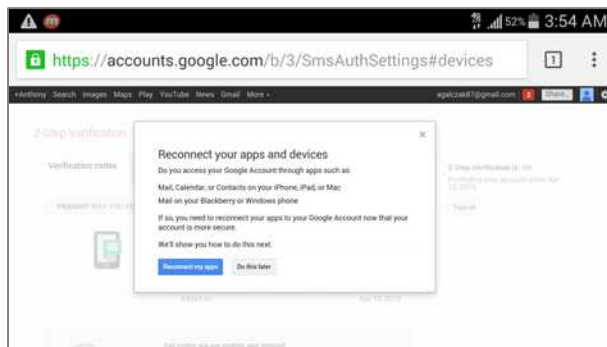
9. Leave the *Trust this computer* checkbox checked in case you need to access it later on. Select *Next*.



10. Select *Confirm*.



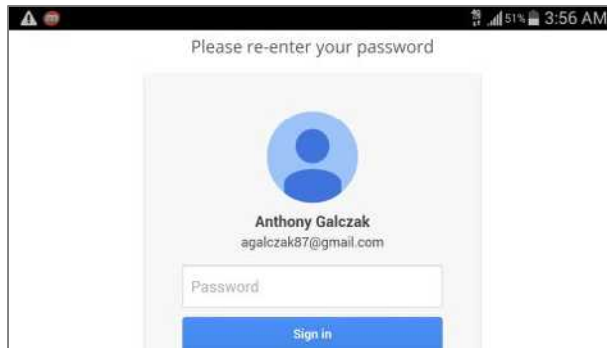
11. Apps and devices must be *Reconnected* if you are using your Google account on a non-Android device. Select *Reconnect my apps*.



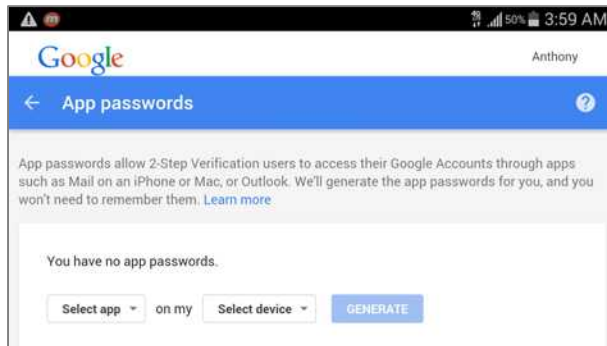


## 5. Vulnerability: Google Account

12. You will be prompted to login again as two-step verification is now on. Scroll down slightly, enter your password and select *Sign in*.

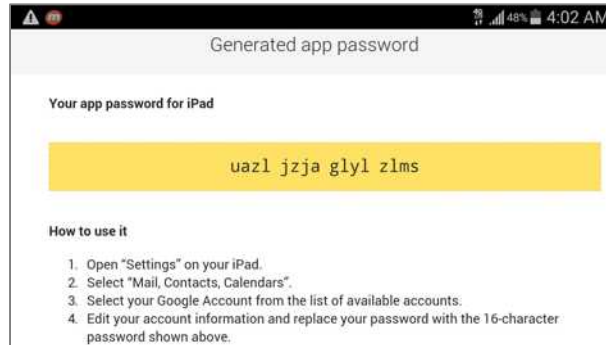


13. Any non-Google applications that you use to access your mail, calendar or contacts (ex. Mail on iPad) you will need to setup an *App password*. Select whichever app you'd like to generate a password for and select *Generate*.

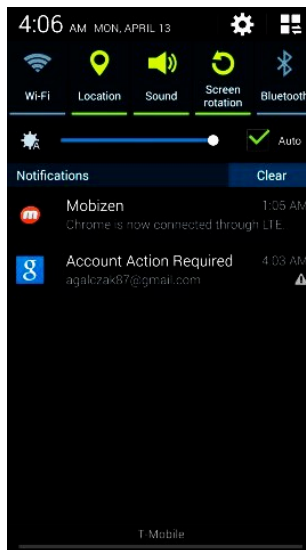


## 5. Vulnerability: Google Account

14. The next page will give a tutorial on how to use your app password for whatever app you would like to use to access your mail, calendar, or contacts. After reading this, scroll down slightly, and then select *Done*.

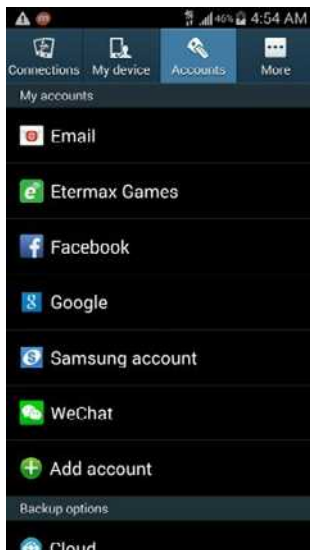


15. If you were signed into this Google account, it will now stop working on your phone. Remove the account and re-add it in order to set your device as trusted. Press the *Home* button, select *Apps/Applications*, and then *Settings*. If you were not already signed into the account, skip to step 19 in this activity.

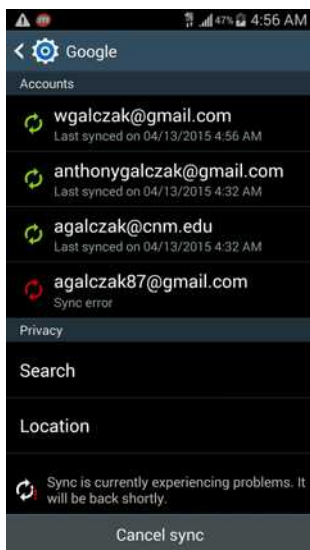


## 5. Vulnerability: Google Account

16. Select Accounts > Google.

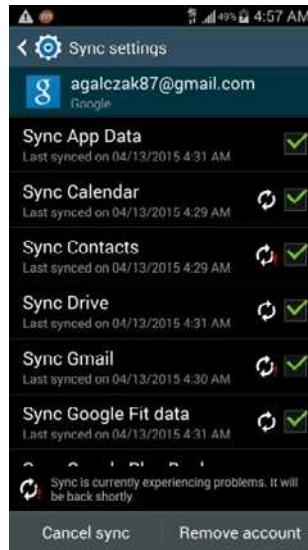


17. Select the account for which you have setup two-step verification.

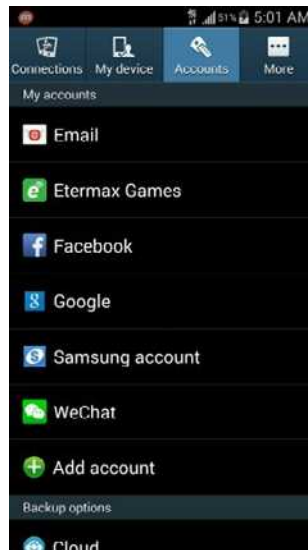


## 5. Vulnerability: Google Account

18. Select *Remove account* twice. (Notice the sync is broken due to two-step verification being turned on)

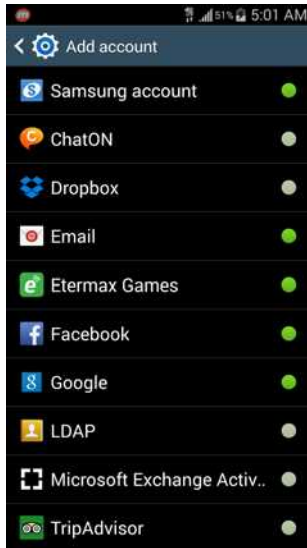


19. Press the *Back* button once, and select *Add account*.

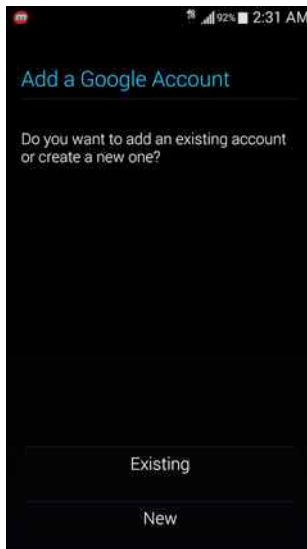


## 5. Vulnerability: Google Account

20. Select *Google*.

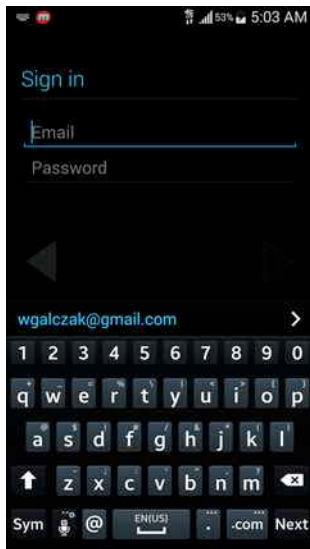


21. Select Existing.

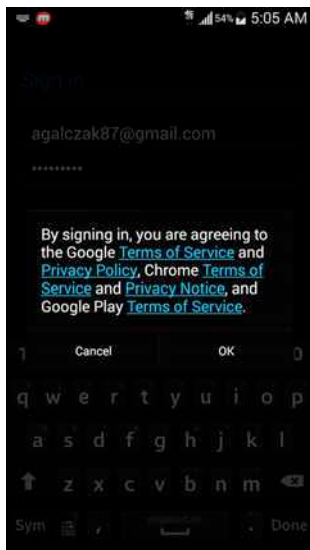


## 5. Vulnerability: Google Account

22. Enter your email and password for your account and select *Next/Done*.

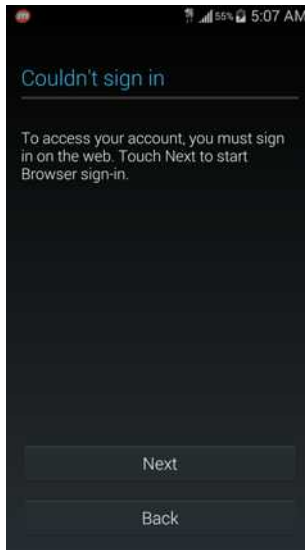


23. Select *OK* to accept the *Terms of Service*.

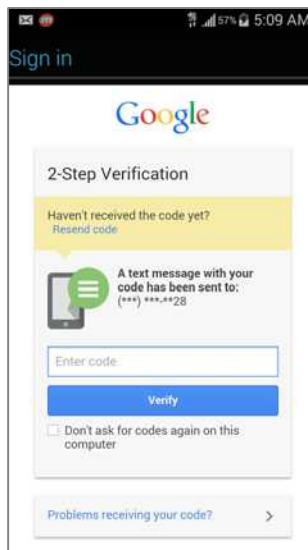


## 5. Vulnerability: Google Account

24. While signing in, it will identify you have two-step verification on. Select *Next* to continue to a web browser verification.

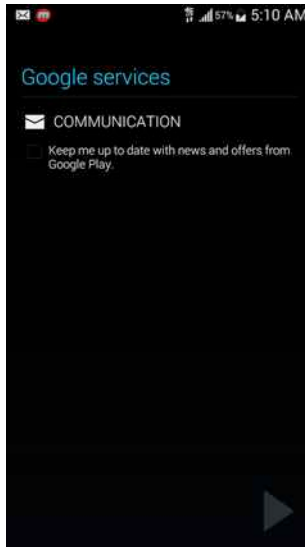


25. You will receive a text message with your verification code. View this message via the Pull-Down Menu, enter it into the *Enter code* text field, and then select *Verify*.

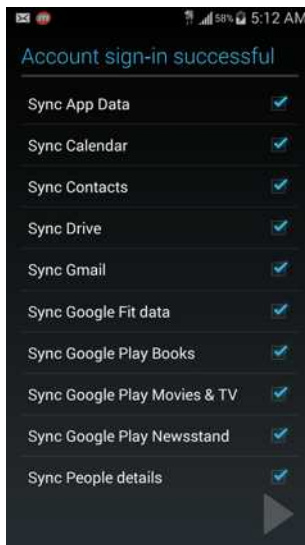


## 5. Vulnerability: Google Account

26. Select the *right arrow* to continue.



27. Select all the sync settings you would like to use and select the *right arrow* to finish setting up your account.





## 5. Vulnerability: Google Account

Congratulations! You have made it through one of the more difficult tasks to secure your Android device, making it virtually impossible for anyone to impersonate you to Google, thereby preventing anyone from gaining access to your Google account information!



## 6. Vulnerability: Documents

*Tradition becomes our security, and when the mind is secure it is in decay.*  
-Jiddu Krishnamurti

### Document Security

In the Android world, there is currently no hardware encryption built into the device, so it is necessary to use an additional application to encrypt individual files. Hardware encryption will be included in the upcoming Lollipop (5.0) update. For individual files it is very simple to encrypt and decrypt them. The application I recommend for document encryption is called *Crypt4All Lite*. Crypt4All Lite uses military-grade 256-bit encryption.

#### Assignment: Install Crypt4All Lite

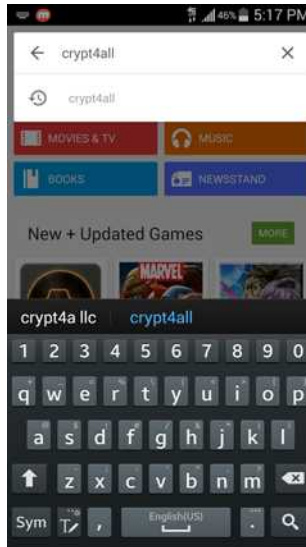
First, we need to install *Crypt4All Lite* from the *Play Store*.

