Practical Paranoia™ macOS 10.13

Security Essentials

- ☑ The Easiest
- ☑ Step-By-Step
- ☑ Most Comprehensive
- ☑ Guide To Securing Data and Communications
- ☑ On Your Home and Office macOS Computer

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

TPP
The Practical Paranoid

Practical Paranoia: macOS 10.13 Security Essentials

Author: Marc Mintz

Editions: v1.0 20170918 • v1.01 20170923 • v1.1 20171001 • v1.2 20171022 • v1.3 20180325 • v2 20180420

Cover design by Ed Brandt

ISBN-10: 1976513650
ISBN-13: 978-1976513657

Dedication

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

Contents At A Glance

Contents In Detail

15 Email

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

–Aung San Suu Kyi[1], Burmese opposition leader and chairperson of the National League for Democracy in Burma

What You Will Learn In This Chapter

- Prevent phishing
- Email encryption protocols
- Configure Mail to use TLS and SSL
- Configure web mail to use HTTPS
- Use Proton Mail
- Use GNU Privacy Guard
- Use S/MIME
- Use Virtru

[1] *https://en.wikipedia.org/wiki/Aung_San_Suu_Kyi*

15.1 The Killer App

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 all are very likely to turn over all records of your email whenever a government agency asks for that data. In most cases, your email is sent and received in clear text so that anyone along the dozens of routers and servers between you and the other person can clearly read your messages. Add to this knowledge the recent revelations about PRISM[2], where the government doesn't have to ask your 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!

[2] *https://en.wikipedia.org/wiki/PRISM_(surveillance_program)*

15.2 Phishing

The act of phishing is epidemic on the Internet. Phishing[3] is the attempt to acquire your sensitive information by appearing as a trustworthy source. This is most often attempted via email.

The way the process often works is that you receive an email from what appears to be a trustworthy source, such as your bank. The email provides some motivator to contact the source, along with what appears to be a legitimate link to the source website.

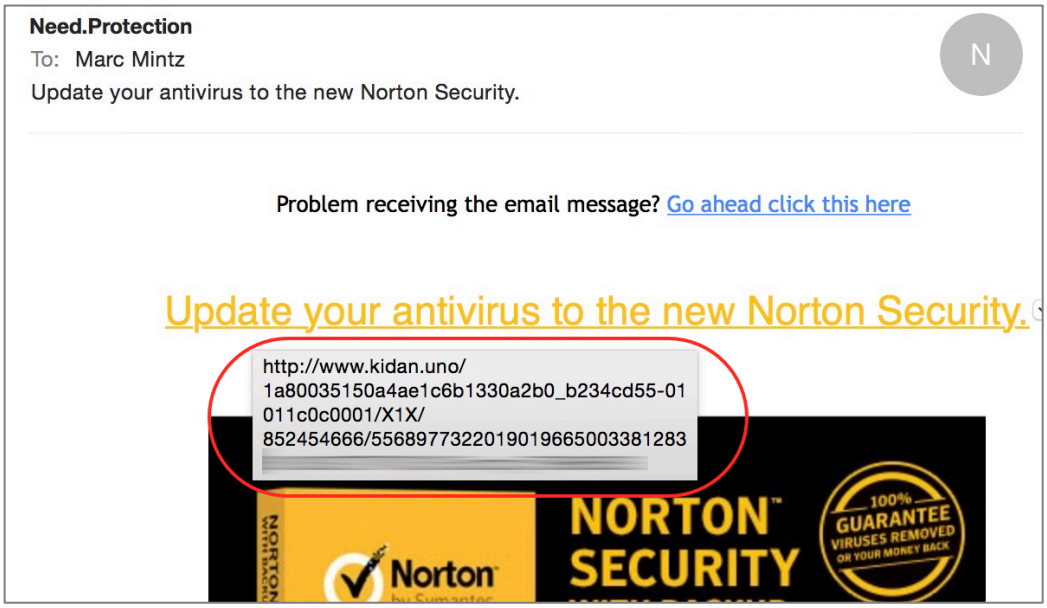
When you click the link, you are taken to what appears to be the trustworthy source (perhaps the website of your bank), where you are prompted to enter your username and password.

At that point, they have you. The site is a fraud, and you have just given the criminals your credentials to access your bank account. In a few moments, your account may be emptied.

The key to preventing a successful phishing attack is to be aware of the *real* URL behind the link provided in the email.

[3] *https://en.wikipedia.org/wiki/Phishing*

The link that appears in an email may have nothing at all to do with where the link takes you. To see the *real* link, hover (don't click) your cursor over the link. After 3 seconds, the *real* link will pop-up.



Some of these scams are getting a bit more sophisticated in their choice of URL links, and attempt to make them appear more legitimate. For example, the email may say it is from *Bank of America*, and the link say *bankofamerica.com*, but the actual URL will be *bankofamerica.tv*, or *bankofamerica.xyz.com*.

If you have any doubts at all, it is best to contact your bank, stock broker, insurance agent, etc. directly by their known email or phone number.

15.3 Email Encryption Protocols

There are three common protocols that provide encryption of email between the sending or receiving computer and the SMTP (outgoing), IMAP (incoming), and POP (incoming) servers:

- **TLS**[4] (Transport Layer Security)
- **SSL**[5] (Secure Socket Layer)**,** the TLS predecessor
- **HTTPS**[6] (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 programmers are prone), this does little good unless you know that the other end of the communication also is using encrypted email. If they aren't, then once your encrypted mail passes from your computer to your email server, it demotes to either the less secure SSL, or if the other end of the communications doesn't support that, demotes to clear text from your email server, through dozens of Internet routers, to the recipient email server, and finally onto the recipient's computer.

---

[4] *http://en.wikipedia.org/wiki/Secure_Sockets_Layer*

[5] *http://en.wikipedia.org/wiki/Secure_Sockets_Layer*

[6] *http://en.wikipedia.org/wiki/Https*

15.4 TLS and SSL With Mail App

Although SSL was originally considered highly secure, it has been broken and should no longer be used for email that is sensitive, secure, or related to the healthcare, legal, government, or military. To use TLS , the following criteria must be met:

- Your email provider offers a TLS. 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.
- Your email provider has enabled and configured your email service to use TLS (they may *offer* TLS, but it may not be *enabled* by default).
- You have configured your email application to use TLS (most email applications now do this automatically. Apple Mail.app has gone to the point they have removed the preference setting for both SSL and TLS).
- Lastly, although not a requirement for TLS, 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.)

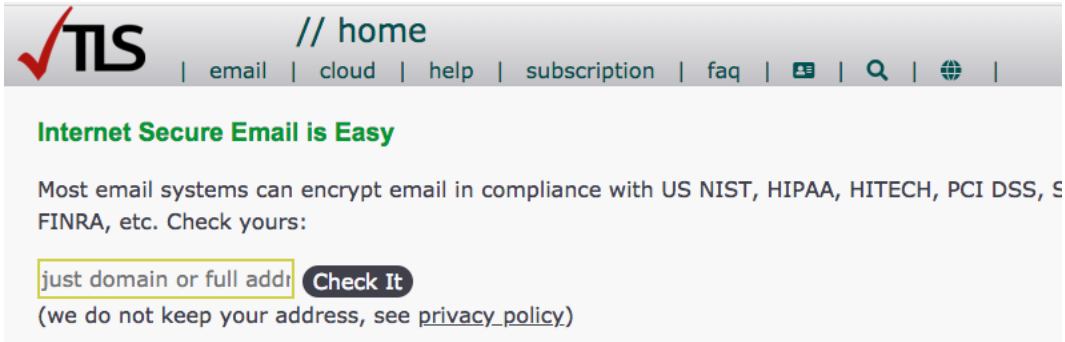
15.4.1 Assignment: Determine if Sender and Recipient Use TLS

In this assignment, you discover if both your own email and that of a recipient use TLS email encryption.

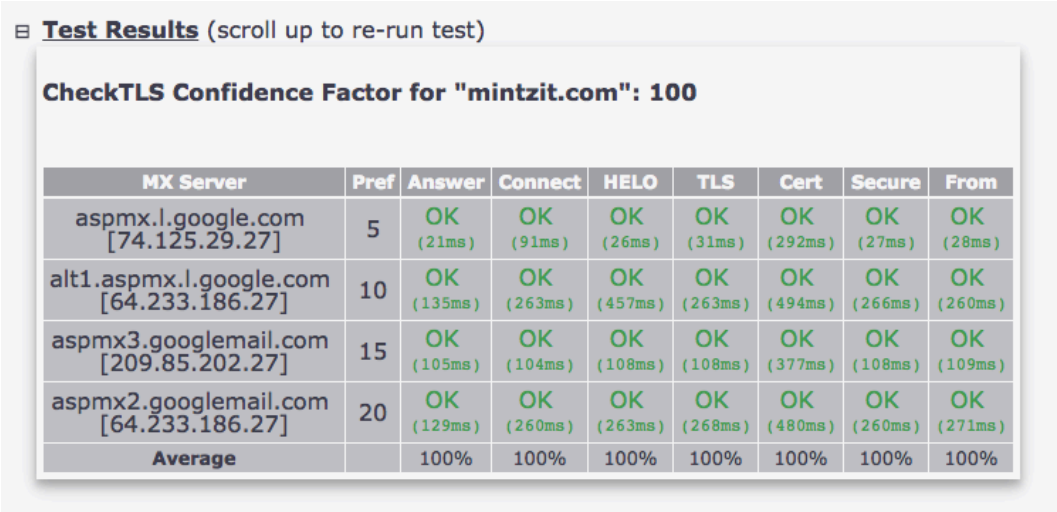
- Note: If you use a web browser for email, you may skip this assignment and move on to the next where we configure your browser-based email to use https.

1. Open a web browser, and then go to *CheckTLS.com.*

2. Scroll halfway down the home page to the *Internet Secure Email is Easy* section.
3. In the *Just domain or full address* field, enter the domain name of your email address. For example, my email address is *marc@mintzit.com,* so my domain is *mintzit.com.* Then select the *Check It* button.



4. The website will run tests against the domain's mail servers (MX servers), and then report on their level of security.



Test Results (scroll up to re-run test)

CheckTLS Confidence Factor for "mintzit.com": 100

MX Server	Pref	Answer	Connect	HELO	TLS	Cert	Secure	From
aspmx.l.google.com [74.125.29.27]	5	OK (21ms)	OK (91ms)	OK (26ms)	OK (31ms)	OK (292ms)	OK (27ms)	OK (28ms)
alt1.aspmx.l.google.com [64.233.186.27]	10	OK (135ms)	OK (263ms)	OK (457ms)	OK (263ms)	OK (494ms)	OK (266ms)	OK (260ms)
aspmx3.googlemail.com [209.85.202.27]	15	OK (105ms)	OK (104ms)	OK (108ms)	OK (108ms)	OK (377ms)	OK (108ms)	OK (109ms)
aspmx2.googlemail.com [64.233.186.27]	20	OK (129ms)	OK (260ms)	OK (263ms)	OK (268ms)	OK (480ms)	OK (260ms)	OK (271ms)
Average		100%	100%	100%	100%	100%	100%	100%

5. If your *Test Results* are not 100% secure, either discuss this with your email provider for a resolution, or change providers.
6. Repeat steps 1-4 using the domain of your recipient email address.

7. If their *Test Results* are not 100% secure, advise them to discuss this with their email provider, or change providers.
    - Remember: Email will typically downgrade to lowest common security protocol.

15.5 Require Google Mail to be TLS Secured

Google mail (Gmail, G-Suite email) uses TLS by default. However, if both the sender and recipient don't support TLS, Google will deliver messages over a non-secure connection. And neither sender nor recipient will know.

However, your Google G-Suite (not Gmail) account can be configured to *only* use TLS. When so configured:

- Your outgoing Google mail (to a non-TLS account) will not be delivered, will bounce back to you, you will received a non-delivery report (NDR). No additional delivery attempts will be made.
- Your incoming Google mail (from a non-TLS account) will be rejected at entry to Google servers. You will not receive any notification. The sender will receive an NDR.

15.5.1 Assignment: Configure Google G-Suite Mail for Only TLS

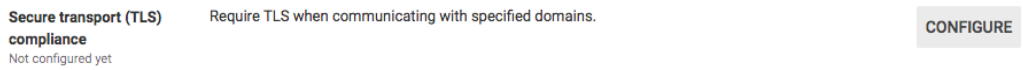
In this assignment, you configure your Google mail account to only allow use of TLS security. This feature is available only with paid G-Suite accounts, not with the free Gmail accounts.

Full details for this operation may be found on the Google *Require mail to be transmitted via a secure (TLS) connection* help page[7]

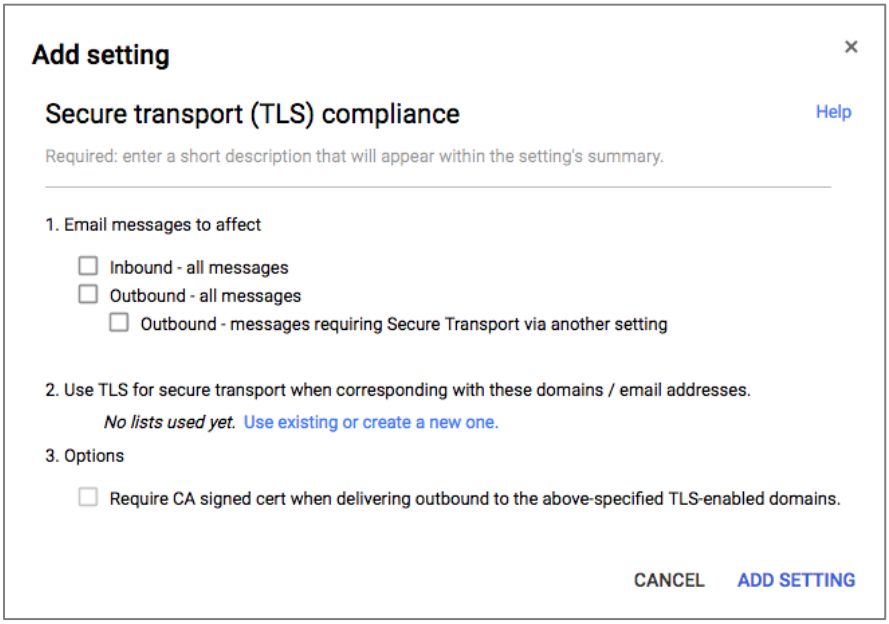
1. Open a web browser, visit and log in to the Google Admin Console at *https://admin.google.com*.
2. Go to *Apps* > *G Suite* > *Gmail* > *Advanced settings.*
3. If the G-Suite account includes more than one *Organization,* select the desired Organization from the left sidebar.

[7] *https://support.google.com/a/answer/2520500?hl=en*

4. Scroll down to the *Compliance* section, hover over *secure transport (TLS) compliance,* and then select the *Configure* button.