1. From your Home Screen, select *Play Store*.

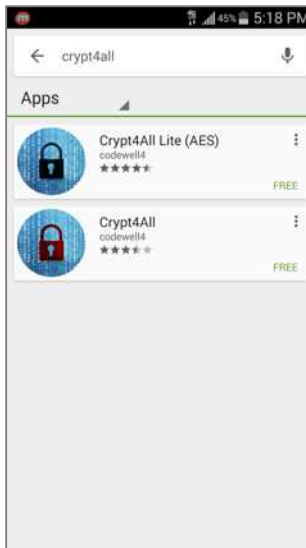


## 6. Vulnerability: Documents

2. Enter *Crypt4All* into the top search bar and select the *Search* button.



3. Select *Crypt4All Lite (AES)*.

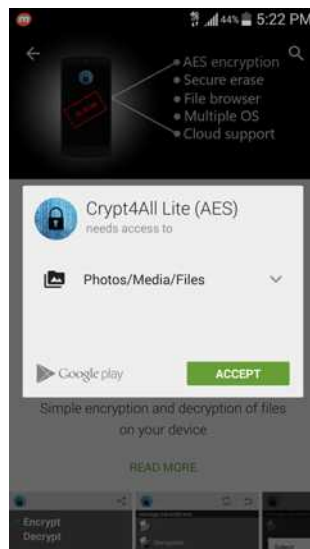


## 6. Vulnerability: Documents

4. Select Install.



5. *Accept* the access requirements.



## 6. Vulnerability: Documents

6. Congratulations! You have successfully installed *Crypt4All Lite*.

### **Assignment: Encrypt a File with Crypt4All Lite**

In this assignment we will encrypt the sensitive data that you would like to protect. Each file is individually encrypted, so you will have to do this process for each file to be protected.

You will need to be somewhat familiar with the directory structure of your device as that is how you will find your files and encrypt them. Your pictures are usually located in the main directory / *DCIM* folder. Freshly downloaded files and folders will be located in the *Download* folder. If you are looking for your SD card data, press the *Back* button twice to get to /*storage* which will contain *extSdCard* which is your SD card's data.

1. From your Home Screen, select *Crypt4All Lite*.

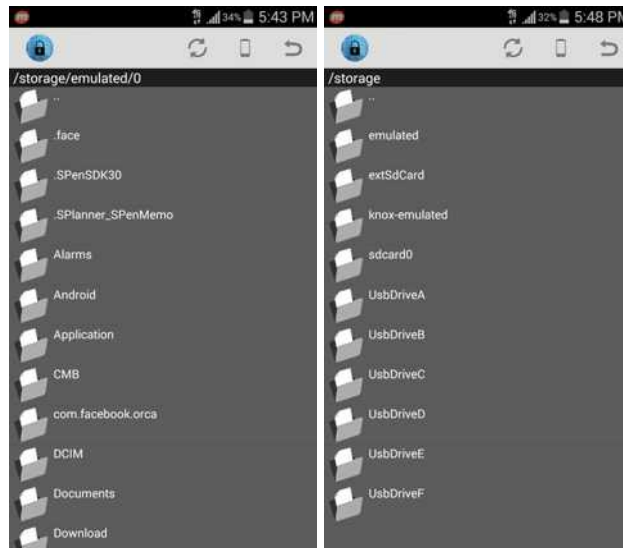


## 6. Vulnerability: Documents

2. Select the *Folder* button to the right of *File path* and the *x* to browse to your file you'd like to encrypt.



3. This will start you in the root phone directory. For the sake of this example I will navigate to a picture in my SD card's DCIM (Pictures) folder.



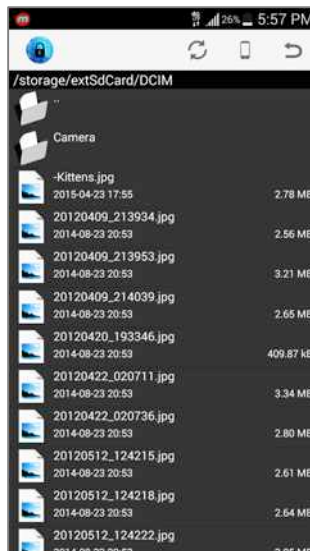


## 6. Vulnerability: Documents

4. Select the folder that contains your file you'd like to encrypt. (In this case I'm selecting *extSdCard* and then *DCIM*.)

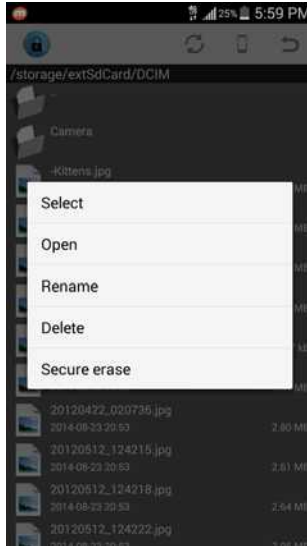


5. Select the file you'd like to encrypt. (In this case it will be *Kittens.jpg*)

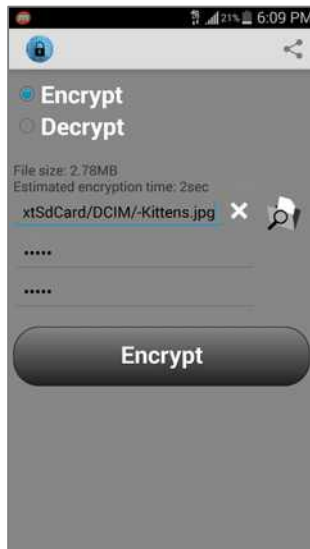


## 6. Vulnerability: Documents

6. Select *Select* to set this file for encryption.

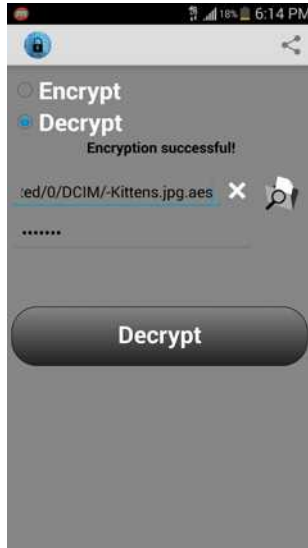


7. Enter a strong password into the *Password* and *Confirm password* fields, and then select *Encrypt*.



## 6. Vulnerability: Documents

- When the encryption process completes, the application will display *Encryption successful!*. At this point your file has been encrypted as an .aes file. Remember the password you used to encrypt this file, as you will need it to decrypt it in the future.



Congratulations, you have encrypted your first file with AES encryption!

### **Assignment: Decrypt a File with Crypt4All Lite**

In this assignment we will decrypt a file that has been encrypted with *Crypt4All Lite*, whether it is a file you have encrypted, or a file sent to you as an .aes file. An .aes file will not be readable by other applications until it is decrypted.

## 6. Vulnerability: Documents

1. From your Home Screen, select *Crypt4All Lite*.

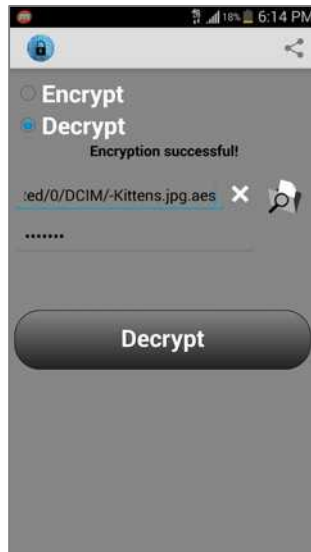


2. Select *Decrypt* at the top to set Crypt4All Lite into decrypt mode.

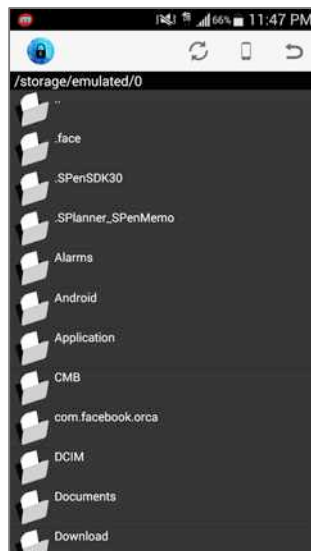


## 6. Vulnerability: Documents

3. Select the *Folder* button to the right of *File path* and the *x* to browse to your file you'd like to decrypt.

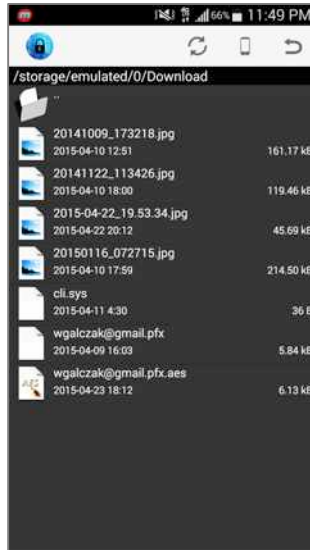


4. For this example I have encrypted my S/MIME certificate in my Download folder, so I am going to navigate to *Download*. Navigate to whatever file path your file is in.

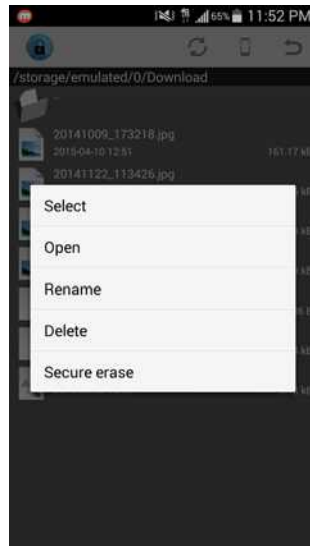


## 6. Vulnerability: Documents

5. Select the file you'd like to decrypt. The file should end in *.aes* signifying it's encrypted with AES encryption.

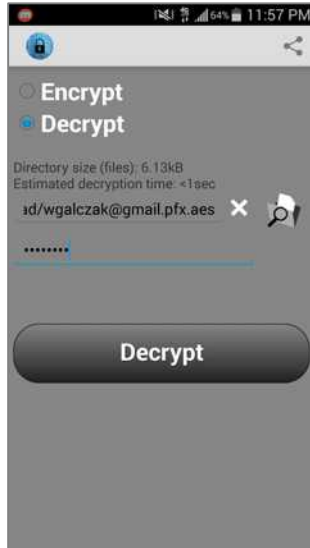


6. After selecting the file, a dialog box will appear. Select *Select* to set the file.



## 6. Vulnerability: Documents

7. At this point your file will be selected and show its name and file path. Enter the password for this file and select *Decrypt*. Keep in mind if you already have a file with the exact name, but without *.aes* it will not be able to decrypt the file again.



8. When successful, *Decryption successful!* will display. Congratulations!



## 6. Vulnerability: Documents

### **Assignment: Secure Erase a File with Crypt4All Lite**

When dealing with sensitive data requiring encryption, you will often want to be able to securely erase the file after it has been used and no longer needed. Luckily Crypt4All Lite comes with a Secure erase feature. I would recommend using this feature whenever you have used a sensitive piece of data and no longer need it, whether this is the encrypted .aes file or the decrypted data. This feature can also be used for any other file type, which is often important when dealing with HIPAA, SEC, or legal requirements.

1. From your Home Screen, select *Crypt4All Lite*.



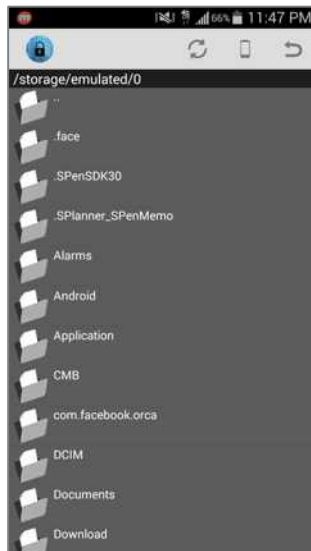


## 6. Vulnerability: Documents

2. Select the *Folder* button to the right of *File path* and the *x* to browse to your file you'd like to decrypt.

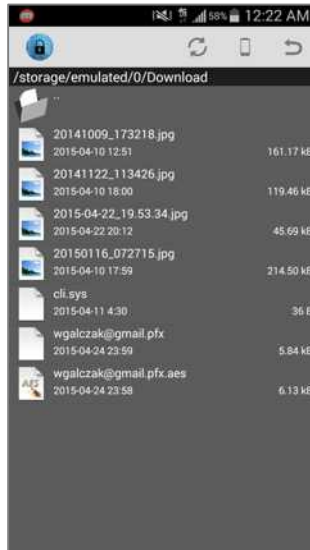


3. Browse to the file you would like to securely erase. In this example, I am going to delete my encrypted S/MIME file inside the download folder.

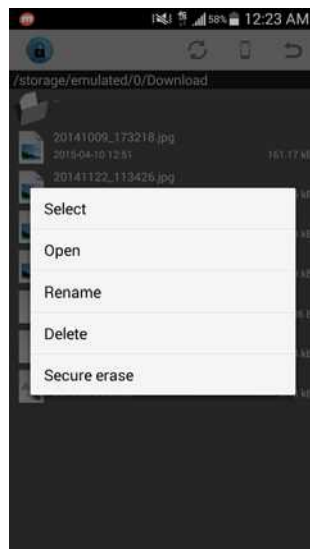


## 6. Vulnerability: Documents

4. Select the file you'd like to securely delete.

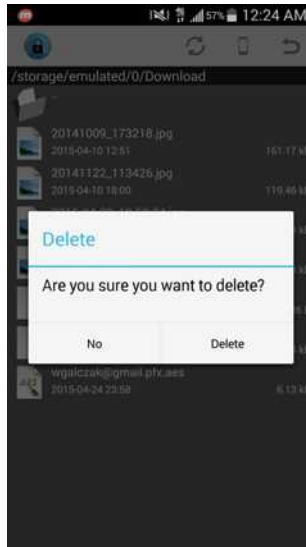


5. Select Secure erase.

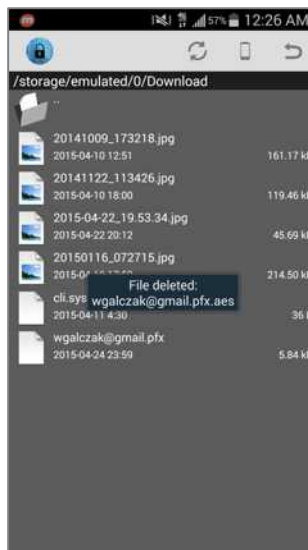


## 6. Vulnerability: Documents

6. For your safety, it will confirm your deletion. Select *Delete*.



7. After successful deletion, the app will display *File deleted*.



Congratulations, your sensitive data has been deleted and kept from the wrong hands, even if your device hasn't.

## 6. Vulnerability: Documents

### Assignment: Encrypt an SD Card

It is common to store data on your SD card. With all of your important pictures, documents and other data on your SD card, it is important to protect this data from prying eyes. If your phone is physically compromised through theft or loss, or if there is a software compromise, the best way to secure your sensitive data is to encrypt it.

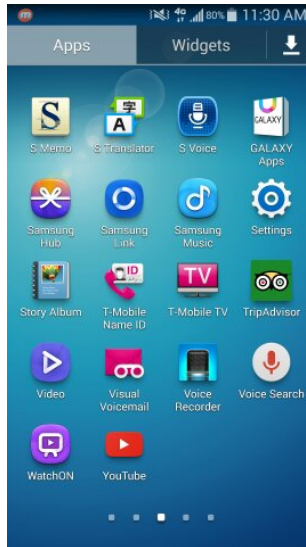
In this assignment we will encrypt your SD card.

1. From your Home Screen, select *Apps / Applications*.

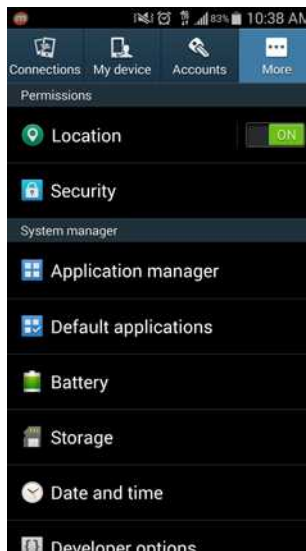


## 6. Vulnerability: Documents

2. Select Settings.



3. Select More > Security.

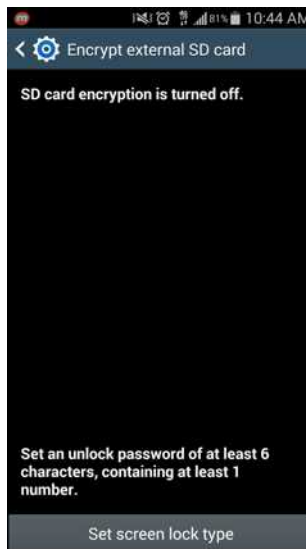


## 6. Vulnerability: Documents

4. Select Encrypt external SD card.

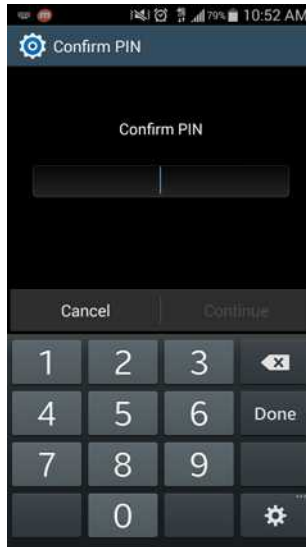


5. In order to use SD card encryption, you will need to set a screen lock type of a Password that is at least 6 characters long and includes 1 number. Select *Set screen lock type*. If you already have a strong password, skip to step 9.



## 6. Vulnerability: Documents

6. Confirm whatever security type you have set, and then select *Done* or *Continue*.

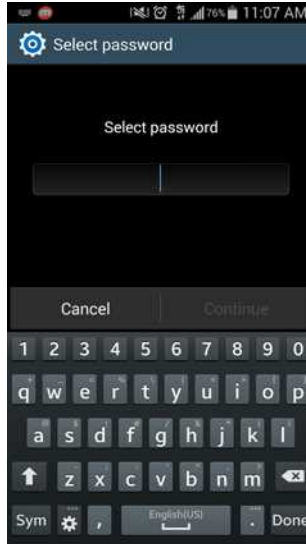


7. Select Password.

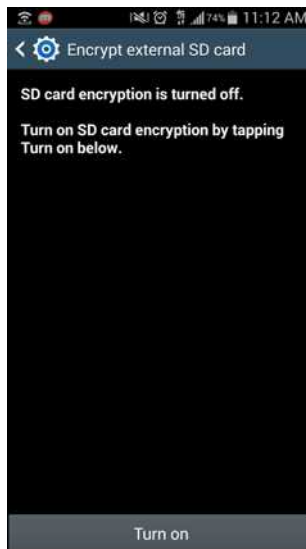


## 6. Vulnerability: Documents

8. Enter a strong password that is at least 6 characters and includes 1 number. After entering a strong password, select *Done* or *Continue*. Confirm the password, then select *Done* or *Continue* again to continue.



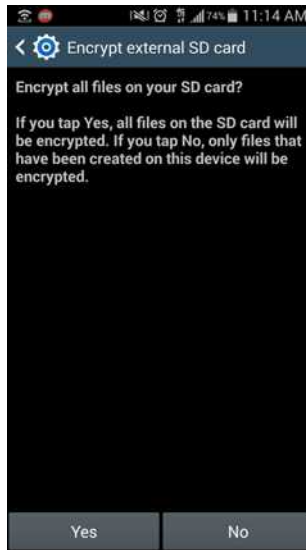
9. Select *Turn on* to turn on SD card encryption.





## 6. Vulnerability: Documents

10. On this screen it will confirm that you'd like to encrypt your entire SD card. Select *Yes*.

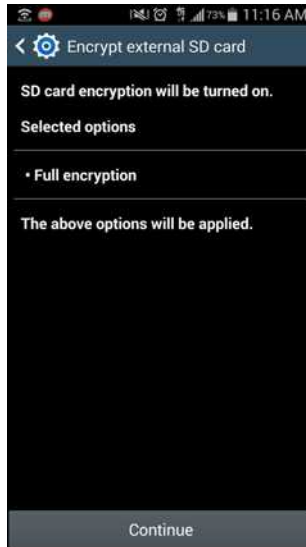


11. I recommend that you also encrypt your multimedia files. Select *No*.

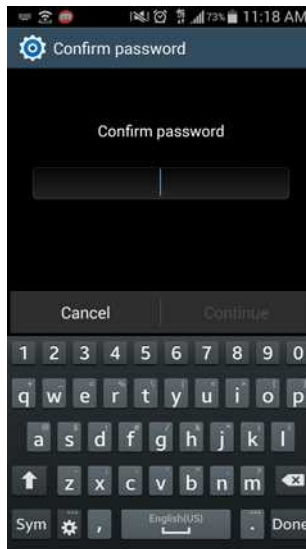


## 6. Vulnerability: Documents

12. On this screen, your level of encryption will be listed. Select *Continue*.



13. Confirm your password, then select *Done* or *Continue* to continue.

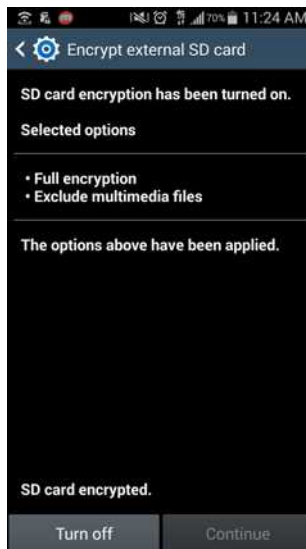


## 6. Vulnerability: Documents

14. This screen will confirm that you would like to turn on SD card encryption. Read all of the information regarding encryption and then select *Apply*.



15. After encryption is complete, the device will display *SD card encrypted*. Congratulations! You have successfully encrypted your SD card.





## **7. Vulnerability: Text Messaging**

*The ignorance of one voter in a democracy impairs the security of all.*  
-John F. Kennedy

## Text Messaging

In 2009 the CTIA <[http://en.wikipedia.org/wiki/CTIA\\_-\\_The\\_Wireless\\_Association](http://en.wikipedia.org/wiki/CTIA_-_The_Wireless_Association)> reported that US cellphone subscribers send an average of 534 text messages a month. AT&T reported in 2012 that their subscribers under 25 years old averaged 5 times this number!

And if the raw number of texts isn't mind-numbing enough, the topics of discussion most certainly are. With few people giving any thought to the facts that:

- Your cellular provider likely archives your text messages for years.
- The government has full access to all of your messages and also archives them.
- The encryption scheme used by cellular providers was broken years ago, and any kid can listen in on your messaging.
- If you are in business, it is possible the competition listens in on your messaging.
- If you are involved with healthcare and text *any* patient information—even to the patient—you are probably in violation of HIPAA compliance and may be subject up to a \$50,000 fine.

Unless you are texting innocuous comments, such as: *I love you* (assuming this is a relationship in the open), *remember to bring home milk*, or *I'll be home by 6pm*, your texting should be secure by way of encryption.

The texting app included with Android—*Messages*—is not secure and does not automatically encrypt your information. The Google included app called *Hangouts* does provide basic encryption. To ensure the security of your communications, I recommend use of another utility.

There are a few texting apps that meet military and HIPAA requirements for security and encryption. One of our favorites is *Wickr*. That fact that it works well, allows for the sender to set a time of auto-destruct, works with Android, iOS, Linux, OS X, and Windows, and is free helps to put it at the top of the list.

## 7. Vulnerability: Text Messaging

If there is a downside to Wickr, it is that you can only communicate securely with others who are also using Wickr. But this is the nature of the security beast.

### **Assignment: Install and Configure Wickr**

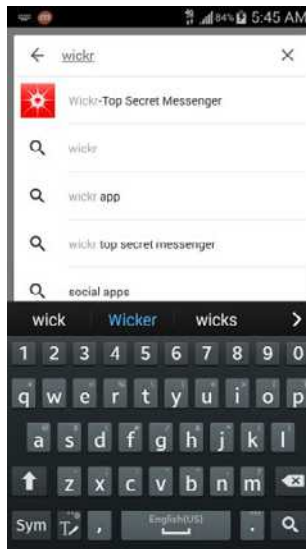
In this assignment we will be install and configure Wickr to create secure, encrypted text communications.

1. From your Home Screen, select *Play Store*.

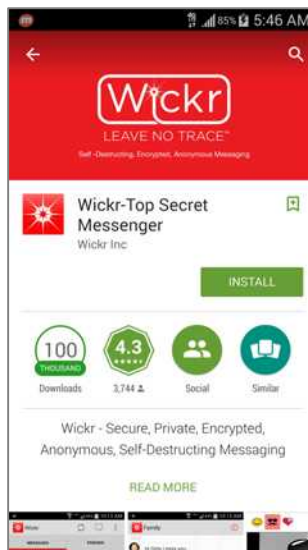


## 7. Vulnerability: Text Messaging

2. Enter *Wickr* into the search bar, and then select *Wickr-Top Secret Messenger*.



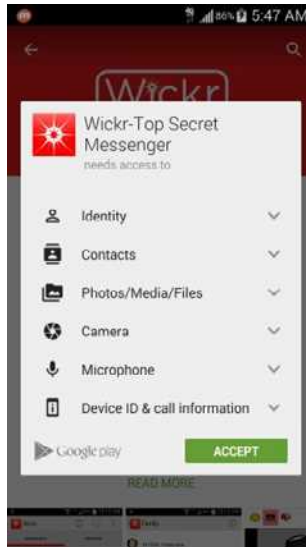
3. Select *Install*.



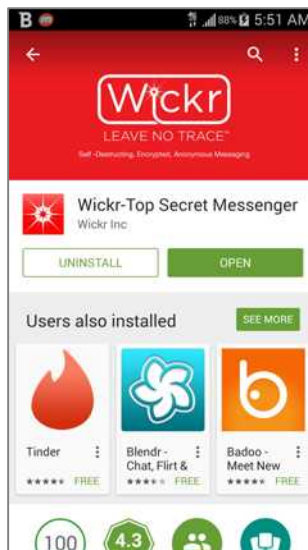


## 7. Vulnerability: Text Messaging

4. *Accept* the access requirements.