5. In the *Add setting* page, select *ADD SETTING.*



6. In the *Secure transport (TLS) compliance* field, enter a description of this setting. For example: *Force TLS with contractors.*
7. In *1. Email messages to effect,* enable both *Inbound* and *Outbound.*
8. In *2. Use TLS for secure transport when corresponding with these domains / email addresses,* add the domain names to be included in forced TLS.
9. In *3. Options,* enable *Require CA signed cert when delivering outbound to the above-specified TLS-enabled domains.* This will prevent man-in-the-middle attacks.
10. Select *Save.*

15.6 HTTPS with Web Mail

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 your user name and password are fully encrypted, as are the contents of all email that you create or open.

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

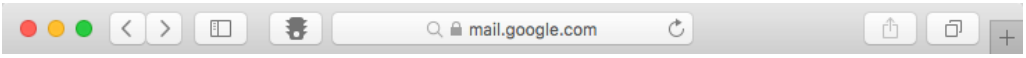
15.6.1 Assignment: Configure Web Mail to Use HTTPS

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

In this assignment, you verify your browser-based email uses HTTPS.

- Note: If you do not use browser-based email, you may skip this assignment, and perform the previous assignment.

1. Launch your web browser.
2. Go to your log in page for your email. In this example, we will be using Google Mail (Gmail).
3. 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.



4. If instead your browser shows the URL to be http://, try revisiting your email log in page, but this time manually enter https://.
5. If you get to the log in page, all is good. Just bookmark the https:// URL and use it instead of the previous non-secure URL.
6. If you cannot get to your log in page, change your email provider NOW!

15.7 End-To-End Secure Email With ProtonMail

If you are serious about email security, then you need to use an end-to-end secure email solution. Forcing TLS for incoming and outgoing email is one option (see previous section 15.5). However, it is likely either sender or recipient use email hosts that don't allow forcing TLS.

There are two other options for point-to-point email encryption:

- Use an email encryption utility. This works well if the other end of the communication also is using the same encryption utility. Our next section 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. An example of this is *Sendinc.com*[8].

An interesting hybrid option is found in *ProtonMail*[9]. ProtonMail includes PGP public key/private key encryption, so that neither you nor the other party need deal with the potential headaches of installing and configuring PGP encryption.

ProtonMail has several advantages for the typical user, including:

- Free with optional monthly/yearly plans.
- Based in Switzerland so all user data is protected by Swiss privacy laws.
- Allows the user to determine the destruction date and includes unlimited retention.
- Allows for encrypted and password protected emailing to non-ProtonMail users.
- Allows for rich text email.

When sending from ProtonMail to a non-ProtonMail user, your recipient receives an email stating that a secure message is waiting. The recipient clicks the link,

---

[8] *https://sendinc.com/*
[9] *https://protonmail.com*

taking the recipient to an authentication page. Upon entering the password the recipient then sees the message. The recipient can directly and securely reply to the message, then you receive their reply in your inbox.

When sending from ProtonMail to ProtonMail, the interface is like other email providers.

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

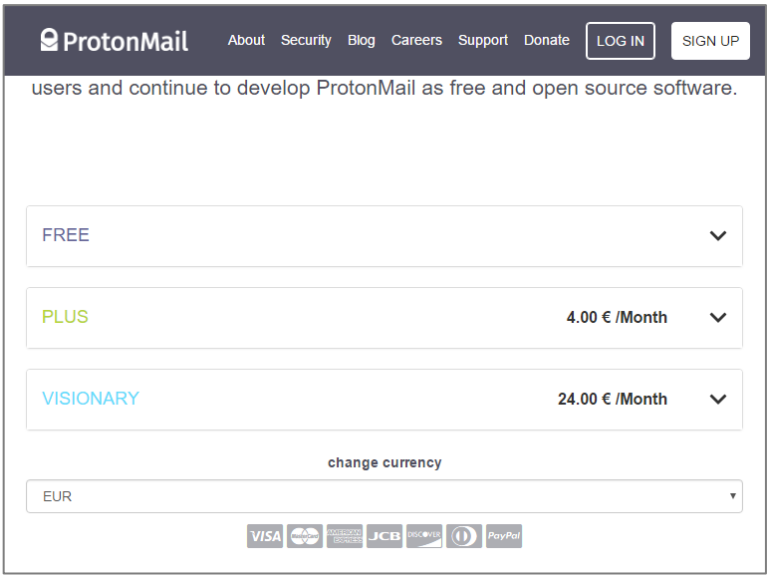
15.7.1 Assignment: Create a ProtonMail Account

In this assignment, you create a ProtonMail account.

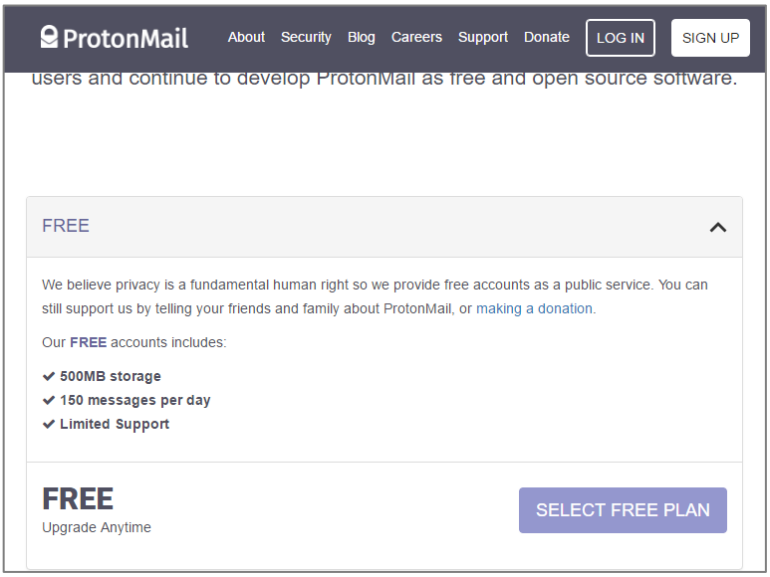
1. Using your web browser, visit *https://protonmail.com*. Select either the *Sign Up* or *Get Your Encrypted Email Account* button.

2. Scroll down to click the drop-down arrow next to the plan you wish to use (PLUS is selected by default). In this tutorial, we will be making a free account.

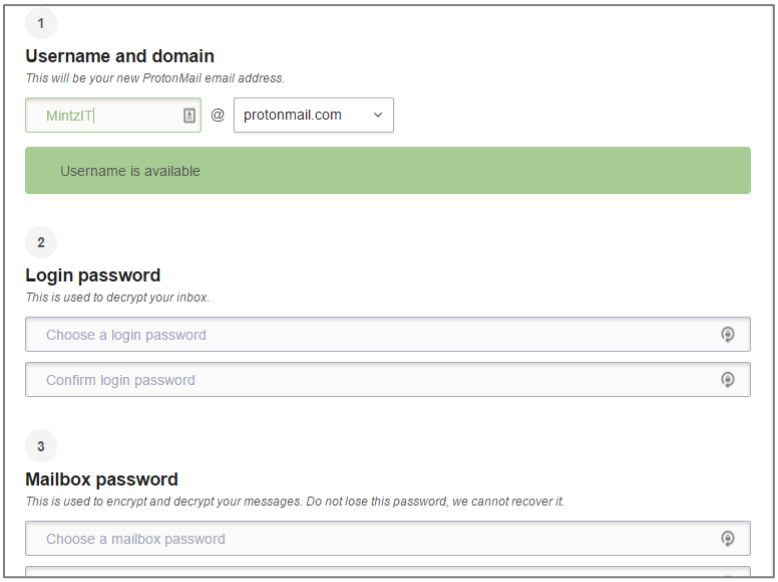
If you wish to use a monthly plan, make sure to double check the currency used on the bottom of the page.



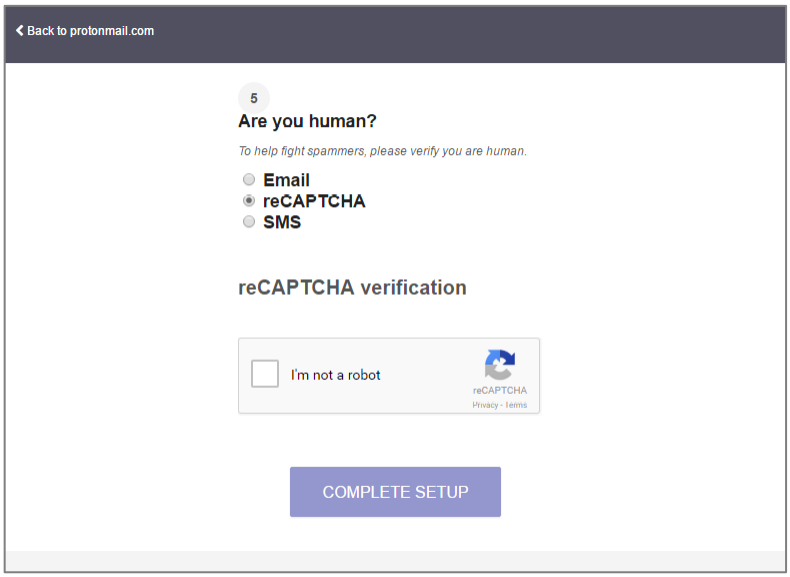
3. Click the *Select Free Plan* button.



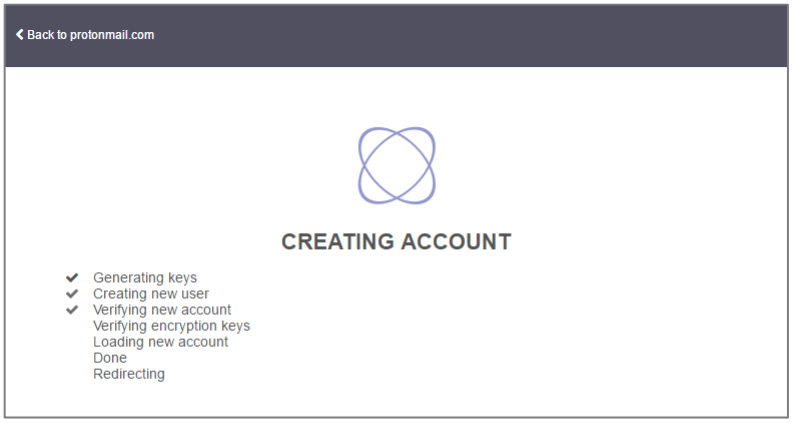
4. Enter the *Username* and *Password* you wish to use. We recommend using easy to remember 15 character passphrases.



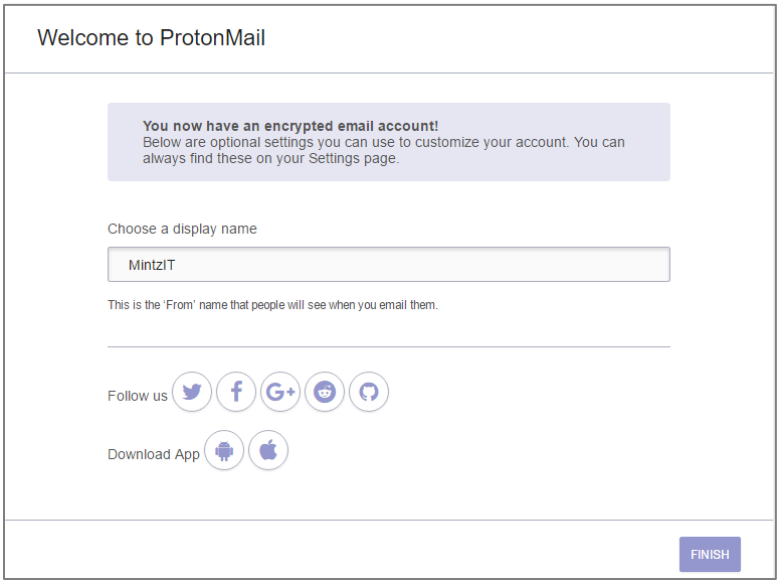
5. Provide a method of verification.



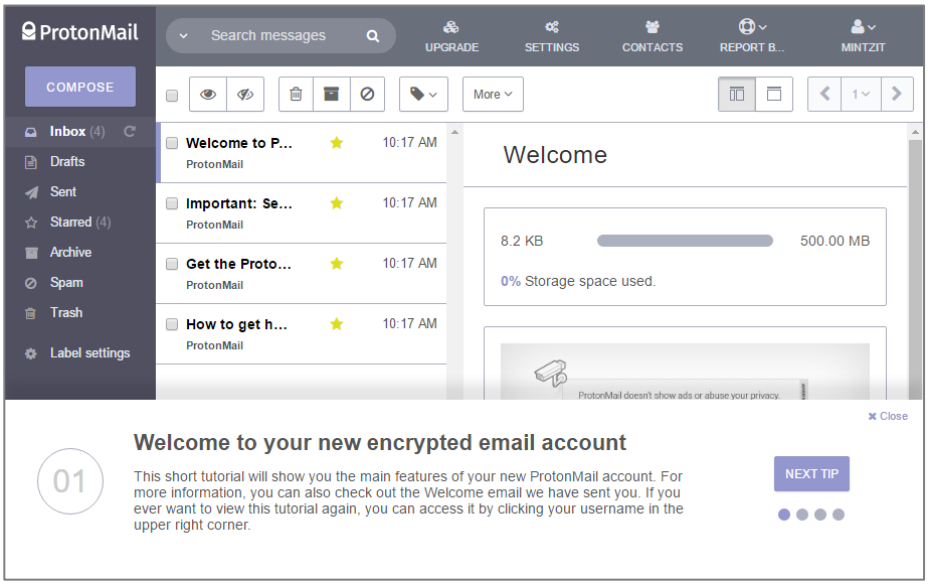
6. ProtonMail begins to create your account.



7. At this stage enter the name that will be seen by other users. You also have the option of downloading iOS or Android Apps. Next click on the *Finish* button.



8. You have now finished the setup process. You will see a short tutorial on the bottom of your screen, it is recommended to read through it to understand some more of the features available to you.



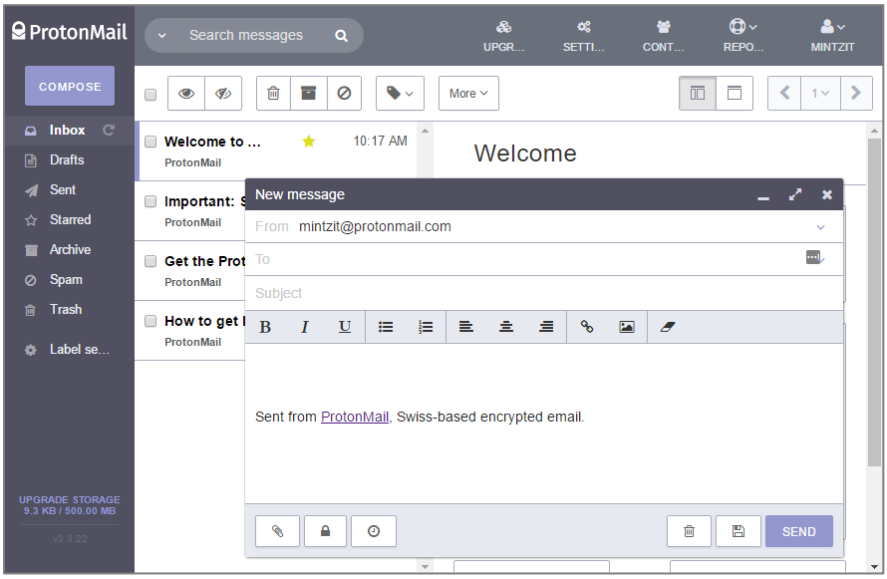
15.7.2 Assignment: Create and Send an Encrypted ProtonMail Email

In this assignment, you send your first fully encrypted email through ProtonMail.