5. Select *Open* to open Wickr.

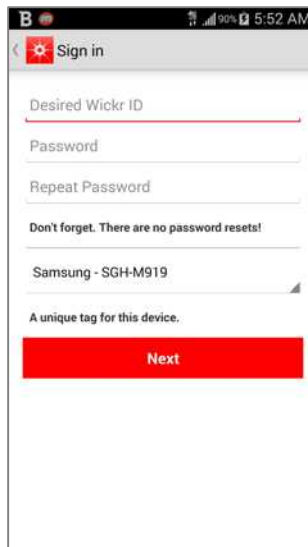


## 7. Vulnerability: Text Messaging

6. Select *New Account* to setup a new Wickr username and password.

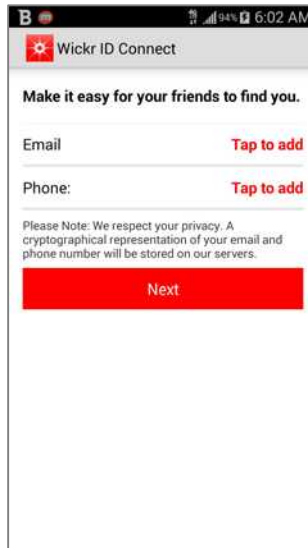


7. Enter your new Wickr ID and password, a name for your device, and then select *Next*.

A screenshot of a mobile application interface. At the top, there is a status bar with a battery icon, signal strength, 99% battery, and the time 5:52 AM. Below the status bar is a grey header with a red gear icon and the text "Sign in". The main content area contains several input fields: "Desired Wickr ID", "Password", and "Repeat Password". Below these fields is a warning message: "Don't forget. There are no password resets!". Underneath is a dropdown menu showing "Samsung - SGH-M919". Below the dropdown is the text "A unique tag for this device." and a large red button with the white text "Next".

## 7. Vulnerability: Text Messaging

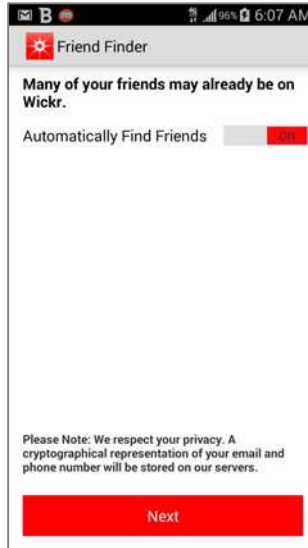
8. Wickr will secure your device and process the information. When this completes, you will be taken to the *Wickr ID Connect* page. Enter your email address and phone number so that other Wickr users will have an easier time finding you. When complete, select *Next*.
  - Note: Wickr will send a verification email and text message to the addresses you specify. Reply to this email and text so that your address will be included in the Wickr database, allowing others to find you. You can also use multiple email addresses and phone numbers if necessary.



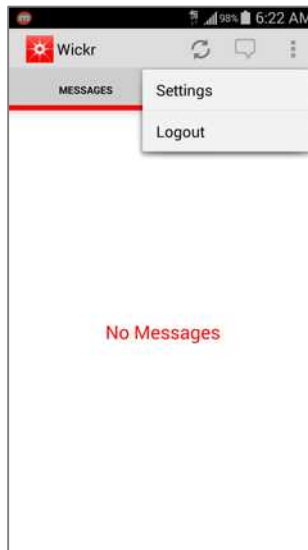
The screenshot shows a mobile application interface titled "Wickr ID Connect". At the top, there is a status bar with a battery icon, signal strength, and the time "6:02 AM". Below the title bar, the text "Make it easy for your friends to find you." is displayed. There are two input fields: "Email" and "Phone:", each with a red "Tap to add" button to its right. Below these fields, a "Please Note" section states: "We respect your privacy. A cryptographical representation of your email and phone number will be stored on our servers." At the bottom of the form, there is a prominent red button labeled "Next".

## 7. Vulnerability: Text Messaging

9. After confirming the email from Wickr, the *Friend Finder* will ask if you'd like to automatically find friends. I'd recommend doing this, as it will search for the names and email addresses of contacts you already have in your phone.

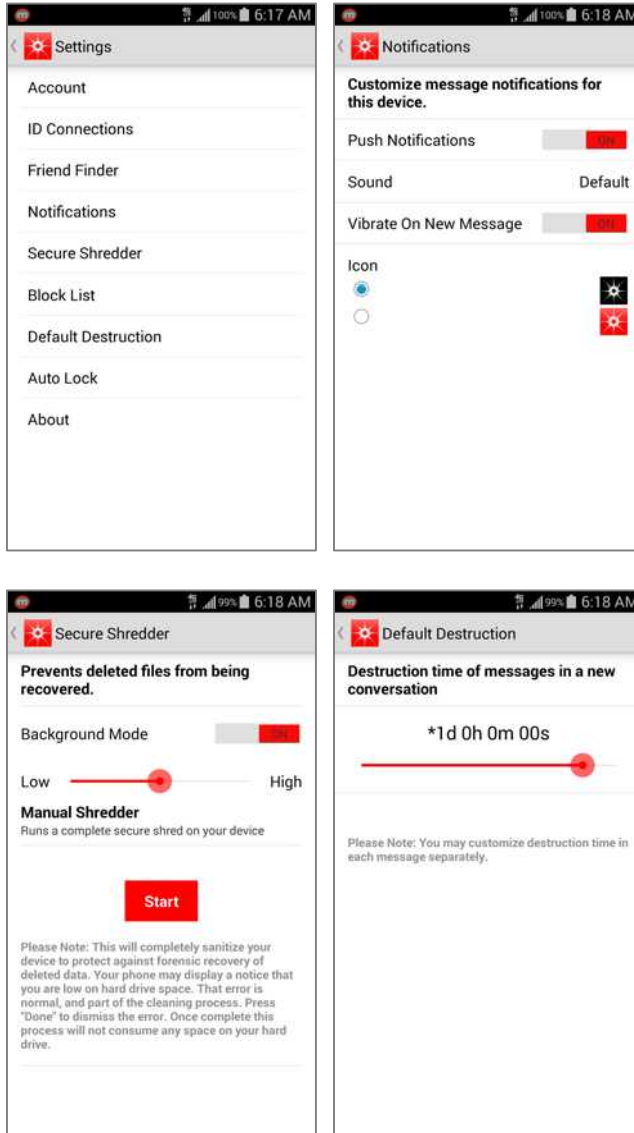


10. Select the *Menu* key in the upper right, and then select *Settings*.



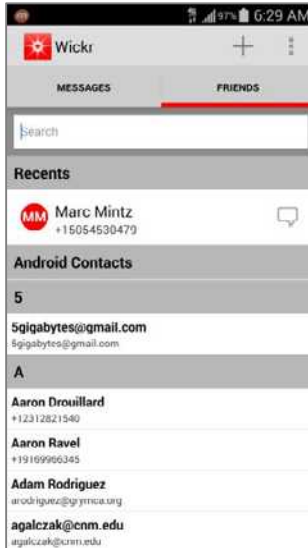
## 7. Vulnerability: Text Messaging

11. You may configure Wickr to taste. Here are my recommended settings.



## 7. Vulnerability: Text Messaging

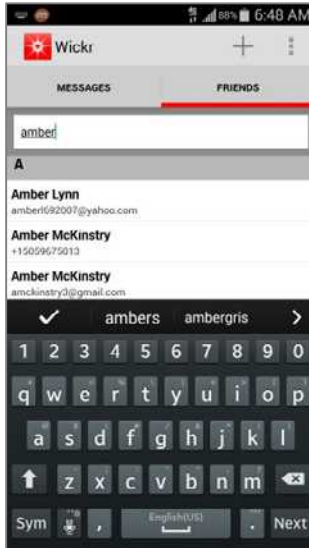
12. In order to use Wickr, those you wish to text with must also have a Wickr account and Wickr installed on their device. Our next step is to start inviting friends to use Wickr. Select the *Friends* button at the top right.



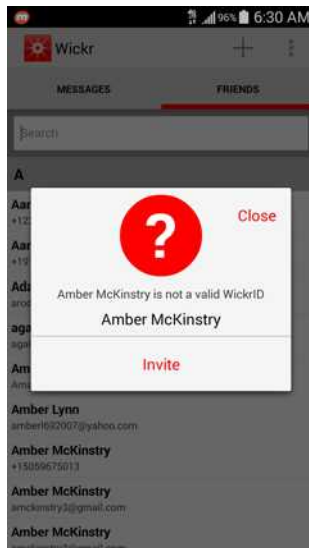
13. To add a friend who already has a Wickr account to your Wickr friends list, select the Add Friend icon in the very top right corner.

## 7. Vulnerability: Text Messaging

14. To add a friend who does not yet have a Wickr account, search for the contact either using the search function or scrolling down to the contact and selecting it. Select the contact you'd like to invite to Wickr.

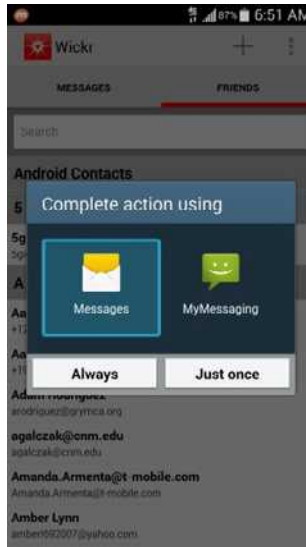


15. Select *Invite*.

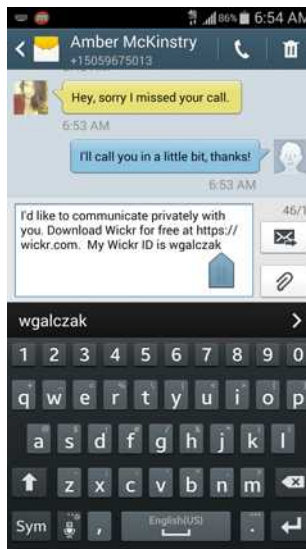


## 7. Vulnerability: Text Messaging

16. Select whichever messaging application you would like to use and select *Always*.



17. A text window opens, addressed to their cell phone, inviting them to download Wickr, and provides your Wicker ID. If you'd like to email them an invitation, select their email address on their contact.





## 7. Vulnerability: Text Messaging

Your Wickr account and app are now fully configured and ready to send and receive securely encrypted text messages.

### **Assignment: Send a Secure Text Message with Wickr**

Once you have Wickr configured, it's time to take it out for a test drive. You will need to have at least one other friend with a Wickr account with whom to text.

1. From your Home Screen, select *Wickr*.



## 7. Vulnerability: Text Messaging

2. The Wickr login page opens. Enter your password, and then select *Done*.

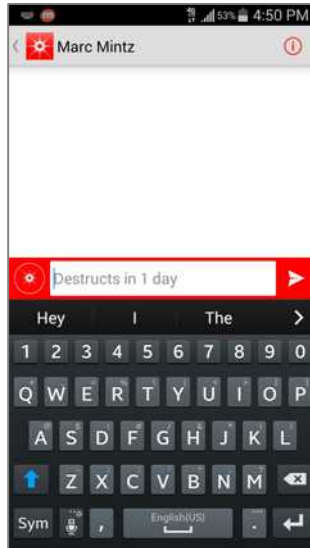


3. From the *Messages* screen, select the contact you'd like to message.



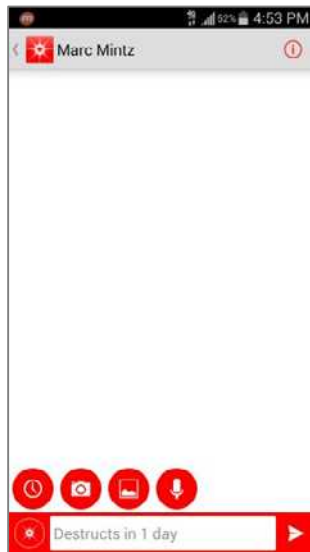
## 7. Vulnerability: Text Messaging

4. A new conversation window opens addressed to this person. Your message will self-destruct after your default set time.



## 7. Vulnerability: Text Messaging

5. Select the Compass icon on the left side of the screen to display additional options.
  - *Timer* allows you to set the time until self-destruct.
  - *Photo* allows you to take a new picture and attach it to your message, or attach an existing photo from your library to the message.
  - *Attach* allows you to attach a file to the message.
  - *Audio* allows you to attach an audio clip to the message.



## 7. Vulnerability: Text Messaging

6. If you would like to change the self-destruct time, select the timer button.



7. Press *x* to exit the self-destruct menu.
8. In the Message field, enter your message (the message field initially displays the self-destruct time.)
9. Select the *Send* button. Your friend will receive your fully encrypted message in seconds!

Great job! You, your friends and business associates may now exchange securely encrypted text messages.



## 8. Vulnerability: Internet Activity

*If you have built castles in the air, your work need not be lost; that is where they should be. Now put the foundations under them.*

–Henry David Thoreau, Walden

## Virtual Private Network

In case you have been sleep reading through this book, let me repeat my wake-up call: *They are watching you on the Internet.* They may be the automated governmental watchdogs, government officials, bored staff at an Internet Service Provider or broadband provider, a jealous (and slightly whackadoodle) ex, high school kids driving by your home or office or sitting on a hill several miles away, or thieves and other criminals.

Regardless, your device and data are at risk.

Perhaps one of the most important steps that can be taken to protect you, your device, and your data, is to encrypt the entire Internet experience all the way from your computer, through your broadband provider, to a point where your surfing, chat, webcam, email, etc. cannot be tracked or understood. This is accomplished using a technology called *VPN–Virtual Private Network*.