- **Prerequisite**: Completion of the previous assignment, or an existing ProtonMail account.

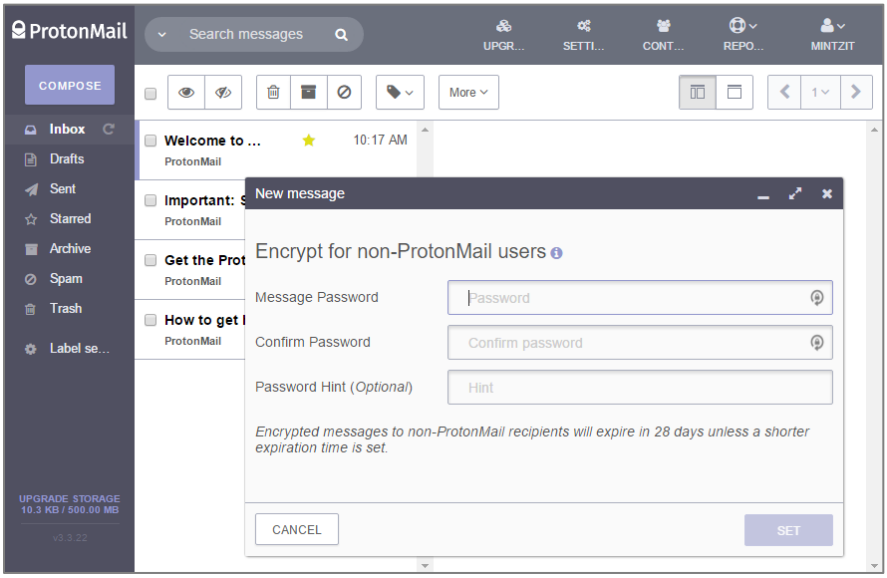
1. If you have just completed the previous assignment, select the *Compose* button in the top left. If not, use your web browser to visit *ProtonMail* at *https://ProtonMail.com*, select the *Login* link, and then log in.

2. The *New Message* window should now be showing, enter the recipient email address, subject and a brief message.

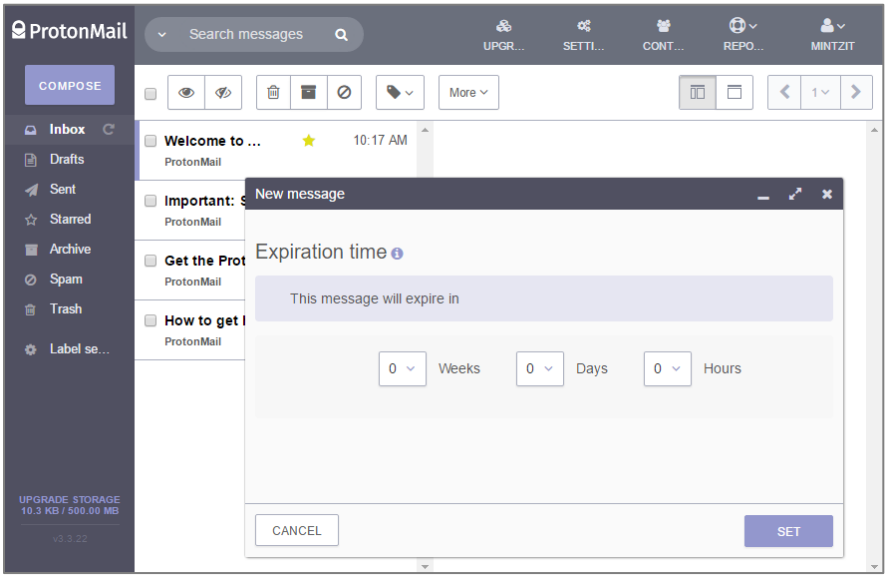


3. Scroll to the bottom of the page, and then configure to your taste. The *Lock* icon allows you to set a password requirement to open the email from a non-ProtonMail account.

    - If you are sending to a recipient who is not a ProtonMail account, you have the option to manually set an encryption password in this screen. If you were sending to another ProtonMail account, the message is automatically encrypted, without need to enter a password.



4. The *Clock* icon allows you to set an expiration time for the email.



5. Once you have finished configuring your email, click the *Send* button. It will take a moment to encrypt and then send.

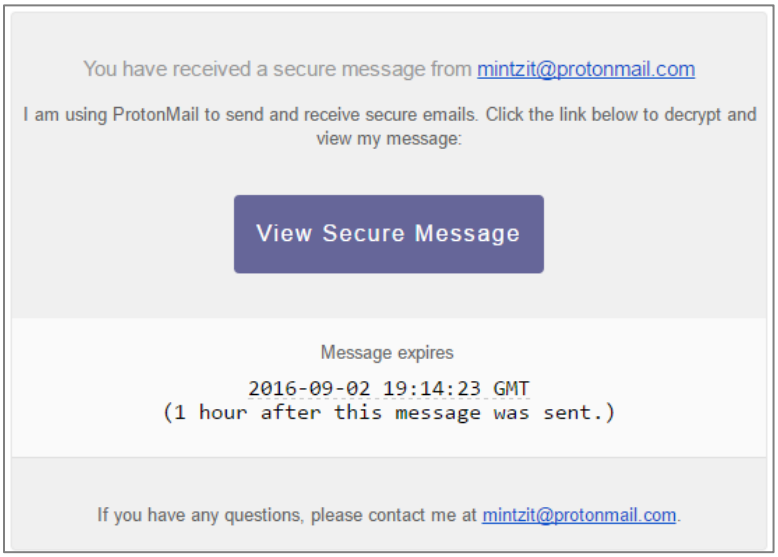
Notification of your email has been sent to the recipient.

15.7.3 Assignment: Receive and Respond to a ProtonMail Secure Email

In this assignment, you reply to a ProtonMail secure email.

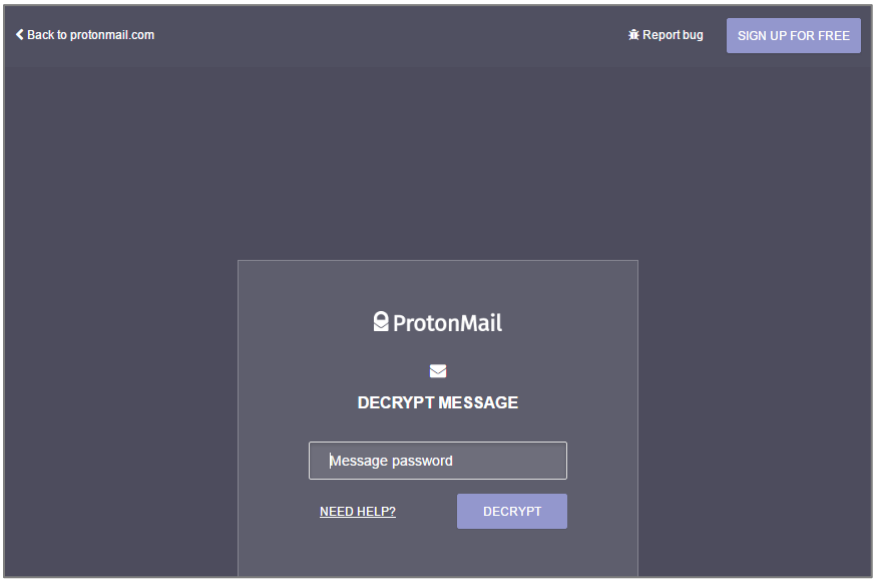
- Prerequisites: Completion of the previous two assignments.

1. After you have sent an email from your ProtonMail account (previous assignment), the recipient receives the following email. To view the message, the recipient selects the *View Secure Message* button within the email.

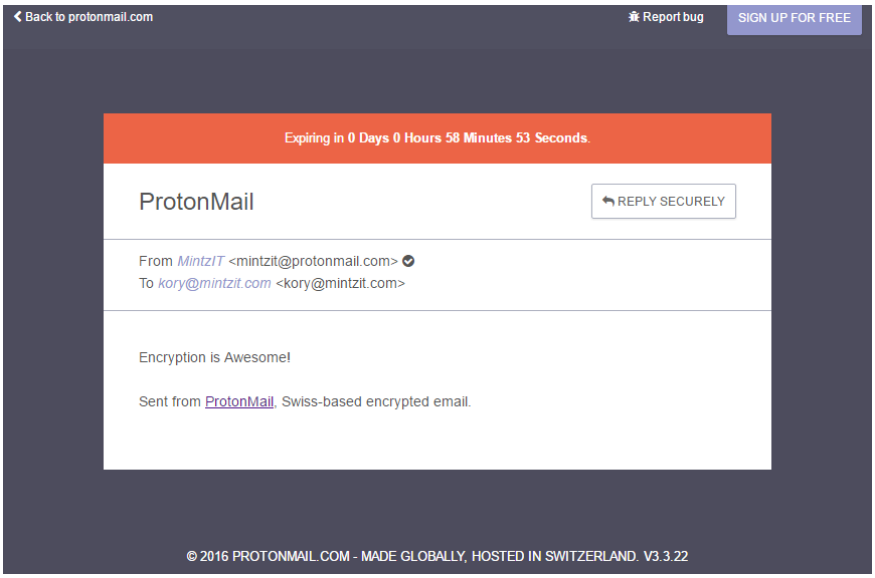


2. If the recipient already has a ProtonMail account, go to step 5. If the recipient does not have a ProtonMail account, they have the option of signing up for

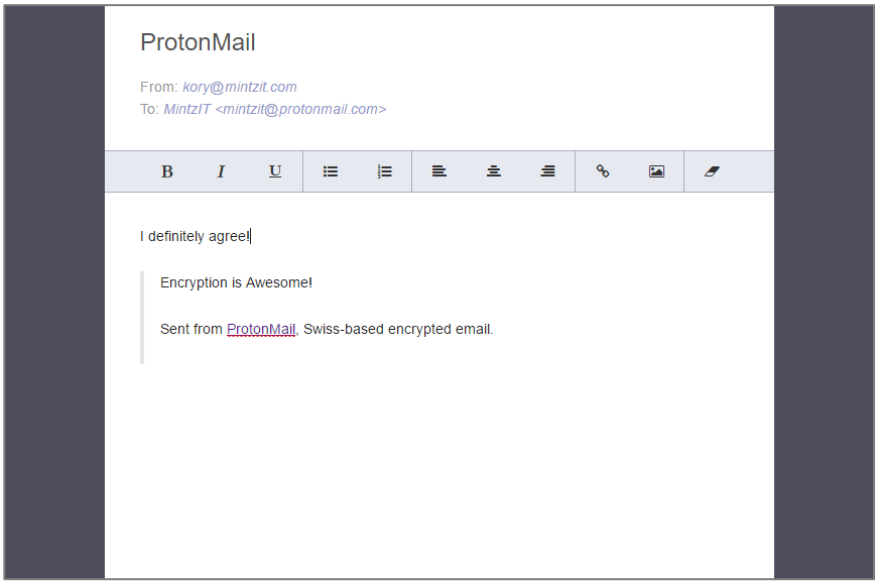
ProtonMail in the top right of the webpage. If they do not wish to sign up they may instead enter the required password to access their email on this page.



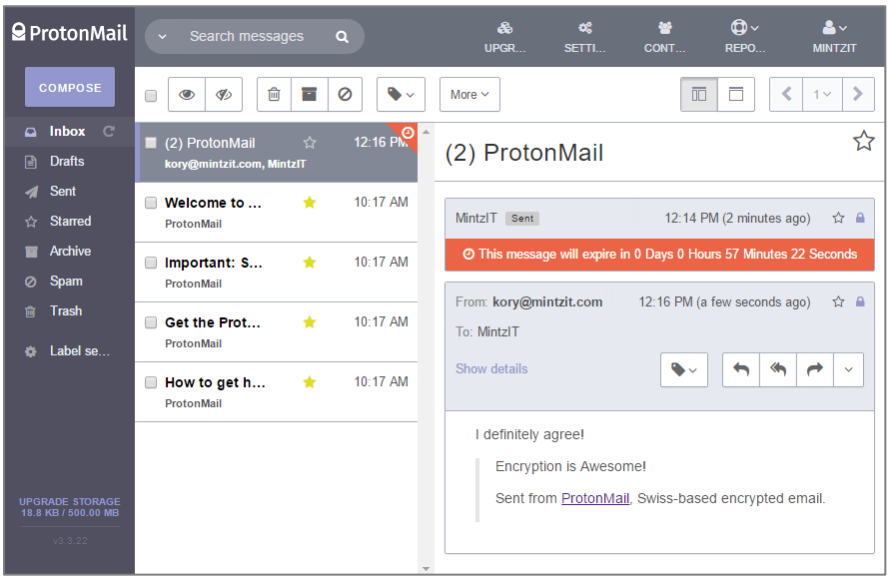
3. After entering the required password, the email is displayed in the recipient's browser. The recipient is also able to reply via this webpage by selecting *Reply Securely*.



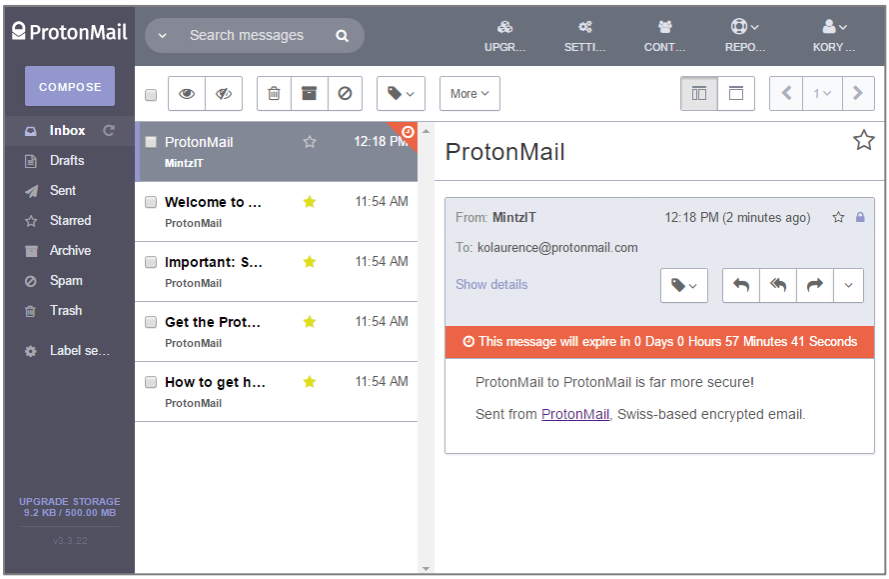
4. The recipient then types in their reply and clicks on the *Send* button in the bottom right.