VPN <[http://en.wikipedia.org/wiki/Virtual\\_private\\_network](http://en.wikipedia.org/wiki/Virtual_private_network)> has been used for years as a way to securely connect multiple locations for an organization into one secure network. More recently it has been used to allow work-at-home staff to remain securely connected to the office.

The concept works like this:

1. Your computer has VPN software installed and configured to connect to a VPN server at the office. This server is connected to your office network. OS X comes with VPN software built into the Network System Preferences that works with many of the commercially available VPN servers, including the most popular–Cisco. Other VPN servers require their own proprietary client software to be installed.
2. On your computer you open the VPN software and instruct it to connect to the VPN server. This typically requires entering your authentication credentials of user name and password, along with a long key.
3. The VPN server authenticates you as an allowed account and begins the connection between itself and your computer.



## 8. Vulnerability: Internet Activity

4. As you send data from your computer to the network connected to the VPN server (typically the regular business network), all of it is military-grade encrypted. When the data is received at the VPN server or at your computer, the VPN software decrypts it.
5. Once your data reaches the VPN server, it is then forwarded to the appropriate service on your organizations network (file server, printer, mail server, etc.)

Although this may sound a bit complex, all a user must do is enter a name, password, and key. Everything else is invisible. The only indicator that anything is different is that the speed of large file transfers is somewhat slower than normal. This is due to the overhead of encryption/decryption process.

We can use this same strategy to securely surf the Internet, but the workflow is just slightly different:

1. Your device has VPN software configured to connect to a VPN server that is not associated with your office, but is just another server on the Internet.
2. On your device, open the VPN software and instruct it to connect to the VPN server. If you are using our recommended software, it is pre-configured with all the settings necessary—nothing much more to do but launch.
3. The VPN server authenticates you as an allowed account and begins the connection between itself and your computer.
4. As you surf the web, all data is military-grade encrypted. When the data is received at the VPN server or your computer, the VPN software decrypts it.
5. Once your data reaches the VPN server, it is then forwarded to the appropriate service on the Internet.

Using this strategy (a VPN Internet server), all of your browser traffic is military-grade encrypted in both directions. It is not possible to decipher any of your traffic (user names, passwords, data) or even the type of data coming and going.

There are hundreds of VPN Internet Servers available. Most of them are free. I don't recommend using the free services for two reasons:

- You get what you pay for (typically here today, gone tomorrow, unstable, etc.)

## 8. Vulnerability: Internet Activity

- You don't know who is listening at the server side of things. Remember, your data is fully encrypted up to the server. But once the data exits the server on the way to the Internet, it is readable. There needs to be a high degree of trust for the administration of the VPN server. I see no reason to have such trust with free services.

### **VPNArea**

One of our favorite VPN providers is VPNArea.net. Although they do not offer a free or trial option, their yearly rate is a reasonable \$59. With this you get servers in almost every country you can name, use on 5 devices, unlimited bandwidth, humans on the other end of the tech support call, and highly responsive bandwidth.

The dominant feature of VPNArea is it is registered in Bulgaria, with servers located in Switzerland. Switzerland national data protection laws are among the strictest in terms of protecting private data, and permitting a VPN provider to not keep logs of client traffic. Other differentiating features include the option to use OpenVPN, L2TP, or PPTP (OpenVPN would be our only choice), 7-day money back guarantee, and their list of over 10,000 DNS servers that do not track or log your activities. This last option is important, as if you are using your ISP, Google, or other common DNS servers, your web travels are logged (called a *DNS Leak*). They also offer the upgrade to your own dedicated VPN server. This provides a significant speed boost as your server isn't timesharing with dozens or hundreds of other users.

### **Assignment: Purchase and Install VPNArea**

In this assignment we will create a paid account (with a 7-day cancellation policy) with *VPNArea.net*, and then install the VPNArea app.

- NOTE: VPNArea has been very gracious in extending a special discount to *Practical Paranoia* students and readers. To receive this discount upon checkout, enter *pparanoia* in the coupon field when registering.

## 8. Vulnerability: Internet Activity

1. From your Home Screen, select *Apps/Applications*.

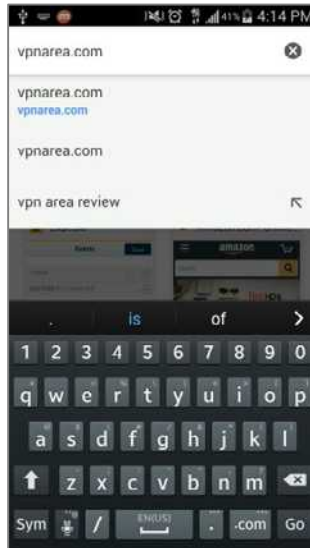


2. Select *Chrome*.



## 8. Vulnerability: Internet Activity

3. Enter *vpnarea.com* into the top address bar and select *Go*.



4. Select *Get Started – Prices*.



## 8. Vulnerability: Internet Activity

5. Scroll down and select *Buy now* under whichever subscription type you'd like.



6. Enter your name, email, username, and password. Enter the captcha, and then select *Buy Now*. Remember your username and password for later.

Sign up in seconds

Anthony

Galczak

Anthony@mintzit.com

United States

wgalczak

\*\*\*\*\*

\*\*\*\*\*

Referral

Select Membership Plan:

PayPal VISA MasterCard

Payza Bitcoin

VISA MasterCard

Coupon Code:

No promotions at the moment

Apply

iayiya

iayiya

Get a new code by clicking "Buy Now" you agree with terms and conditions

Buy Now

## 8. Vulnerability: Internet Activity

7. Select *Buy Now* one more time.



8. Select your payment method with PayPal. In this example, we will use *Pay with a Card*.



## 8. Vulnerability: Internet Activity

9. Enter your card information and select *Continue*.



The screenshot shows the PayPal mobile payment interface. At the top, the URL is <https://www.paypal.com/ct>. Below the URL bar, there is a notification for "OFFSHORE SECURITY" and a shopping cart icon with "My total: \$9.90 USD". The main heading is "Pay with a card" with a "Powered by PayPal" logo. The form includes a dropdown menu for "United States", a "Card number" input field, a "Have a prepaid gift card?" link, a "VISA" logo, an "Expiration:" field with "01" and "2015" dropdowns, a "Security code:" input field, a "Zip code" input field, and an "Email address" input field. A yellow "Continue" button is at the bottom, with a link "Have a PayPal account? Log in to PayPal" below it.

10. Enter your billing address and select *Pay Now*.



The screenshot shows the PayPal mobile payment interface for billing address entry. At the top, the URL is <https://www.paypal.com/ct>. Below the URL bar, there is a "Back" button, a notification for "OFFSHORE SECURITY", and a shopping cart icon with "My total: \$9.90 USD". The main heading is "Pay with a card" with a "Powered by PayPal" logo. The form includes "Billing info" with "First Name" and "Last Name" input fields, an "Address line 1" input field with a "+" button, a dropdown menu for "ALBUQUERQUE", a dropdown menu for "NM" and an input field for "87110". There is a "Ship to billing address" checkbox and a "Change >" button. A yellow "Pay Now" button is at the bottom, with a link "Signup for a PayPal account (recommended)" above it.



## 8. Vulnerability: Internet Activity

11. You will receive a receipt for your purchase. Jot down the receipt number for your records and then press the *Home* button.

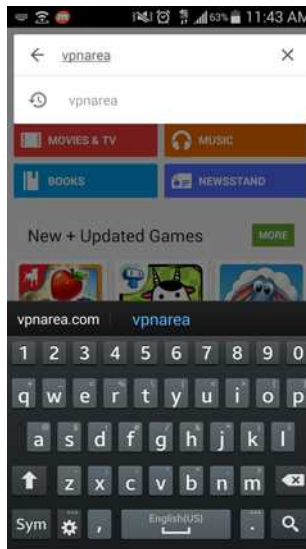


12. From your Home Screen, select *Play Store*.



## 8. Vulnerability: Internet Activity

13. Enter *vpnarea* into the top search bar and select the *Search* button.



14. Select *VPNArea*.

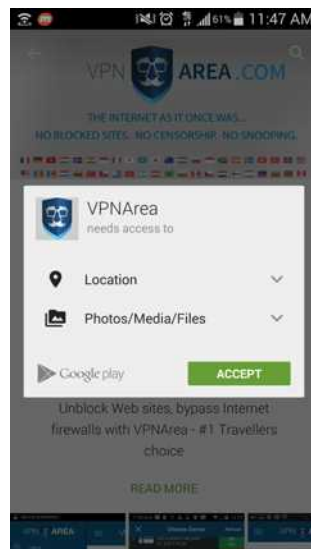


## 8. Vulnerability: Internet Activity

15. Select Install.



16. *Accept* the access requirements.



Congratulations! You have purchased and installed VPNArea.

## 8. Vulnerability: Internet Activity

### **Assignment: Configure VPNArea**

In this assignment we will configure and VPNArea for an active VPN connection on your device. You will need your VPNArea username and password for this activity.

1. From your Home Screen, select *VPNArea*.

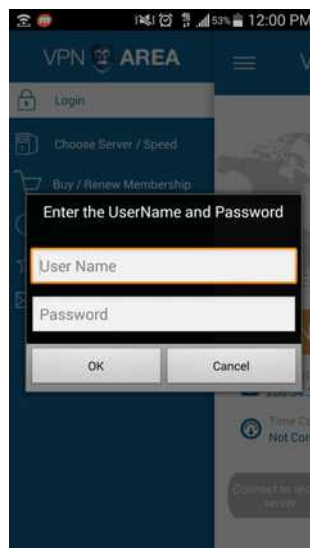


## 8. Vulnerability: Internet Activity

2. Select the *Menu* key in the upper left and then select *Login*.

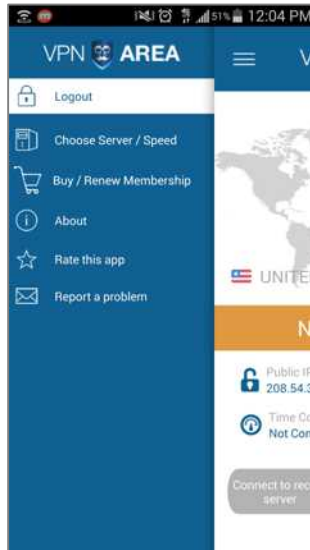


3. Enter your username and password and then select *OK*.

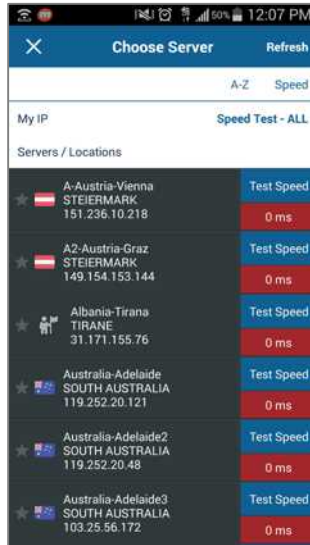


## 8. Vulnerability: Internet Activity

4. Notice that *Login* changed to *Logout*. Now select *Choose Server / Speed*.

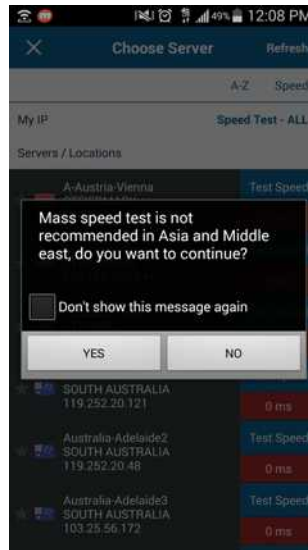


5. Select *Speed Test – ALL* in the upper right to find your best connection.

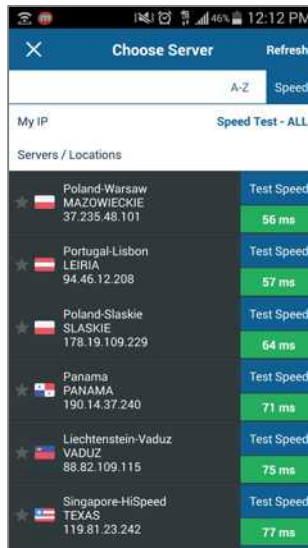


## 8. Vulnerability: Internet Activity

- Unless you are in Asia or the Middle East, check the box for *Don't show this message again* and then select *Yes*.

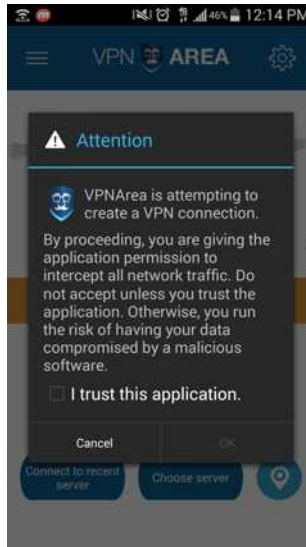


- Next, select a server. You can select your own or the fastest. For this example, select *Speed* and then select the fastest server.