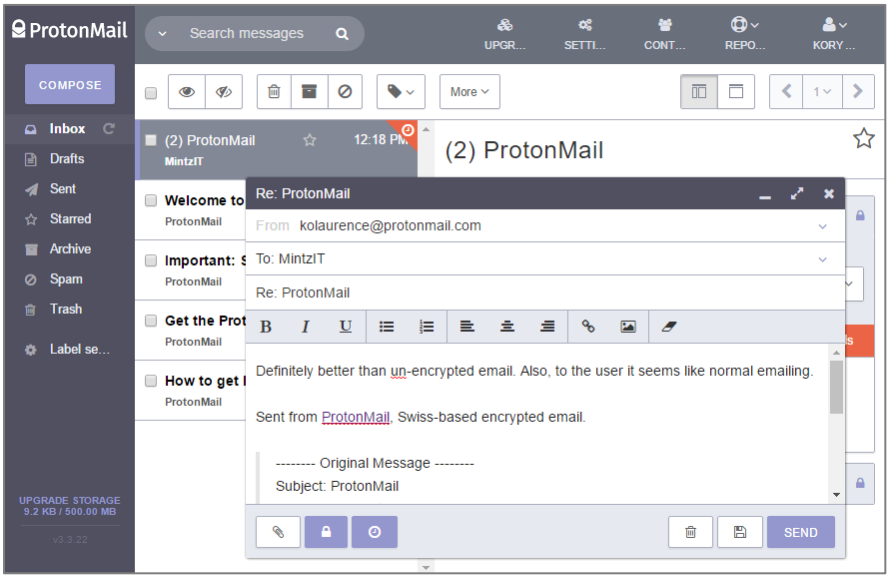


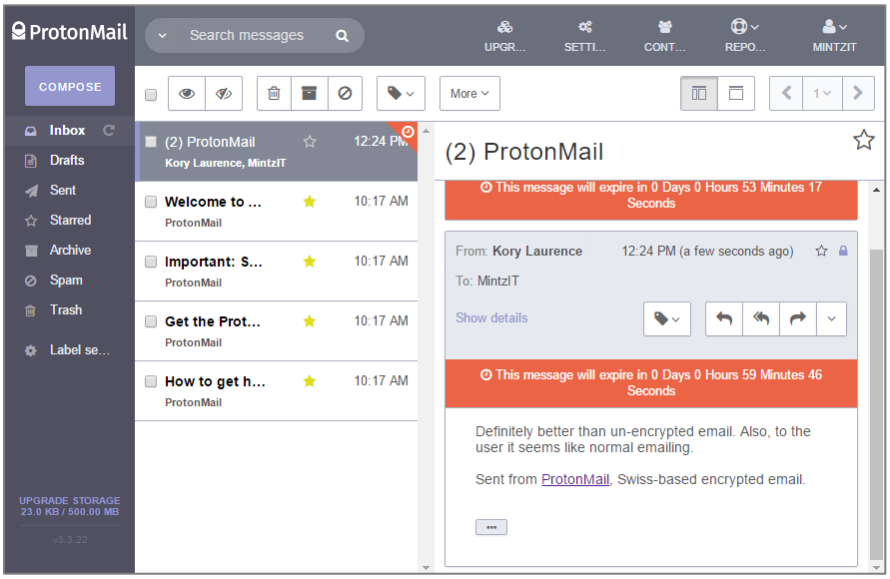
5. The original sender will receive a reply.



6. For either the original sender or the recipient, if they are using ProtonMail, it will show in their inbox like normal email. The email is decrypted and is fully viewable. Note that at no point is the message transmitted across the internet without encryption.






ProtonMail
Search messages
UPGR...
SETTI...
CONT...
REPO...
MINTZIT
COMPOSE
Inbox
Drafts
Sent
Starred
Archive
Spam
Trash
Label se...
UPGRADE STORAGE
23.0 KB / 500.00 MB
v3.3.22
More
(2) ProtonMail
Kory Laurence, MintzIT
12:24 PM
Welcome to ...
ProtonMail
10:17 AM
Important: S...
ProtonMail
10:17 AM
Get the Prot...
ProtonMail
10:17 AM
How to get h...
ProtonMail
10:17 AM
(2) ProtonMail
This message will expire in 0 Days 0 Hours 53 Minutes 17 Seconds
From: Kory Laurence
12:24 PM (a few seconds ago)
To: MintzIT
Show details
This message will expire in 0 Days 0 Hours 59 Minutes 46 Seconds
Definitely better than un-encrypted email. Also, to the user it seems like normal emailing.
Sent from ProtonMail, Swiss-based encrypted email.

15.8 End-To-End Secure Email With GNU Privacy Guard

The gold standard for email security is to fully encrypt the message at the sender's computer in a format that only the intended recipient can decrypt. This tool also must be capable of alerting the recipient if the message has been tampered with in any way (i.e., a man-in-the-middle attack.) The leader in this arena is PGP (Pretty Good Privacy), now owned and maintained by Symantec. Fortunately, there is an open source utility that provides all the core functionality and security of PGP, for free.

Setting up *GPG*[10] (GNU Privacy Guard)–available for macOS, Windows, and Linux–takes a few more steps than our previous strategies in this section, and those with whom you wish to exchange secure email will need to also install GPG. But once both sender and recipient have their GPG in place, it is effortless to share fully encrypted messages.

Both PGP and GPG use the same strategy to securely encrypt email communications, and can exchange email with each other. Each user creates a *public key* and a *private key.* The Public Key typically is stored at a GPG server in the cloud, which can be found with a search for your name. The Private Key remains only on the user's computer. When sending an email to another person, your email application will automatically use the recipient's Public Key to encrypt the message. When the recipient receives the email, only the recipient' Private Key is able to decrypt and open the message.

If there are shortcomings to PGP and GPG, one is that as of this writing, there are only two iOS apps and one Android app, none of which are well received. Also, GPG is designed to work within an email client application, not a web browser. Although there are plug-ins for FireFox to allow for GPG, you are best to stick with the built-in Mail.app. Another issue is that before one can exchange encrypted email with someone else, both need to manually retrieve each other's public key. This typically is just a two-click process, but still…

[10] *https://gnupg.org/*

Cryptography can quickly become Ph.D.-level material. I will cover everything you are likely to need to fully enable encryption and digital signing using GPG. Should you wish to delve deeper, visit the GPGTools Support site[11].

15.8.1 Assignment: Install GPG and Generate a Public Key

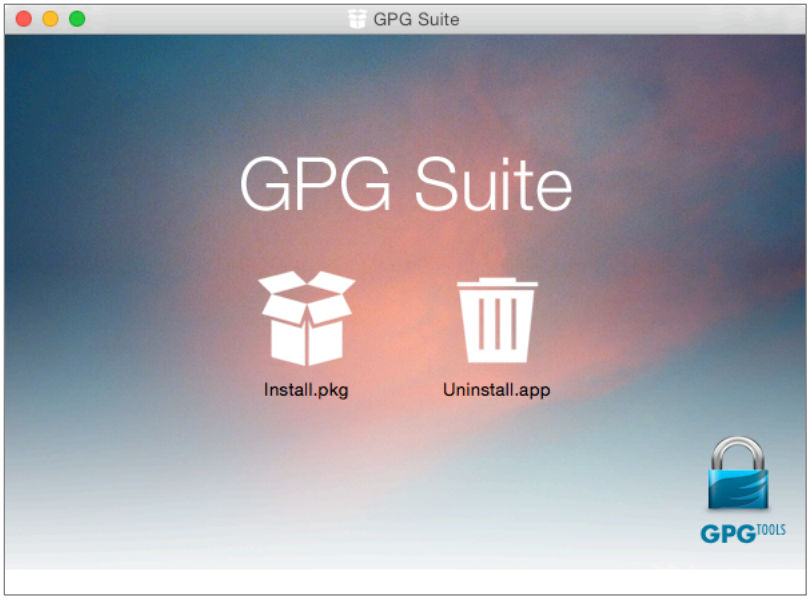
To encrypt your email, you need to have GPG installed, and have your recipient's Public Key installed in your GPG keychain. For your intended recipient to decrypt and read your email, the recipient needs to have GPG installed (or Gpg4win[12] if using Windows, or GPA[13] if using Linux.) The recipient will also need to have your Public Key stored in their computer.

In this assignment, you install GPG on your computer, and upload your Public Key to the *GPG Public Key Server*, making it available to anyone wishing to send encrypted email to you.

1. Use your browser to visit *GPGTools https://gpgtools.org,* and then select the *Download GPG Suite* button.

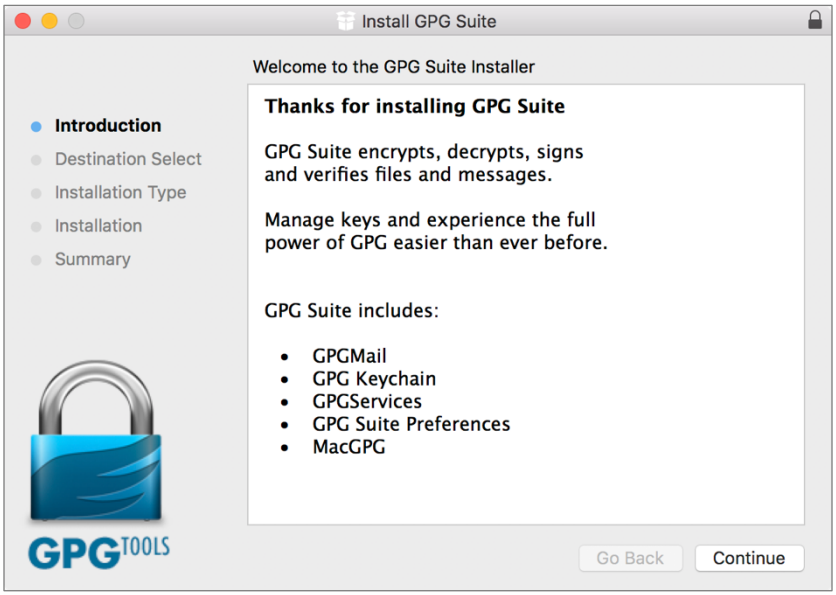
[11] *http://support.gpgtools.org/kb*
[12] *https://www.gpg4win.org*
[13] *https://www.gnupg.org/related_software/gpa/index.en.html*

2. The software will begin to download to your computer.
3. Go to your Downloads folder, locate and then double-click on the *GPG Suite.dmg* file. This will mount the GPG disk image to your desktop, and then open the disk image to reveal the GPG Suite window.

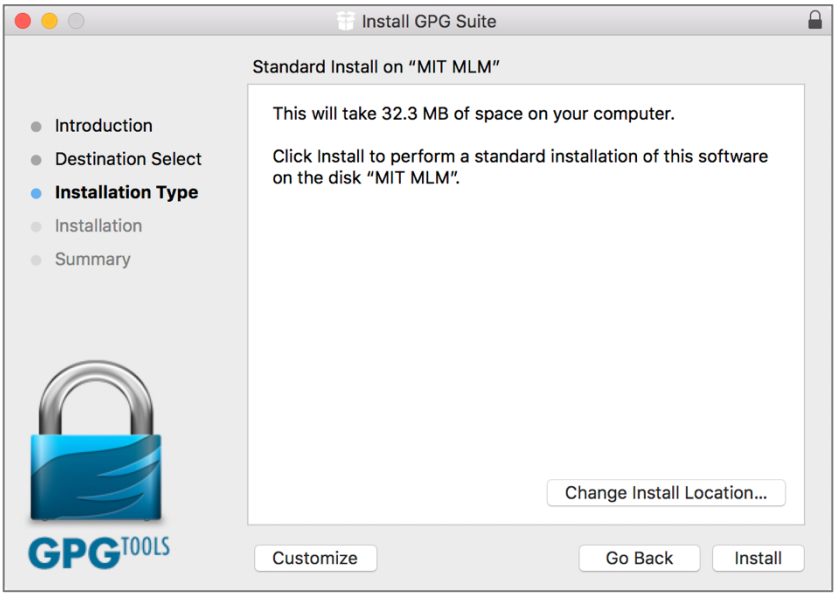


4. Double-click the *Install.pkg* icon inside of the GPG Suite window to launch the *Install GPG Suite installer*.

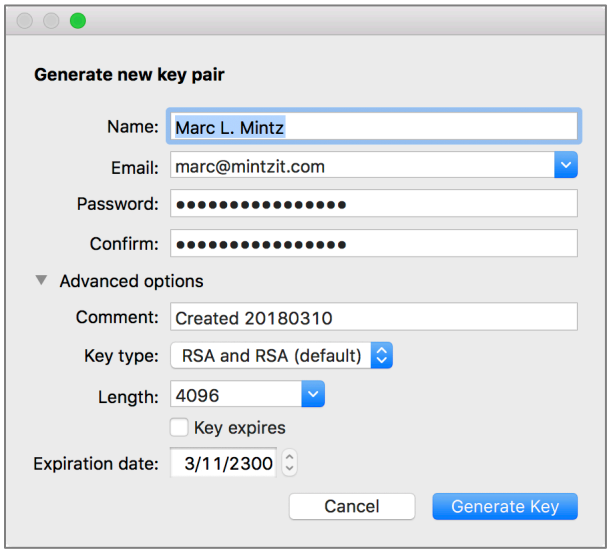
5. Select the *Continue* button.



6. At the *Standard Install on "<Name of hard drive>"* window. Select the *Install* button.



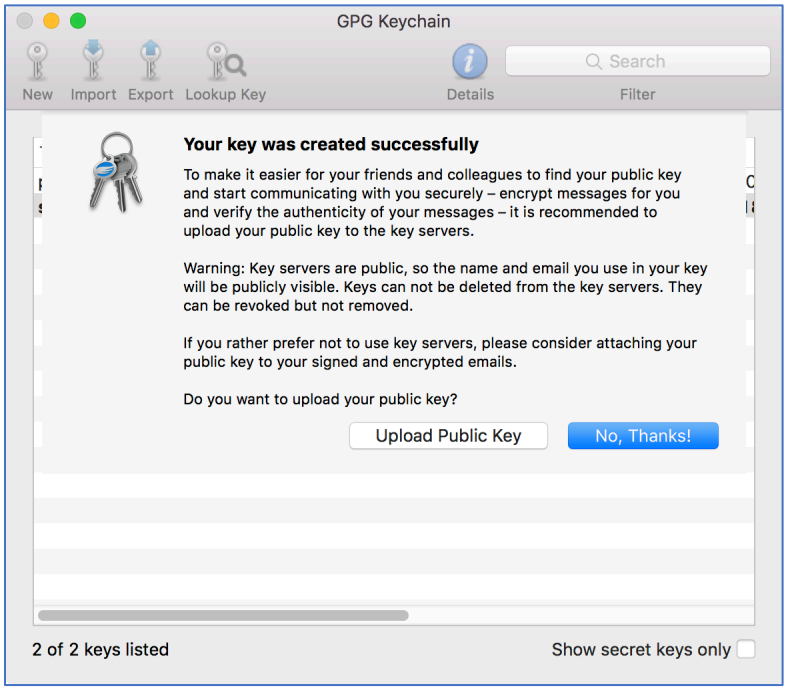
7. The authentication window will appear. Enter an administrator name and password, and then select the *Install Software* button.
8. *The installation was completed successfully* window appears. Click the *Close* button.
9. The *GPG Keychain.app*, located in /Applications opens.
10. Select the *Advanced Options* link to expand the window, and then complete all fields.