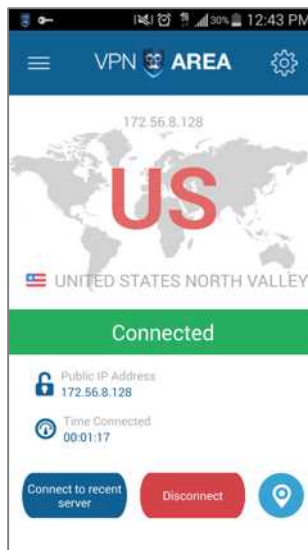


## 8. Vulnerability: Internet Activity

8. Check the box for *I trust this application.* and select *OK.*



9. When the connection is made, it will show *Connected.*





## 8. Vulnerability: Internet Activity

Congratulations! You have configured VPN so that any time you need complete privacy with your Internet communications, it is ready for you.



## 9. Vulnerability: Google Wallet and Credit Cards

*While money can't buy happiness, it certainly lets you choose your own form of misery.*

–Groucho Marx

## 9. Vulnerability: Google Wallet and Credit Cards

There were over 500 million credit card “thefts” in the United States in 2014. Possibly 110 million in the Target breach alone! This is a mind-boggling number. How is it that there can be as many as 2 credit cards breached per adult in a year?

The answer is that merchants *love* to keep your credit card information in their greedy little hands. By storing your card information, it makes it effortless for the merchant to close a sale. With the credit card on record, the buyer has neither the time nor the bother of having the search for the card to get in the way of the purchase.

This arrangement has the unintended consequence of making the merchant customer credit card database look like Fort Knox to a cyber thief. With enough resources and time, the thief can breach the database, harvest millions of personal identity and credit card records, and turn Target, Home Depot, or any other merchant into their money machine!

There are strategies available to help avoid such problems—primarily keeping various pieces of personal and card information on different servers. But even with such a strategy it is possible to breach all the data given adequate resources, and an insider.

According to cyber security experts, the real answer is in preventing the merchant from storing your data in a manner that is useable by anyone but the individual owner. Luckily, Google Wallet has acquired SoftCard and this has given Google Wallet <https://www.google.com/wallet/> the ability to be the ultimate Android application for Near Field Communications (NFC) [http://en.wikipedia.org/wiki/Near\\_field\\_communication](http://en.wikipedia.org/wiki/Near_field_communication) payments.

When using Google Wallet, the merchant never has access to your credit card number, expiration date, security code, or any other identifiable aspect of your card. All the merchant gets is a one-time-use code called a Google Wallet Virtual One Time Card that confirms that you do indeed have a valid credit/debit/gift card, and that you (with the confirmation of your Google Wallet PIN) are the rightful holder of said card. The merchant is authorized to charge to that card—but all the merchant has at the end of the transaction is data about the service/merchandise that was purchased, and a one-time-use code! There is nothing in the database worth stealing, and your card information remains hidden behind your locked Android device.

## 9. Vulnerability: Google Wallet and Credit Cards

Google Wallet is compatible with the majority of Android phones running Android 2.3+ and even iPhones running iOS6.0+ so it supports the vast majority of devices out on the market today.

A great feature of Google Wallet is it supports all the of “loyalty cards” that every store is offering you these days. Not only will you have fingertip access to all those loyalty cards with their rewards and points, it will also give you the ability to sign up for a new loyalty card if need be. Through this system you can also receive notifications for your rewards and points for all those cards that were otherwise filling your wallet or purse.

If you have one of the four major card providers, you have a Google Wallet-compatible credit card. Since Google Wallet has recently acquired SoftCard, the best place to find out where you can process NFC payments is <https://www.gosoftcard.com/where.html>. I’ve found the most common places to accept NFC payments are chain restaurants and chain grocery stores, however this is expanding by the day.

Now let’s set up your device to use it with Google Wallet.

### **Assignment: Install and Configure Google Wallet**

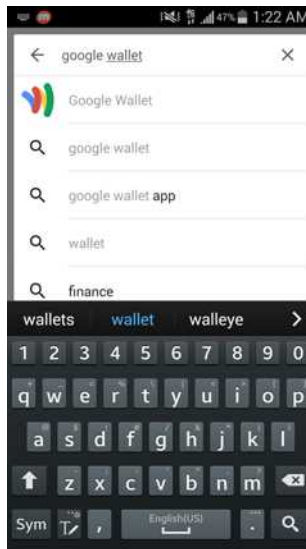
Most Android devices sold today come with Google Wallet pre-installed. If your device does not have it, we will now install it.

## 9. Vulnerability: Google Wallet and Credit Cards

1. From your Home Screen, select *Play Store*.



2. Enter *Google Wallet* into the search bar at the top and select *Google Wallet*.

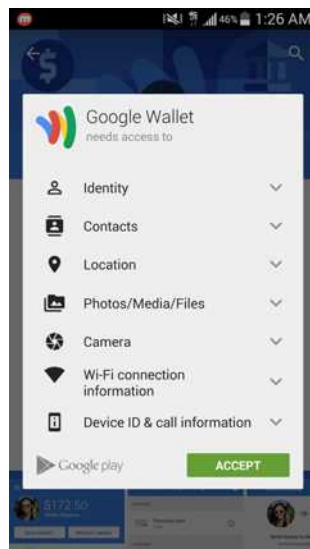


## 9. Vulnerability: Google Wallet and Credit Cards

3. Select *Install*.

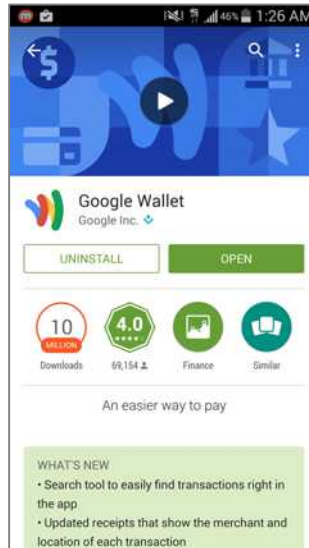


4. *Accept* the access requirements.

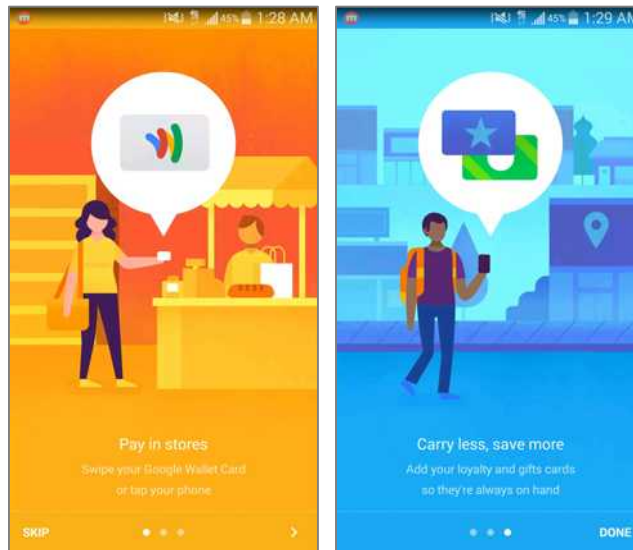


## 9. Vulnerability: Google Wallet and Credit Cards

5. Select *Open* to open Google Wallet.



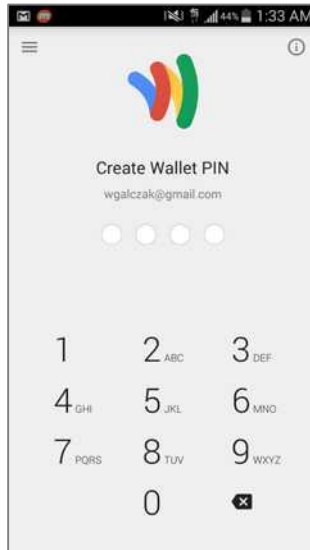
6. Google Wallet will tell you the payment methods it supports. Read these, press the *right arrow* button in the bottom right twice, and then finally *Done* to continue. When this completes, Google will send you a tutorial email.





## 9. Vulnerability: Google Wallet and Credit Cards

7. Enter and confirm a secure PIN to use with Google Wallet.



Congratulations, you have setup Google Wallet. You can request money or send money to others via email. In order to use Google Wallet for NFC payments you will need to follow the next assignment to set up a bank account or credit card.

### **Assignment: Add a Credit Card or Bank Account with Google Wallet**

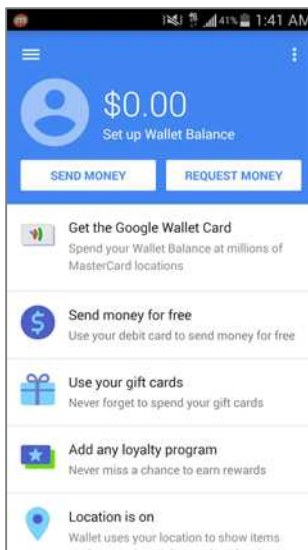
In order to use the NFC capability of Google Wallet we will need to add a credit card or bank account as a payment method. Remember that your information will not be given to the merchant, it will only be saved with your Google credentials and locked with your Google Wallet PIN.

## 9. Vulnerability: Google Wallet and Credit Cards

1. From your Home Screen, select *Wallet*.

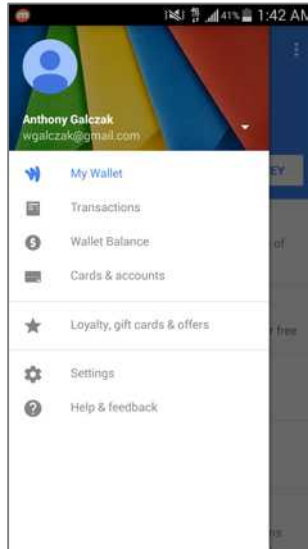


2. Select the *Menu* (3 dots) key in the upper left.

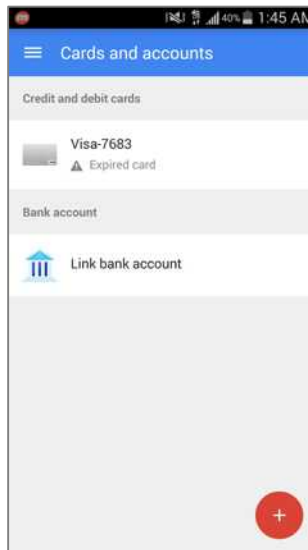


## 9. Vulnerability: Google Wallet and Credit Cards

### 3. Select Cards & accounts.

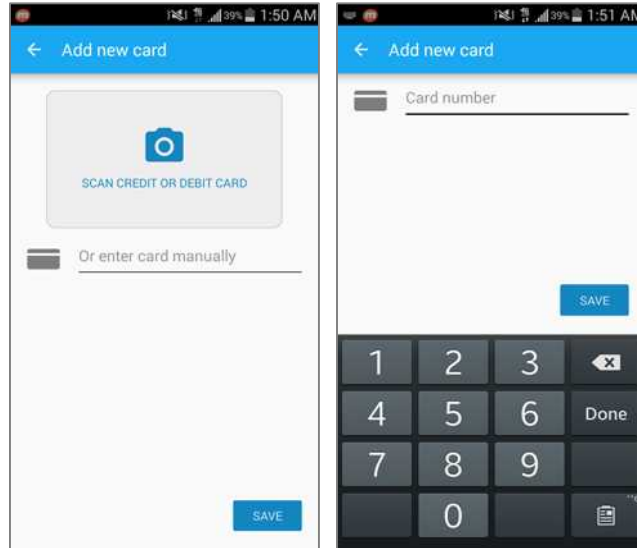


4. Any cards that have added in the past using *Google Wallet* or *Google Checkout* will be here. In order to add a new card, select the red *plus sign* in the bottom right. If you would like to link your bank account instead, skip to step 6 in this activity.

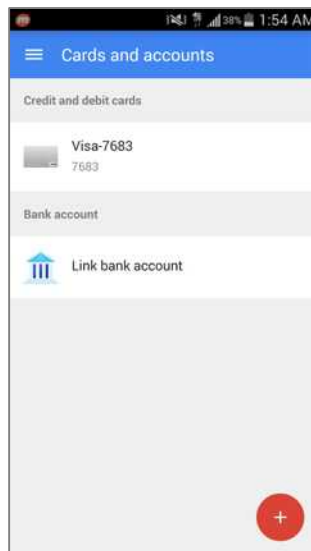


## 9. Vulnerability: Google Wallet and Credit Cards

- At the *Add new card* screen you can either take a picture of your card or enter the information manually. Select the empty field (*Or enter card manually*), enter your information, and then select *Save* to continue.



- After you enter your card information, it will appear under *credit and debit cards*, if you'd like to instead use a bank account, select *Link bank account*.



## 9. Vulnerability: Google Wallet and Credit Cards

7. Enter your financial institution's information, and then select *Next* in the upper right to continue.

Link bank account NEXT

ROUTING # ACCOUNT #

Enter account details

Checking account

Routing # (9 digits)

Account # (3-17 digits)

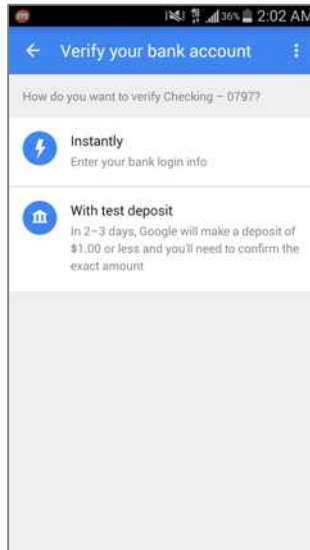
Retype account # (3-17 digits)

Name on account

By clicking Next above, you authorize Google (and its affiliate)

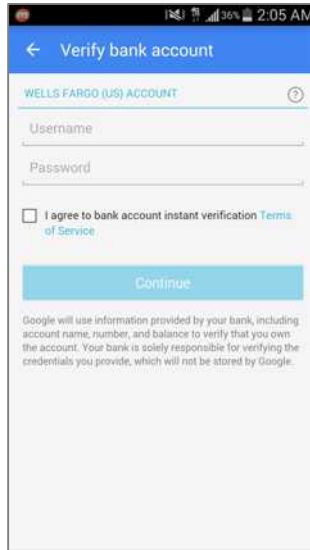
## 9. Vulnerability: Google Wallet and Credit Cards

8. You will need to verify your bank's info. If you use online banking just select *Instantly*, and then enter your bank username and password. Otherwise you can select *With test deposit* and have Google put a small verification deposit in your account.