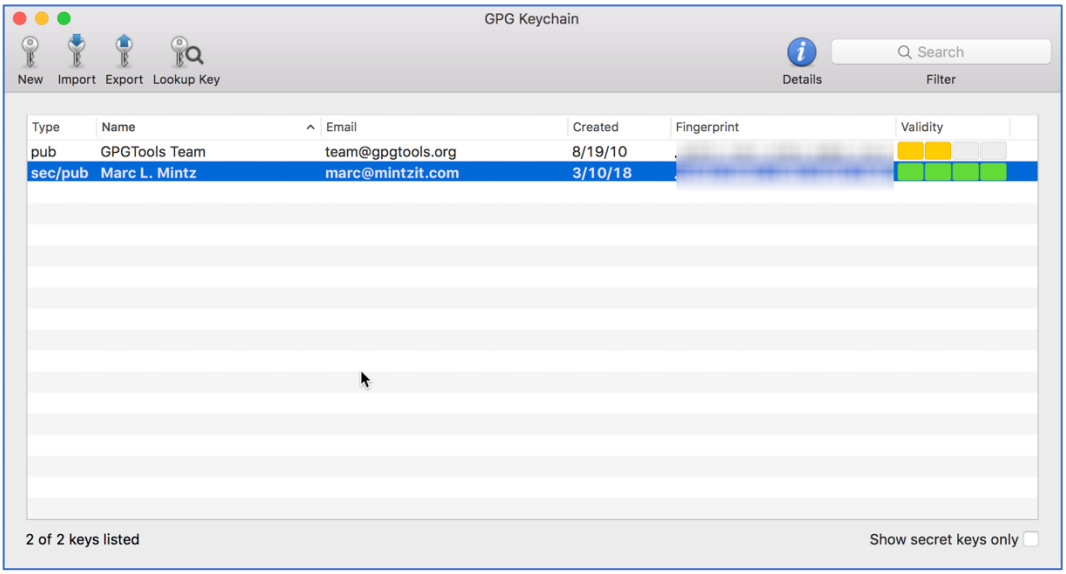
- *Name*: Enter your full name as used in your email.
- *Email*: Enter the email address for which GPG encryption is being configured.
- *Password* & *Confirm*: This is a password to protect access to this record. As with all passwords, make it strong.
- *Comment*: As you may eventually create many keys, enter a comment to refresh something unique about this key pair.
- *Key type*: Select *RSA and RSA (default)*. This is the strongest option currently available.
- *Length*: Select 4096. The larger the encryption bit depth, the more secure.

- *Expiration Date*: I typically leave this disabled, allowing any of my encrypted email to be accessed (given the proper credentials) forever. However, if you prefer to set your key to self-expire, making any sent emails created with it unreadable after a certain date, then by all means enable this option.

11. Select the *Generate key* button.
12. The new key will start to generate. During this time, the random key generator uses activity on your computer to help create a random key. You should move your cursor, or type some characters in another application during this time.
13. The *Your key was created successfully* window appears. This window gives the option to upload your public key. Remember, the public key allows others to send encrypted email to you–it does not present a security concern if others have access to it. Click the *Upload Public Key* button.



14. When your Public Key generation completes, the *GPG Keychain* window will display your new key.



Congratulations! You have successfully installed GPG to help encrypt your email.

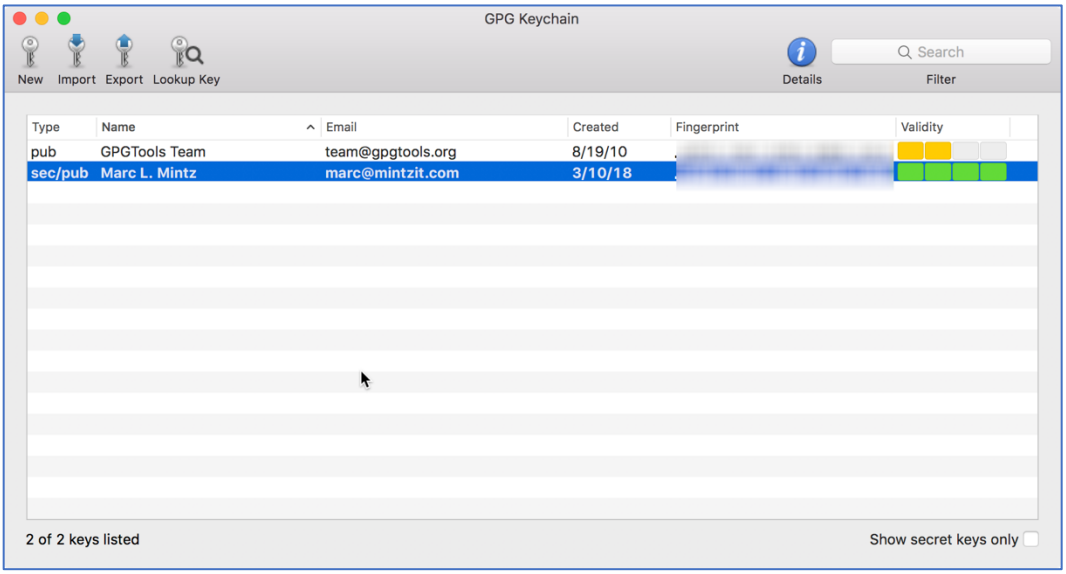
15.8.2 Assignment: Add Other Email Addresses to a Public Key

- Prerequisite: Completion of the previous assignment.

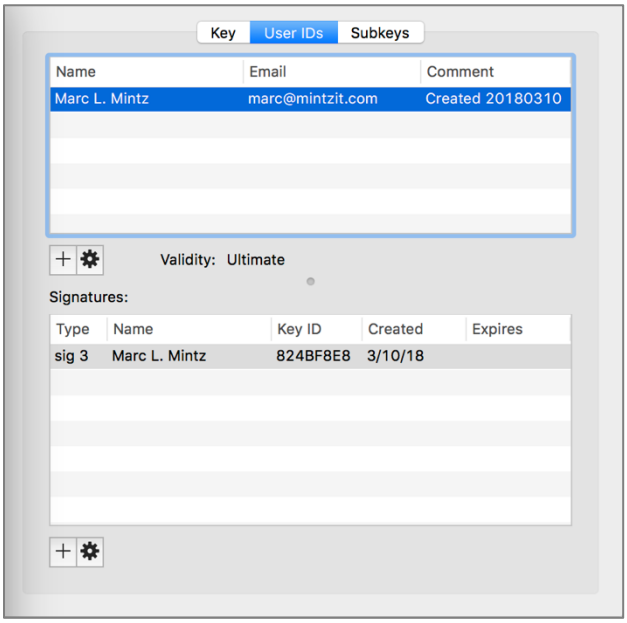
Many people have more than one email address. If you wish, you may create keys for each of your other addresses simply by repeating each of the steps in the previous assignment. However, you may find that both tedious and somewhat redundant. An alternative is to bind all your email addresses together under one key.

In this assignment, you add your other email.

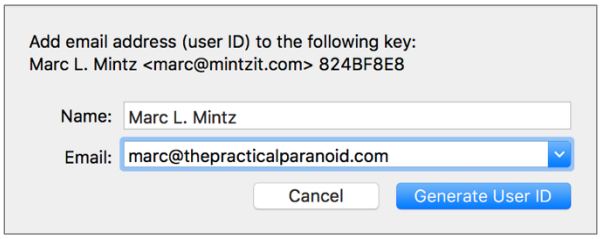
1. Open *GPG Keychain*, located in your */Applications* folder, and then double-click on your entry from the previous assignment.



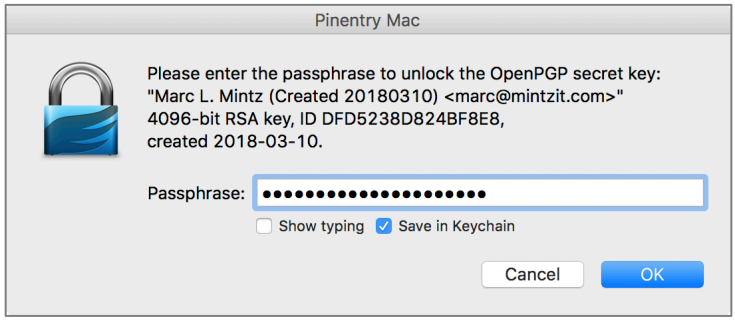
2. The *Key Inspector* window will open. Select the *User IDs* tab, from top half of the window, select the account *Name,* and then select the + button.



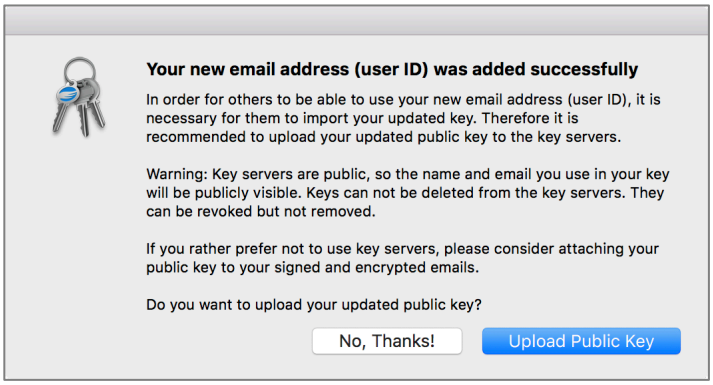
3. In the window that opens, enter your *Full name,* along with the new *Email address* you want to be bound to your original email/key combination, and then select the *Generate user ID* button.



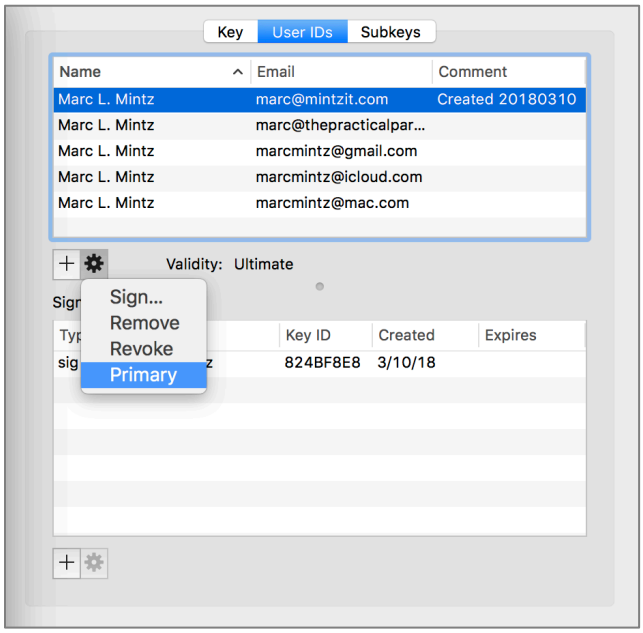
4. In the *Pinentry Mac* window:
    a. enter the password/passphrase used when creating the original signature.
    b. Enable *Save in Keychain* checkbox.
    c. Click the *OK* button.



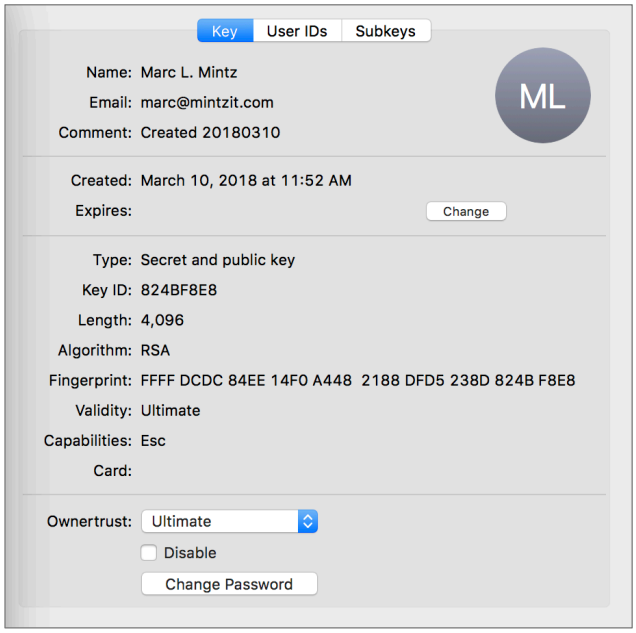
5. The *Your new email address (user ID) was added successfully* window appears. Click *Upload Public Key* button.



6. Repeat steps 2-5 for each of your email addresses.
7. When all your email addresses have been added, select the one address you use most often, click the *gear* icon, and then select the *Primary* button to set this as your primary account.

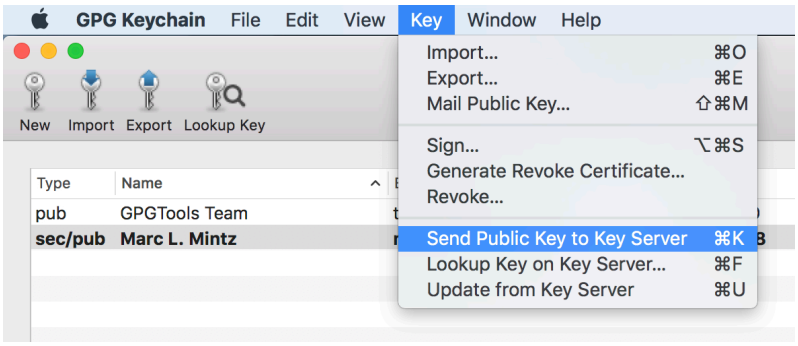


8. Though not required, let's add a photo to better identify you. Select the *Key* tab.



9. Click the circle with your initials located in the top right corner. This will open a window to locate the desired photo.
10. Navigate your computer to locate the desired photo, and then double-click the photo to add it to your keys.

11. Lastly, upload your changes to the Public Key Server. Select the *Key* menu > *Send Public Key to Server*.
    - Note: You may also mail your public key to someone else from the *Key* menu > *Mail Public Key…*



Congratulations! You have successfully added all your email accounts to GPG, allowing encrypted communications with any account.