## 9. Vulnerability: Google Wallet and Credit Cards

9. Enter your login info, check the box to accept the Terms of Service, and then press *Continue*.



Congratulations! You have setup a payment method with your Google Wallet account and can now use this service to conveniently process payments at merchants using NFC. Let's go shopping!

### **Assignment: Add a Loyalty Card to Google Wallet**

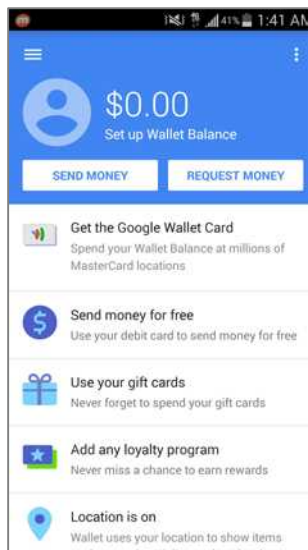
This is one of my favorite features of the Google Wallet application. If you've ever signed up for a reward card to get 10% off a purchase at a store you know how quickly you can fill your wallet with these incessant cards. No longer! You can now add all those loyalty cards into your Google Wallet and leave them at home.

## 9. Vulnerability: Google Wallet and Credit Cards

1. From your Home Screen, select *Wallet*.



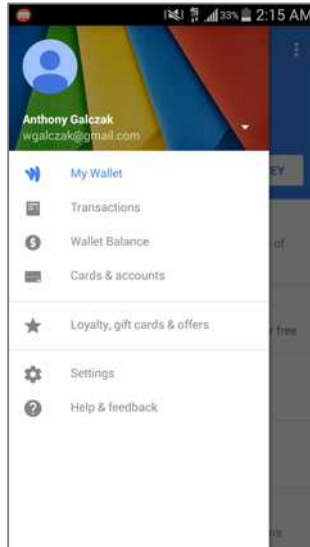
2. Select the *Menu* (3 dots) key in the upper left.



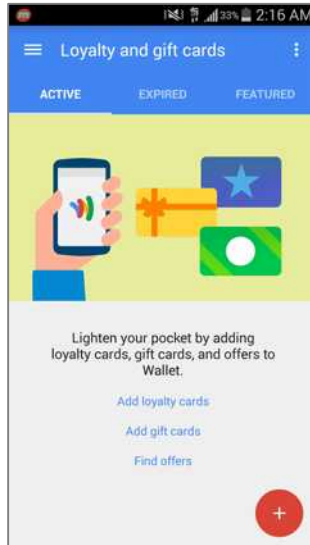


## 9. Vulnerability: Google Wallet and Credit Cards

### 3. Select *Loyalty, gift cards & offers*

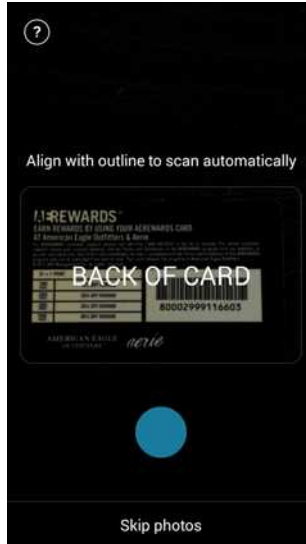


### 4. Select *Add loyalty cards*.

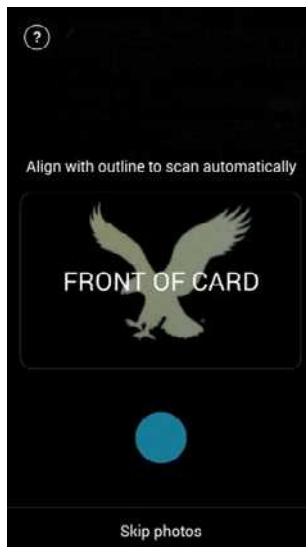


## 9. Vulnerability: Google Wallet and Credit Cards

5. Pull your loyalty card out and hold your phone over the back of the card. Select the *blue circle* to take a picture of the card. If you'd instead like to enter the information manually, select *Skip photos* and skip to step 8.



6. Now take a picture of the front of the card by flipping the card over and selecting the *blue circle* again.

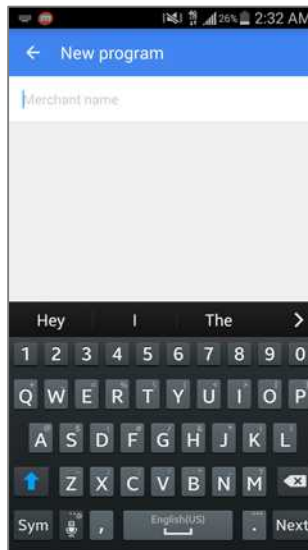


## 9. Vulnerability: Google Wallet and Credit Cards

7. It will now want you to confirm your photography is up to par. If everything looks readable, select *Next*.

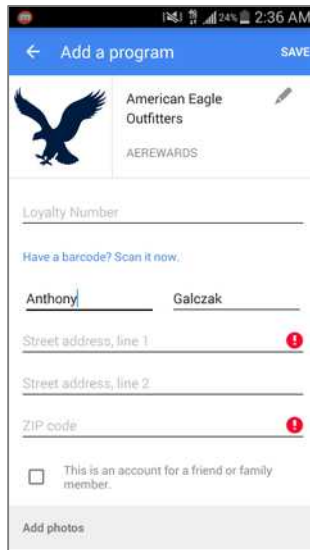


8. If you would like to skip photos or have already taken them, enter your merchant on the *New program* screen.





## 9. Vulnerability: Google Wallet and Credit Cards

9. When it recognizes your merchant it will ask for your loyalty card number and information. It will also display your photos here. Enter your info and select *Save*.



2:36 AM

← Add a program SAVE

 American Eagle Outfitters   
AEREWARDS

Loyalty Number \_\_\_\_\_

Have a barcode? Scan it now.

Anthony Galczak

Street address, line 1 \_\_\_\_\_ !

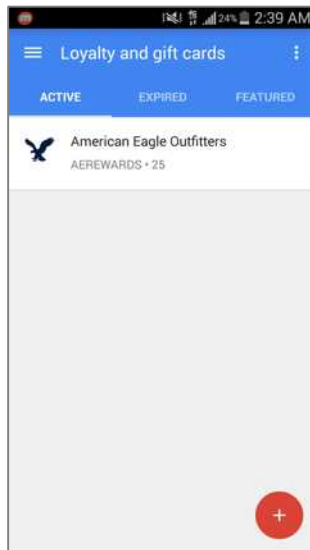
Street address, line 2 \_\_\_\_\_

ZIP code \_\_\_\_\_ !

This is an account for a friend or family member.

Add photos

10. After your card has been successfully entered, it will show up on your *Loyalty and gift cards* screen.



## 9. Vulnerability: Google Wallet and Credit Cards

### **Assignment: Enable Tap and Pay and NFC**

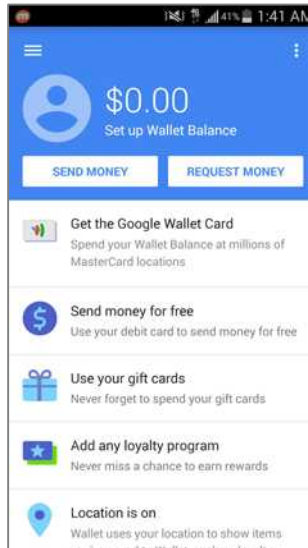
In order to do your first in-store purchase using Google Wallet you will need to enable Tap and Pay in Google Wallet and also enable NFC functionality on your device.

1. First we will enable *Tap and Pay*. From your Home Screen, select *Wallet*.

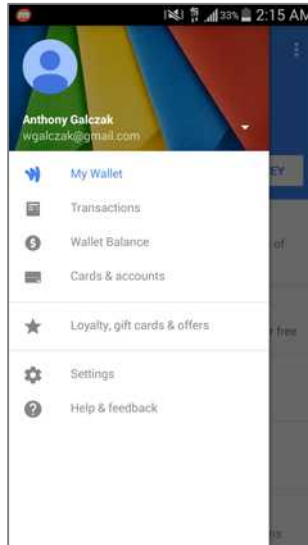


## 9. Vulnerability: Google Wallet and Credit Cards

2. Select the *Menu* (3 dots) key in the upper left.

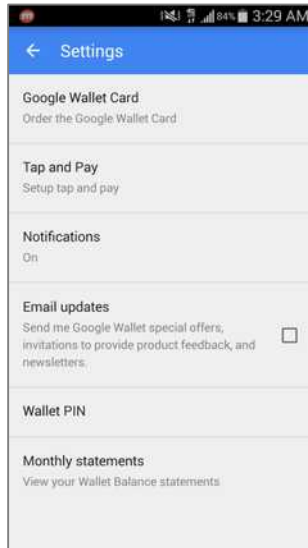


3. Select *Settings*.

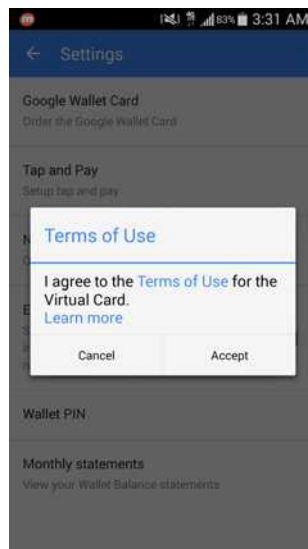


## 9. Vulnerability: Google Wallet and Credit Cards

4. Select *Tap and pay*.

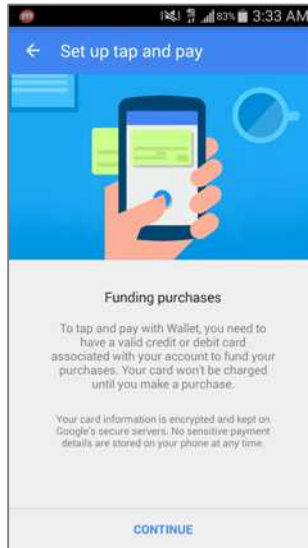


5. Read the *Terms of Use*, and then select *Accept* to continue.

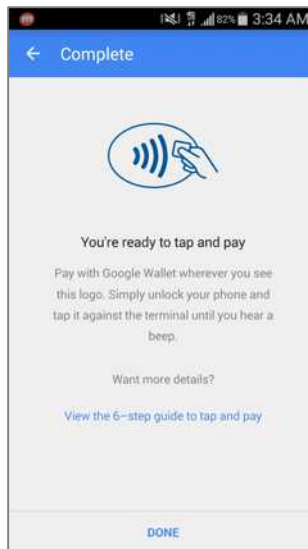


## 9. Vulnerability: Google Wallet and Credit Cards

6. Google Wallet will explain how to fund purchases for tap and pay. Press *Continue*.



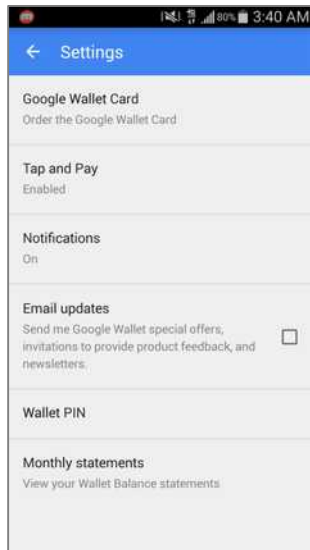
7. Google Wallet will now display a helpful guide on how to use tap and pay. Read this, and then select *Done*.





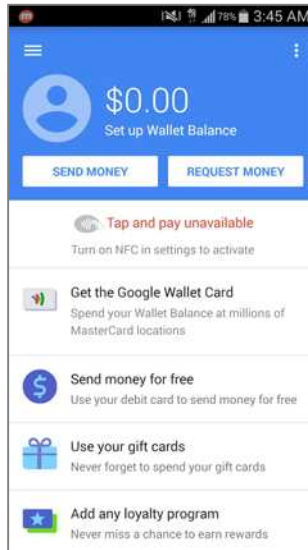
## 9. Vulnerability: Google Wallet and Credit Cards

8. On the *Settings* screen, under *Tap and Pay*, it says *Enabled*. Press the *Back* button to go back to the main screen of Google Wallet.