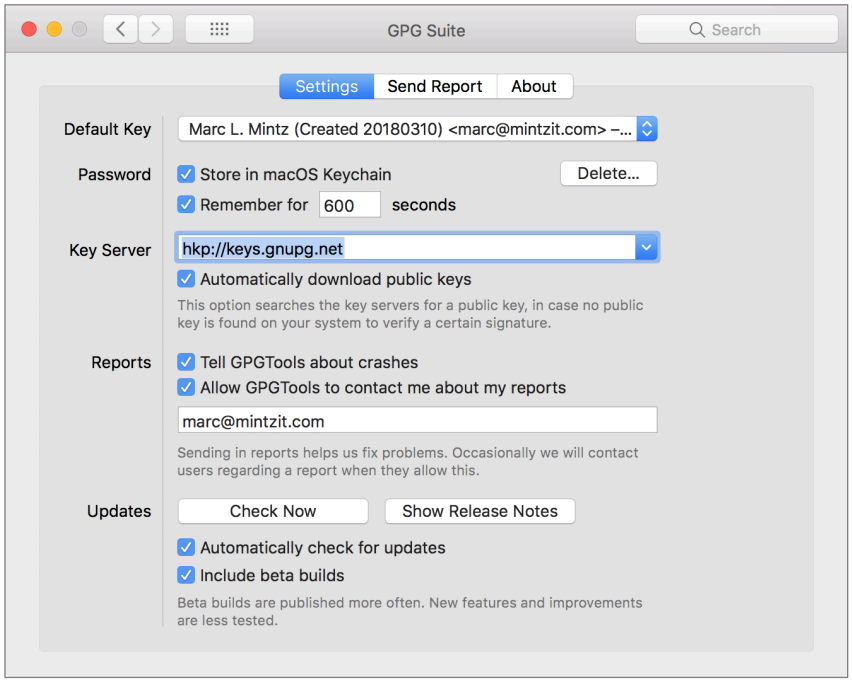
15.8.3 Assignment: Configure GPGMail Preferences

In this assignment, you configure GPGMail Preferences.

1. Open the *Mail.app*, open the *Mail* menu > *Preferences* > *GPG Mail*, and then configure as shown below.

2. Close the *Preferences* window.
3. *Quit* Mail.app.

4. Open the *Apple* menu > *System Preferences* > *GPG Suite,* select the *Settings* tab, and then configure as follows.



- *Default Key*: From the pop-up menu select your primary email account.
- Enable *Password: Store in macOS Keychain.*
- Enable: *Password: Remember for 600 seconds.*
- *Key server*: Unless your organization prefers using another server, stick with the default of *hkp://keys.gnupg.net*.
- Enable: *Reports Tell GPGTools about crashes,* and *Allow GPGTools to contact me about my reports*. Enter your email address for GPGTools to use when discussing reports.
- Enable: *Updates: Automatically check for updates,* and *Include beta builds.* Normally, I'm not fond of beta builds. But with GPTTools, it appears to be in constant beta.

5. *Quit* System Preferences.

Your GPG is now fully installed, configured, and ready for use!

15.8.4 Assignment: Install a Friend's Public Key

For you to send encrypted mail to someone else, it is necessary to have their *GPG Public Key*.

In this exercise, you find a friend's Public Key and add it to your GPG Keychain.

- Prerequisite: GPGTools must be installed.

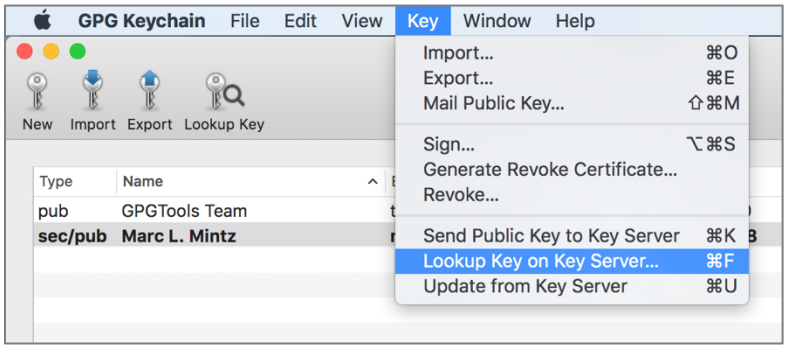
Option A: The No Sweat Strategy

The easiest way to add a friend's Public Key is to have them send to you an email from their GPG-enabled account (signed, but not encrypted.) Once you have their email, you also have their Public Key. But you may be listening a long time to crickets before they send you an email.

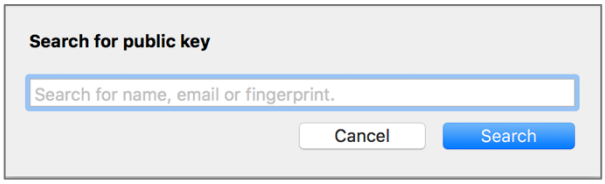
Option B: DIY

The Do It Yourself option is to lookup your friends key on a GPG key server.

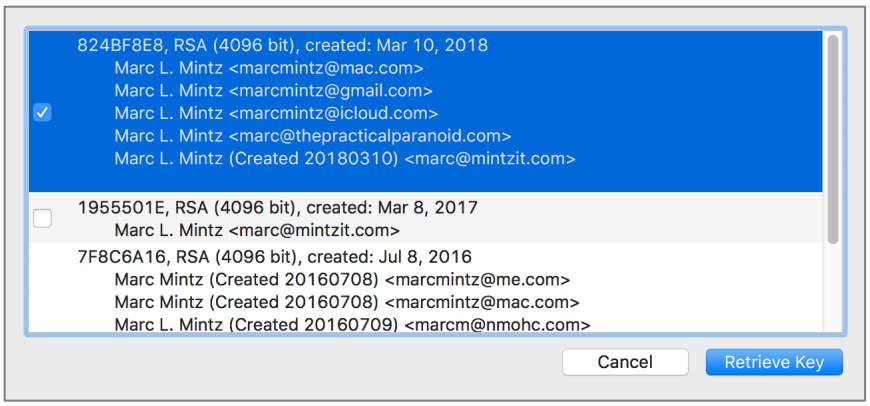
1. Open the *GPG Keychain Access.app* located in your */Applications/* folder.
2. Select *Key* menu > *Lookup key on key server.*



3. The *Search for public key* window opens.



4. Enter the full name of the person you wish to either send encrypted mail to, or receive from, and then select the *Search key* button. A list of possible matches appears. If you don't yet know anyone with a GPG key, feel free to use *Marc L. Mintz*. Shown below are the search results for a *Marc L. Mintz*.



5. the target public key (if you aren't sure which is correct, select all of them), and then select the *Retrieve key* button.
6. The Public Key is now added to your GPG Keychain.

You are now ready to send encrypted email to your friends!

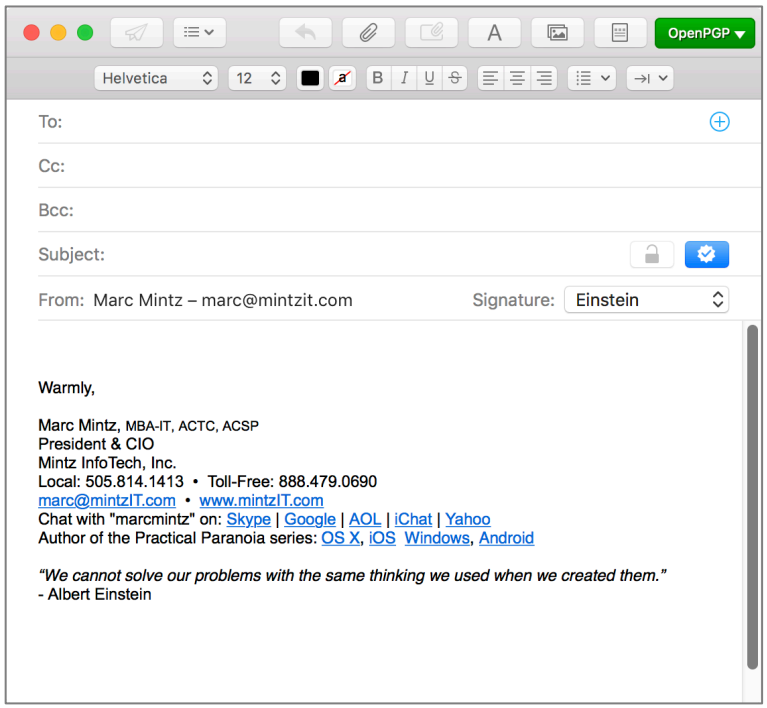
15.8.5 Assignment: Send a GPG-Encrypted and Signed Email

Once you have created your key and have the Public Key of the intended recipient from the previous assignments, you are ready to send your first encrypted and signed email.

In this assignment, you send your first GPG-encrypted and signed email.

1. Open your macOS *Mail.app*.

2. Create a new outgoing mail document. Notice that you have two new icons to the left of the *Subject* line.



   - *Lock* icon: Enables encryption for your document.
   - *Signed* (checkmark) icon: Enables signed emails. A signed email will notify the recipient if the message has been altered in any way between the sender and recipient.

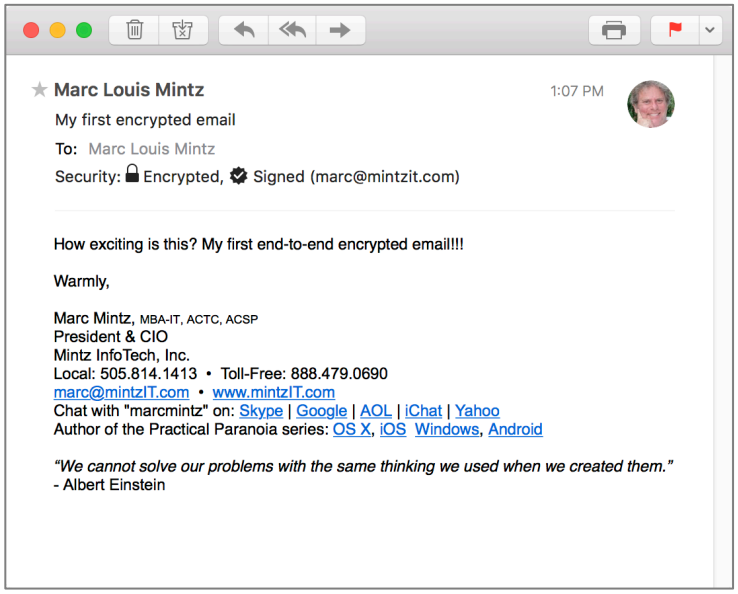
3. In the *To:* field, enter the email address of someone with GPG enabled on their computer (feel free to use my address of marc@mintzit.com for your test). Once you have entered an email address that is registered with GPG (as you have done in the previous assignment), the *Lock* icon will turn blue, allowing selection/enabling.
4. Verify the *Lock* icon is blue, indicating the email will be encrypted.
5. Select the *Send* button, and your email is on its way to the recipient, fully secure because only the designated recipient will be able to read the email.

Wahoo! You have sent your first securely encrypted email.

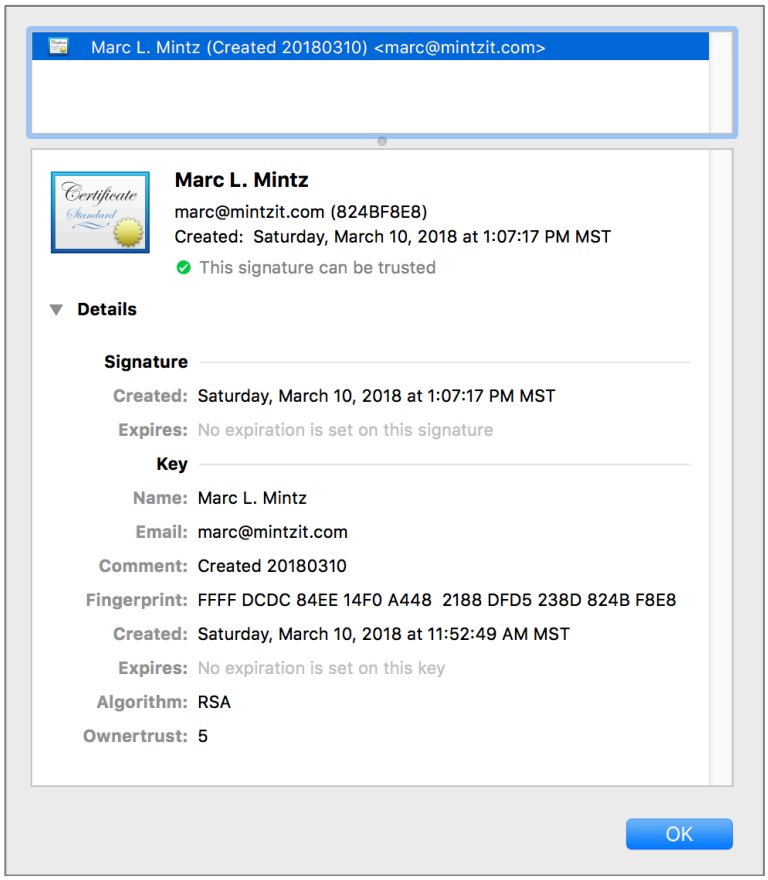
15.8.6 Assignment: Receive a GPG-Encrypted and Signed Email

In this assignment, you receive and read a GPG-encrypted and signed email.

1. When the email arrives at the recipient, it automatically is decrypted (assuming the recipient also has followed the steps detailed in the *Get Your Friend's Public Key* assignment). The message will have an indicator if it is encrypted or signed or both.



2. Should the recipient have any doubts as to the authenticity of the email, click on the *Signed* icon. The certificate will display. Note the Short ID to the right of the sender's email address.



3. This Short ID can be verified. The recipient can open *GPG Keychain Access*, double-click the sender's name, and then view their *Short ID* in the pop-out window.

15.8.7 Assignment: Encrypt and Sign Files with GPGServices

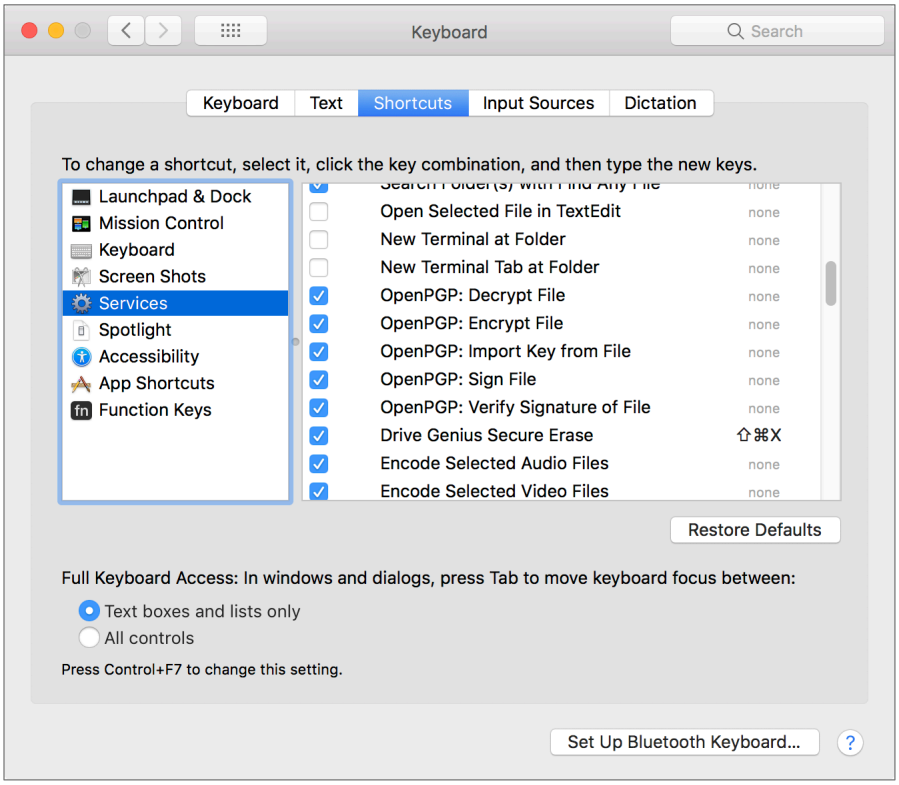
GPGServices allows encryption, decryption, and signing of any type of file for cross-platform use.

In this assignment, you encrypt and sign a file with GPGServices.

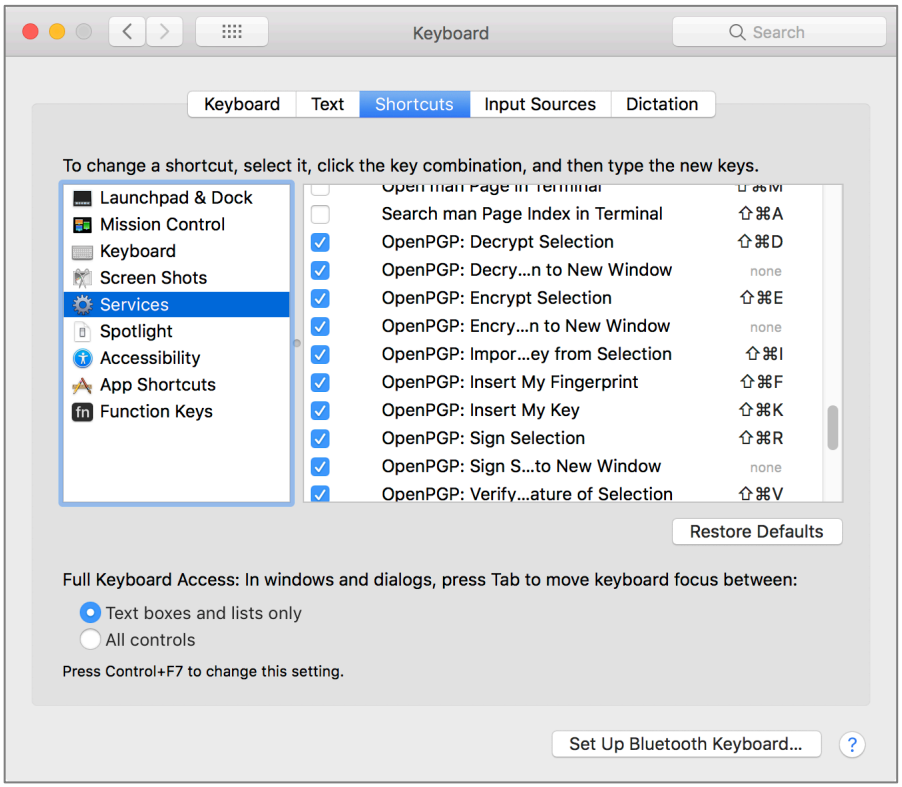
Verify all GPGServices have been activated

1. Open *System Preferences* > *Keyboard* > *Shortcuts* tab > *Services* in sidebar.

2. From under the *Files and Folders* group, verify that all *OpenPGP* modules are enabled.

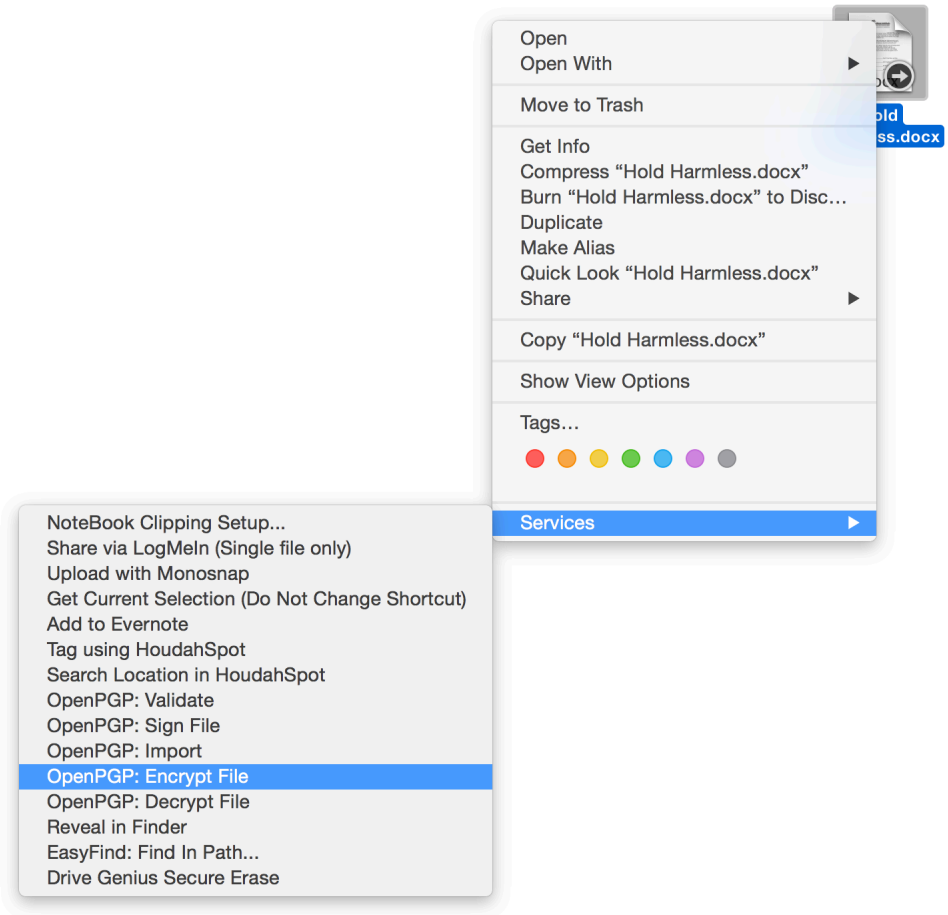


3. While still in the *System Preferences* > *Keyboard* > *Shortcuts* tab > *Services*, scroll down to the *Text* group, and then verify that all *OpenPGP* modules are enabled.

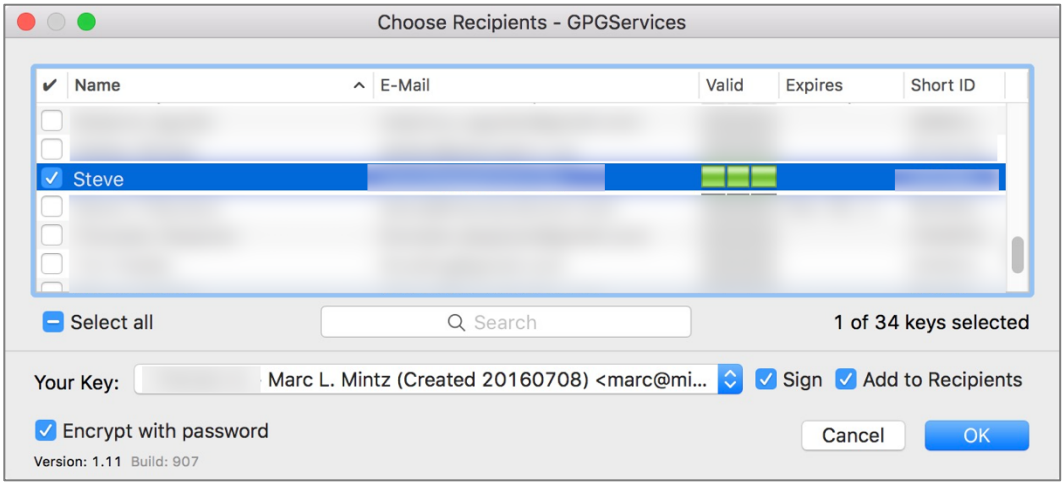


4. Close System Preferences.

5. To sign or encrypt a file or folder, right-click on it. From the pop-up menu, select *Services* > *OpenPGP: Encrypt File.*

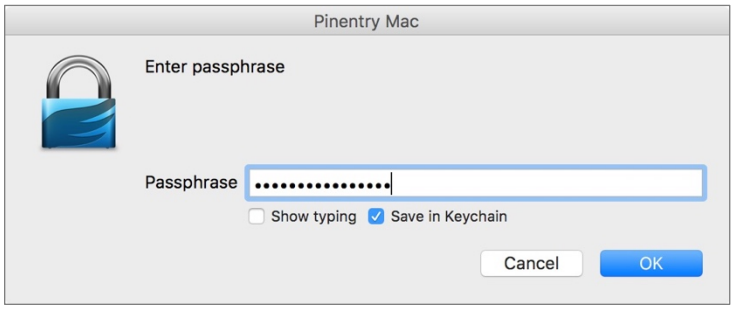


6. The *Choose Recipients – GPGServices* window appears. Configure as:

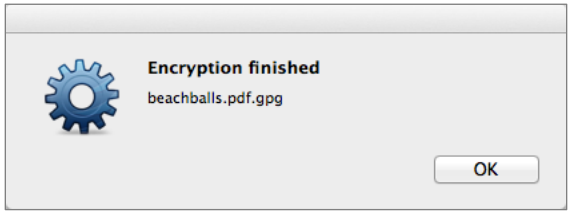


- Enable the checkbox for those you wish to allow to access this encrypted file or folder.
- Select which *Secret Key* will be used (which of your emails).
- Enable the *Sign* checkbox so the recipient can validate the file/folder came from you.
- You can further enhance security by enabling *Encrypt with password*. This will require the recipients to know a password in order to open the file.

7. Select the *OK* button.
8. If you have enabled *Encrypt with password,* at the *Pinentry Mac* window, enter the desired password in the *Passphrase* field, and then select the *OK* button.



9. You will be prompted a second time to enter the passphrase, do so, and then select the *OK* button.
10. In a few seconds, the *Encryption Finished* window appears. Select the *OK* button.



11. Your encrypted file will be found next to the original, with a *.gpg* file extension.

This encrypted file can now be attached to an email, uploaded to a server, or placed on a storage device. Only the selected recipients will be able to open and view the file.

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

S/MIME[14] (Secure/Multipurpose Internet Mail Extensions) uses the same fundamental strategy of employing both Public and Private Keys to secure email as do PGP and GPG. 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 GPG is that S/MIME is built right into both the macOS/OS X and the iOS Mail.app. No need to install another application.

Unlike GPG, 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. However, 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.

Because your keys are stored with a CA, if that CA resides in a country that complies with USA National Security Letters, then it is possible for the US Government agencies to gain access to your private key, giving them full access to your email. Should you have concerns over the government having access to your communications, you should use either PGP/GPG, or S/MIME with a CA located in a country that does not comply with National Security Letters.

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 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 sent the email, but that the name in the *From* field is tied to that email address.

[14] *http://en.wikipedia.org/wiki/S/MIME*

- **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), financial, legal, and business use.**

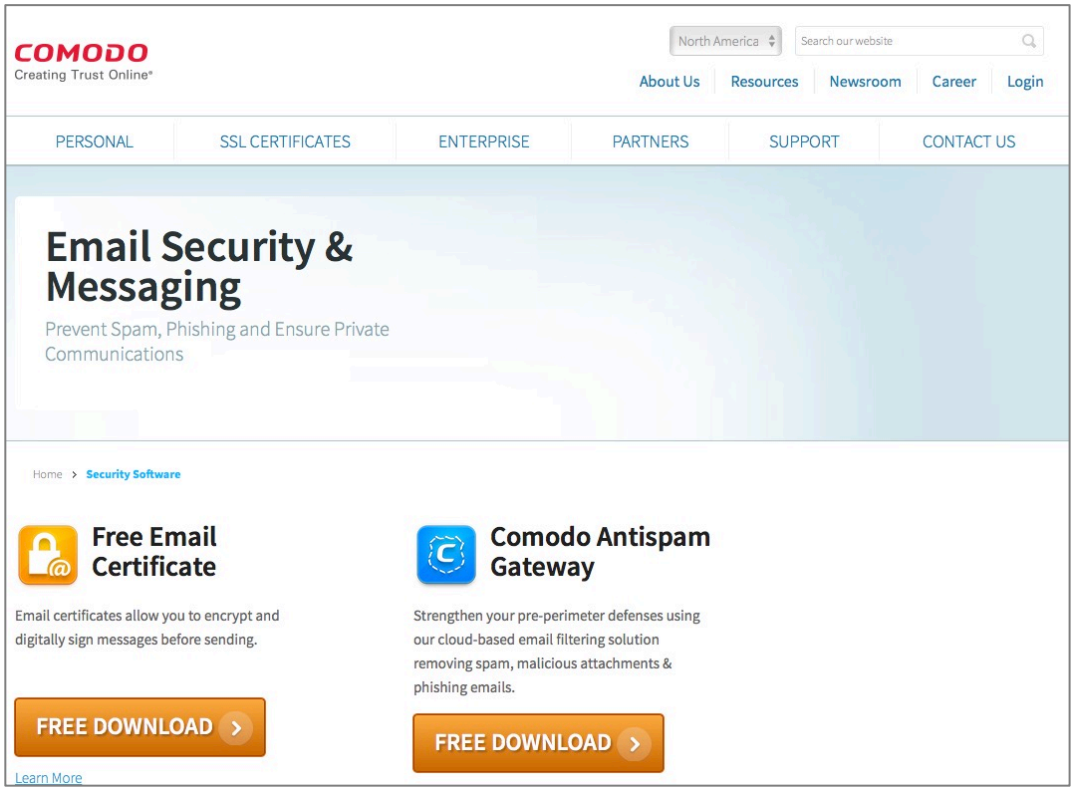
15.9.1 Assignment: Acquire a Free Class 1 S/MIME Certificate

In this assignment, you 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.