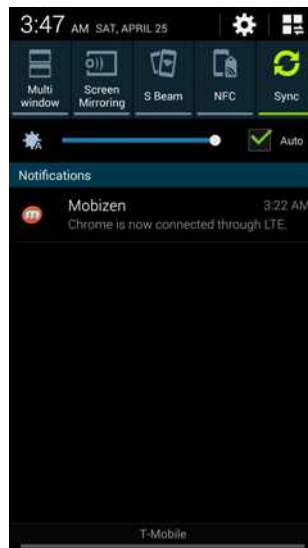


## 9. Vulnerability: Google Wallet and Credit Cards

9. Notice that it displays *Tap and pay unavailable*. This is where we turn on NFC (Near Field Communications). We can turn on NFC two different ways—in settings, or in the pull-down menu. I will show you the pull-down menu first. Pull-down the top menu.



10. If necessary, scroll over the notifications to the right if. Find and select *NFC*.



## 9. Vulnerability: Google Wallet and Credit Cards

11. If your device does not have the notification icon for NFC or if you'd prefer to do it in settings then press the *Home* button now. Select *Apps / Applications*.



12. Select *Settings*.



## 9. Vulnerability: Google Wallet and Credit Cards

13. Select *Connections* and toggle *NFC* to *On*.



Congratulations! You have enabled *Tap and Pay* and *NFC*. You are now ready to use Google Wallet to do NFC purchases in retail stores.

### **Assignment: Use Google Wallet in Stores**

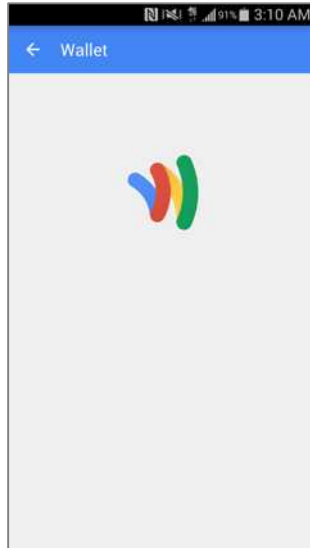
In this assignment we will make a purchase using Google Wallet. You will need *Tap and Pay* and *NFC* enabled for this assignment. Bulky device cases can sometimes block the NFC signal, if you run into problems remove the case from your device.

1. Go to a brick and mortar store that accepts Google Wallet. Close your eyes, take a few steps, you are bound to trip over one. Or if you want to play it safe, look for the NFC or Google Wallet logos.



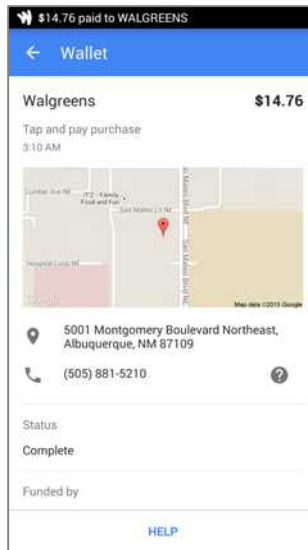
## 9. Vulnerability: Google Wallet and Credit Cards

2. When at the checkout register, hold your Android device within an inch of the contactless terminal. Google Wallet will automatically open and show a *W* loading screen.



## 9. Vulnerability: Google Wallet and Credit Cards

3. As soon as the storefront terminal recognizes your device (this should only take a few seconds), it will beep. In my example the terminal asked for my PIN, this is when you enter your Google Wallet PIN. Other terminals may have you enter your PIN on your device instead. After you enter your PIN and hit *Enter* on the terminal, you will get a confirmation of your purchase on your device.



Congratulations! You have made your first Google Wallet Tap and Pay payment. Notice at the top it displays details on your purchase. There are also details on the address and phone number to the merchant. Lastly, you will get an email detailing the entire purchase to your Gmail account.

*Ahhhh...* Didn't that feel wonderful? Retail therapy *and* no chance of identity or credit card theft.

*Let's do it again!*

## The Final Word

If you have followed each of the steps outlined in this book, your device now is secured to a level higher than even the NSA requires for its own staff. Although this won't prevent one of the bad guys from stealing your precious device, it will prevent them from accessing your data. And since you have at least one current backup at the home or office, and one on the Internet, you are still in possession of the items with *real* value—your data, and peace of mind.





# Index

- 802.1x ..... 115
- AES ..... 115
- Android Updates ..... 48
- anti-malware ..... 74
- Anti-Theft..... 97, 98, 99, 101, 103
- Antivirus ... 74, 75, 76, 80, 81, 83, 98
- Assignment.....26, 29, 35, 42, 48, 51, 62, 65, 68, 71, 75, 80, 83, 87, 91, 92, 97, 101, 105, 109, 117, 122, 127, 134, 143, 145, 147, 154, 157, 171, 176, 178, 180, 182, 185, 193, 194, 202, 208, 214, 219, 225, 227, 229, 235, 244, 260, 263, 267, 272, 276, 287, 297, 307, 316, 325, 329, 335, 341, 348
- Aung San Suu Kyi..... 169
- Authentication for App Purchases ..... 68
- backup ..... 29, 52, 53, 55, 56, 57, 60, 86, 87, 90, 91, 92, 95, 106, 192, 193, 351
- Backups ..... 86
- Benjamin Franklin..... 133
- Bitdefender .....74, 75, 76, 78, 79, 80, 83, 85, 97, 99, 100, 101, 103
- Blog ..... 21
- Browser Email ..... 176
- certificate..... 184, 185, 186, 187, 188, 189, 192, 193, 194, 195, 196, 197, 198, 199, 202, 203, 204, 205, 206, 207, 208, 213, 214, 216, 217, 221, 222, 225, 227, 228, 229, 230, 231, 269
- Certificate Authorities ..... 184
- CipherMail..... 208, 209, 211, 212, 214, 215, 219, 220, 224, 225, 226, 227, 229, 230
- Cisco ..... 26
- CISPA ..... 17
- Clear Browsing Data ..... 141, 142
- Comodo ..... 185, 189, 202, 206, 207, 222
- Cookies.....138, 139, 145
- credit card ..... 324, 350
- Crypt4All Lite.....260, 261, 263, 267, 268, 272
- Data Recovery ..... 92
- Device theft..... 86
- Document Security..... 260
- Douglas MacArthur ..... 113
- DuckDuckGo .....145, 146, 147, 148, 149, 151
- email ..... 17, 24, 26, 90, 114, 141, 169, 170, 171, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 189, 193, 194, 198, 199, 200, 201, 202, 205, 206, 207, 208, 211, 212, 219, 222, 223, 224, 225, 226, 227, 229, 230, 232, 234, 239, 240, 254, 328
- encrypted email..... 170, 184
- Encryption ..... 114, 133, 170, 175, 177, 232
- Entropy..... 86

## Index

- Ethernet..... 97
- Face Unlock..... 25
- Facebook..... 21, 25, 26
- Fire ..... 86
- Firefox ..... 154, 155, 163, 164, 168, 189, 190, 194, 195
- Firewall..... 116
- Flash..... 17
- Format SD card..... 111
- Formatting an SD Card..... 109
- GNU Privacy Guard..... 177
- Google Account . 233, 234, 235, 244
- Google Checkout ..... 331
- Google Chrome.. 134, 143, 144, 154
- Google Wallet.....323, 324, 325, 335, 348
- GPG ..... 184
- GPS ..... 100
- Groucho Marx..... 323
- Henry David Thoreau ..... 303
- HIPAA..... 178, 185, 272, 286
- HTTPS..... 133, 152, 153, 170, 171, 175, 176, 177, 178
- Hypertext Transport Layer Secure ..... 170
- Incognito Mode ..... 143, 144
- Java..... 17
- JavaScript ..... 140
- Jiddu Krishnamurti ..... 259
- John F. Kennedy ..... 285
- Joseph Heller ..... 13
- Kaspersky ..... 74
- Keychain ..... 207
- Kies ..... 52, 57, 58, 59, 61, 86
- L2TP ..... 307
- LastPass ..... 26, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47
- Loyalty Card ..... 335
- Malware.....74, 80, 81, 97
- Mintz’s extrapolation of Sturgeon’s Revelation..... 16
- National Security Agency ..... 24
- Near Field Communications... 324, 346
- Newsletter ..... 21
- NFC ..... 324, 325, 329, 335, 341, 346, 347, 348
- Noodle Koogole ..... 151
- NoRoot Firewall.....116, 117, 118, 120, 122, 127, 132
- NSA..... 15, 24, 154, 232, 351
- OpenVPN ..... 307
- Orbot ..... 154, 157, 158, 161, 162, 164, 167, 168
- passphrase..... 25
- Password ..... 25, 133, 170, 175, 177, 178, 234
- Pattern..... 25, 26, 28, 29, 33, 108
- Pattern lock.....25, 26, 29, 33
- phishing..... 17, 74
- PIN.....25, 29, 31, 84, 85, 108, 199, 324, 329, 350
- Play Store ..... 36, 37, 62, 64, 68, 71, 74, 75, 87, 117, 145, 155, 157, 208, 234, 243, 260, 287, 313, 326
- PPTP..... 307
- PRISM ..... 17, 169
- Private Key..... 184, 214
- Proxy..... 154, 158, 164, 166
- Public Key ..... 184
- rooted ..... 74

## Index

- S/MIME..... 177, 184, 185, 193, 195, 196, 201, 202, 208, 211, 213, 214, 219, 225, 227, 228, 229, 232, 269, 273
- Screen Lock..... 26, 27, 29, 31, 199
- Screen Timeout ..... 65, 67
- SD card... 82, 87, 105, 109, 111, 263, 264, 276, 278, 280, 281, 283
- Secure Erase..... 272
- Secure Socket Layer ..... 133, 170
- Secure Web Page..... 152
- Securely Erase..... 105
- SendInc..... 177, 178, 180, 182
- SoftCard ..... 324, 325
- software..... 74, 178
- SSL ..... 133, 170, 171, 177
- Static electricity ..... 86
- Symantec..... 17
- System Software ..... 51
- System Updates..... 48
- Tap and Pay..... 341, 345, 348, 350
- Text Messaging ..... 285, 286
- The Guardian ..... 24
- theft..... 17
- Theodore Sturgeon..... 16
- TKIP ..... 115
- TLS..... 170, 171, 175, 177
- TOR ..... 154, 158, 162, 164, 167, 168
- trojan horses..... 17, 74
- two-step authentication ..... 244
- Two-Step Verification..... 234, 244, 249, 251, 252, 255
- Unauthorized Apps ..... 71
- US-CERT ..... 48, 64
- Virtual Private Network ... 114, 304
- viruses..... 17
- VPN ... 114, 116, 120, 132, 303, 304, 305, 306, 307, 316, 321
- VPNArea..... 307, 314, 315, 316
- Water damage ..... 86
- WEP ..... 114
- Wickr..... 286, 287, 297
- Wi-Fi ..... 97, 114
- William Hazlitt ..... 233
- worms..... 17, 74
- WPA ..... 114
- WPA2 ..... 114
- zero-day exploits..... 18

## Index

# ***Your Virtual CIO & IT Department***

## **Mintz InfoTech, Inc.** **when, where, and how you want IT**

Technician fixes problems.  
**Consultant delivers solutions.**

Technician answers questions.  
**Consultant asks questions, revealing core issues.**

Technician understands your equipment.  
**Consultant understands your business.**

Technician costs you money.  
**Consultant contributes to your success.**

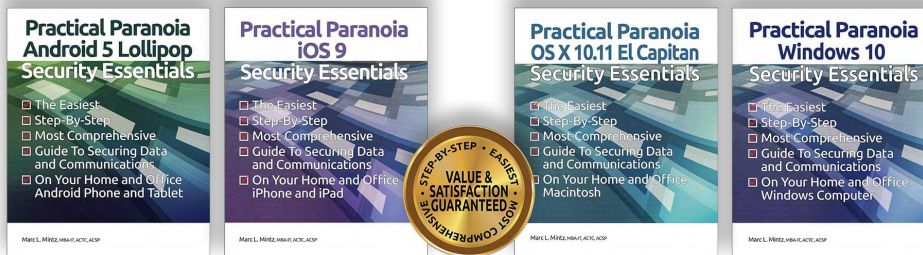
**Let us contribute to your success.**

Mintz InfoTech is uniquely positioned to be your Virtual CIO and provide comprehensive technology support. With the only MBA-IT consultant in New Mexico heading our organization, our mission is to provide small and medium businesses with the same Chief Information and Technology Officer resources otherwise only available to large businesses.

Mintz InfoTech, Inc.  
Toll-free: +1 888.469.0690 • Local: +1 505.814.1413  
Email: [info@mintzIT.com](mailto:info@mintzIT.com) • <https://mintzIT.com>



# Practical Paranoia Security Essentials Workshops & Books Android, iOS, OS X, Windows



This is an age of government intrusion into every aspect of our digital lives, criminals using your own data against you, and teenagers competing to see who can crack your password the fastest. Every organization, every computer user, every one should be taking steps to protect and secure their digital lives.

The *Practical Paranoia: Security Essentials Workshop* is the perfect environment in which to learn not only *how*, but to actually *do* the work to harden the security of your OS X and Windows computers, and iPhone, iPad, and Android devices.

Workshops are available online and instructor-led at your venue, as well as tailored for on-site company events.

Each Book is designed for both classroom, workshop, and self-study. Includes all instructor presentations, hands-on assignments, software links, security checklist, and review questions and answers. Available from Amazon (both print and Kindle format), and all fine booksellers, with inscribed copies available from the author.

Call for more information, to schedule your workshop, or order your books!

Mintz InfoTech, Inc.

Toll-free: +1 888.479.0690 • Local: +1 505.814.1413  
info@mintzIT.com • <http://thepracticalparanoid.com>