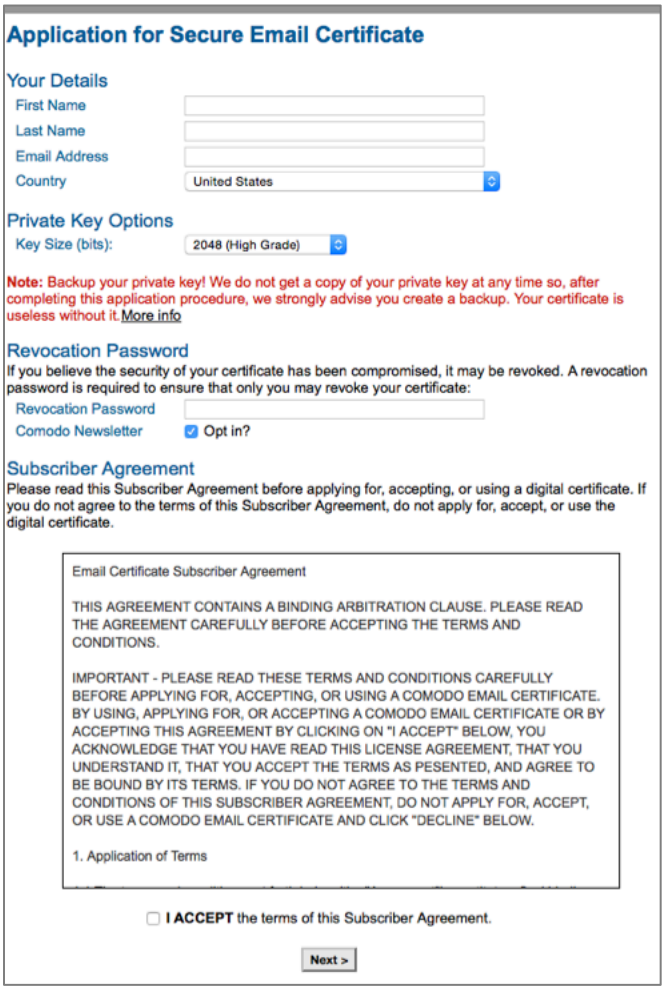
- Note: A Class 1 certificate is appropriate for home users only. For business use, see the assignment to *Acquire a Class 3 S/MIME Certificate.*

1. Open your web browser and surf to Comodo at *https://comodo.com*.
2. From the navigation bar, select the *Personal* tab > *Free Personal Email Certificate*.

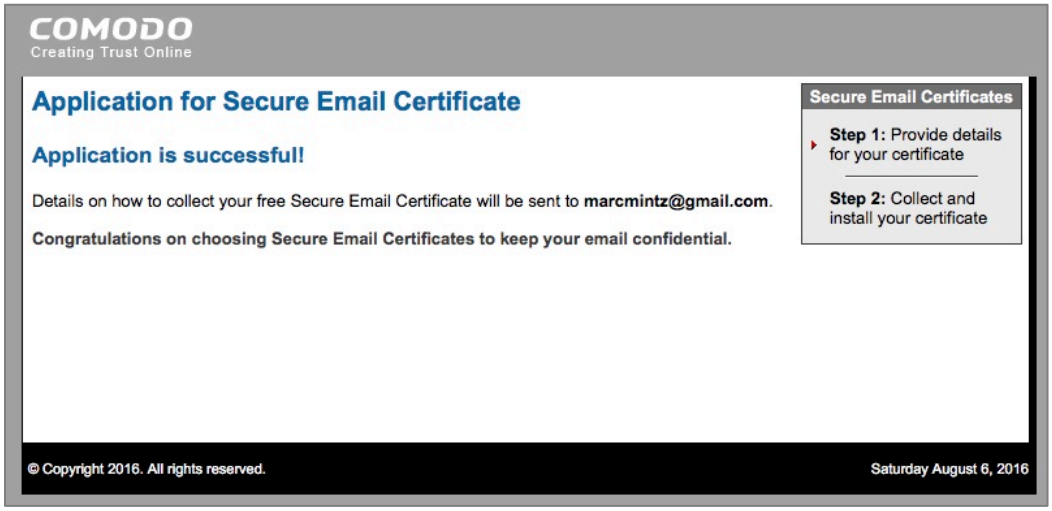
3. This takes you to the *Email Security & Messaging* page. Select the *Free Email Certificate* > *Free Download* button.



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.

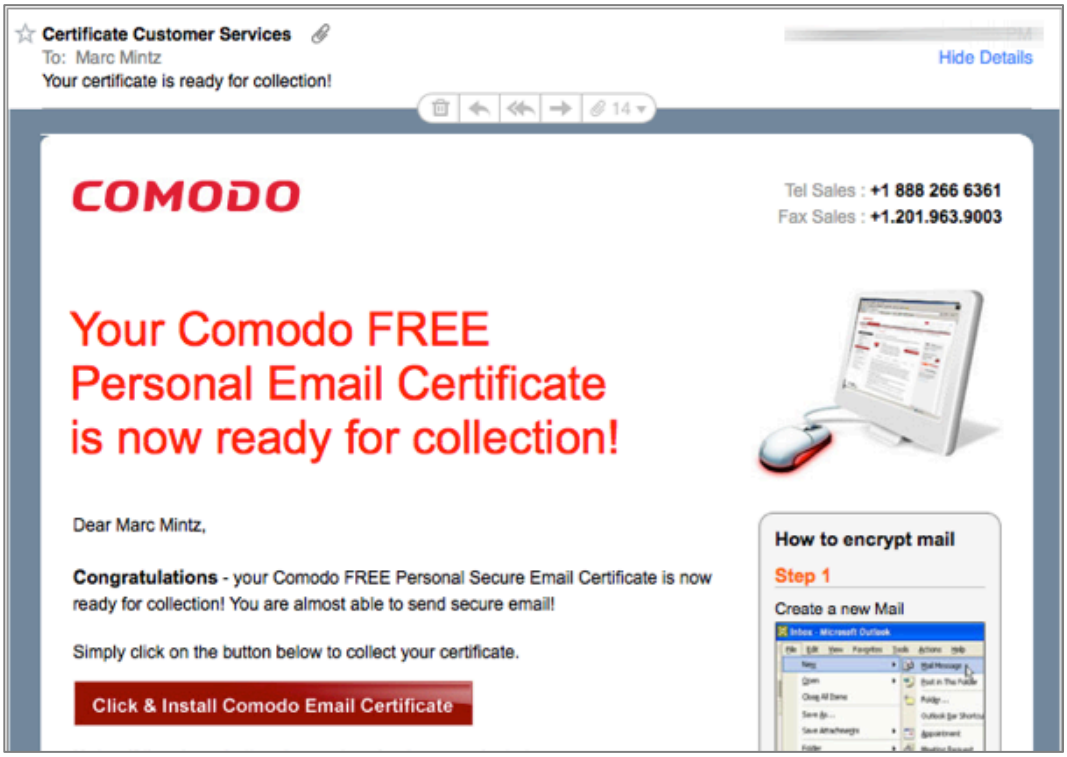


5. If all was completed correctly, you will see the *Application is Successful* page!



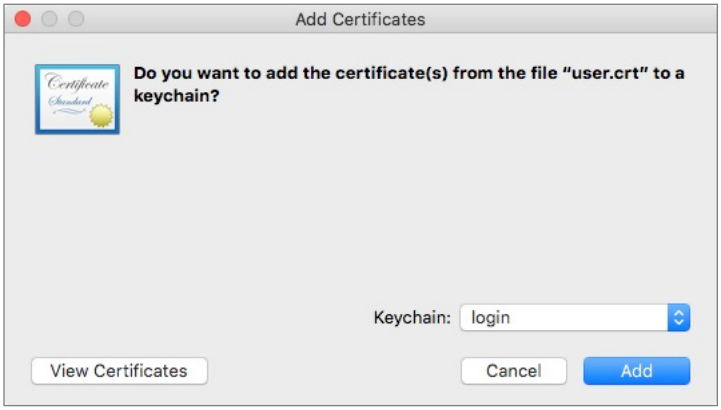
6. The certificate will be sent to the email address you specified.

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



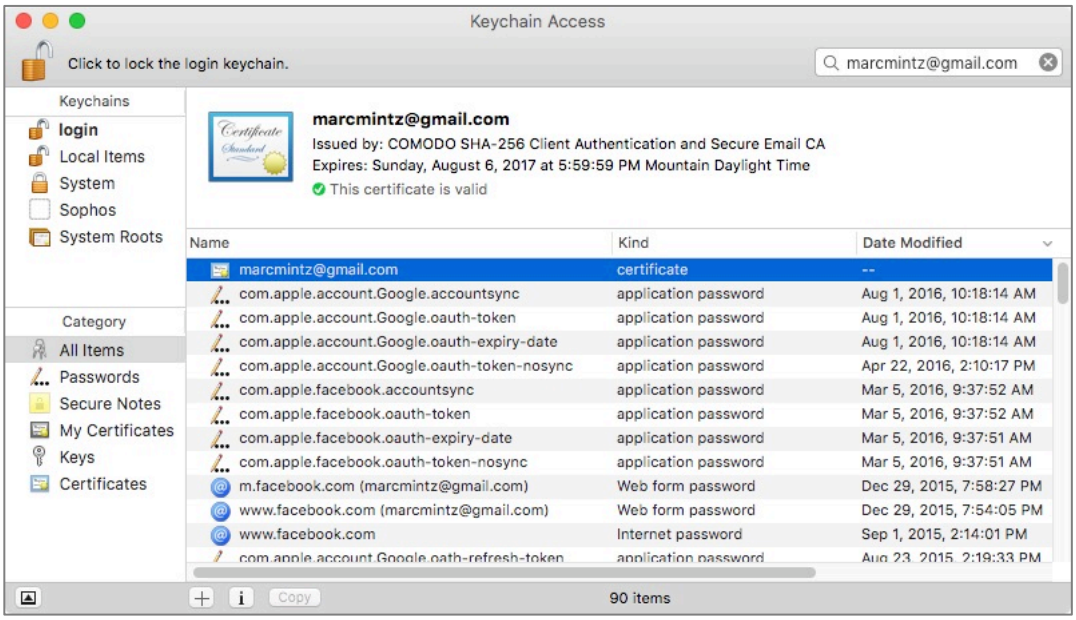
8. Although the button says *Click & Install Comodo Email Certificate*, all it does is download the certificate. You will need to manually install the certificate.
9. Once downloaded, the certificate will be found in your *Downloads* folder, named something like *user.crt*. Navigate in the Finder to 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*, and then select the *Add* button. This will add the certificate to your own default Keychain database,

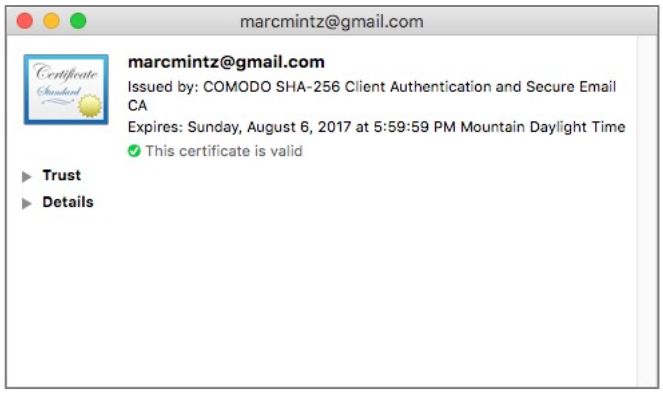


Validate Certificate Installation

11. To quickly find the new certificate, in the Keychain Access utility, in the *Search* field, enter the email address for the new certificate, and then tap the *Return* or *Enter* key.



12. Double-click on the new certificate. This will open the certificate info window.



13. Quit the Keychain Access application.

14. Repeat steps 1-10 for each of your email addresses for which you need secure communications.

Wahoo! The hard part is over. You now are the proud owner (at least for a year) of email certificates for each of your email accounts. Next step is to migrate the certificate to your iOS device.

15.9.2 Assignment: Acquire A Class 3 S/MIME Certificate for Business Use

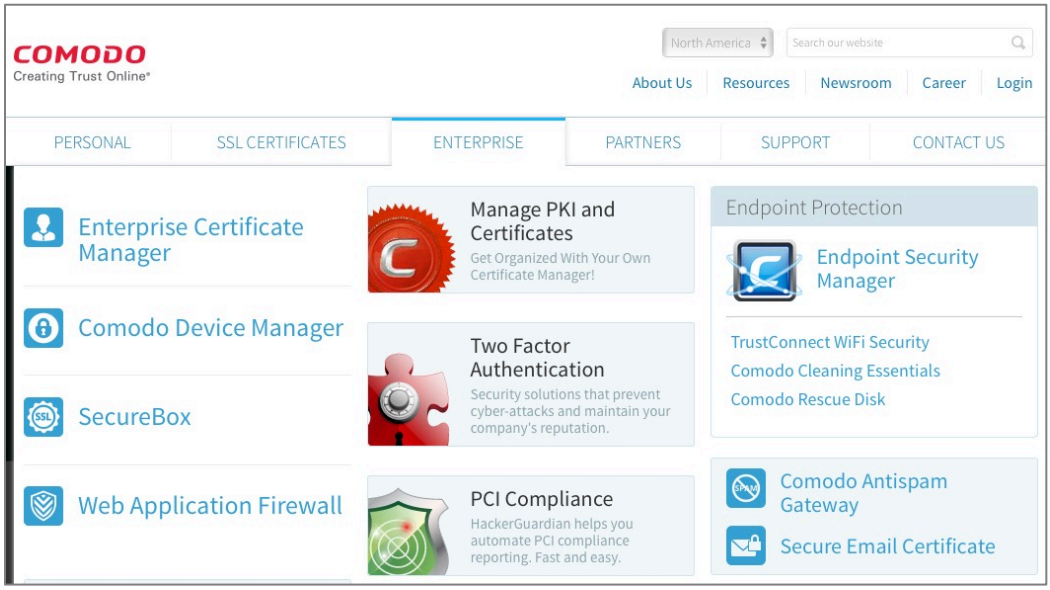
Getting a Class 3 certificate is significantly more involved than that of a Class 1. This is due to the need for identity verification, but also to the need for an infrastructure to help with managing potentially thousands of email addresses within an organization.

In this assignment, you acquire and configure a Class 3 S/MIME Certificate from Comodo.

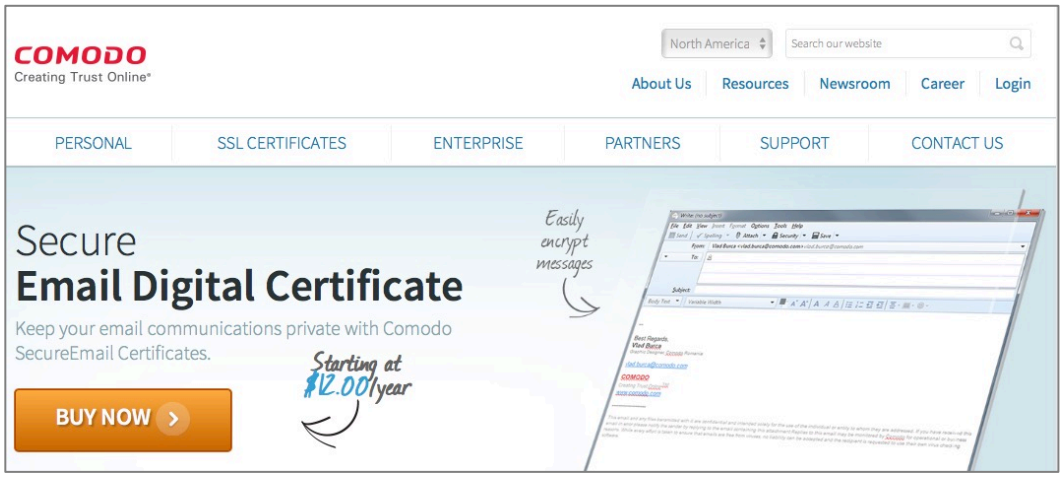
- Note: A Class 3 S/MIME Certificate is appropriate for business use, but may also be used by home users

1. Using your web browser, visit *Comodo.com*

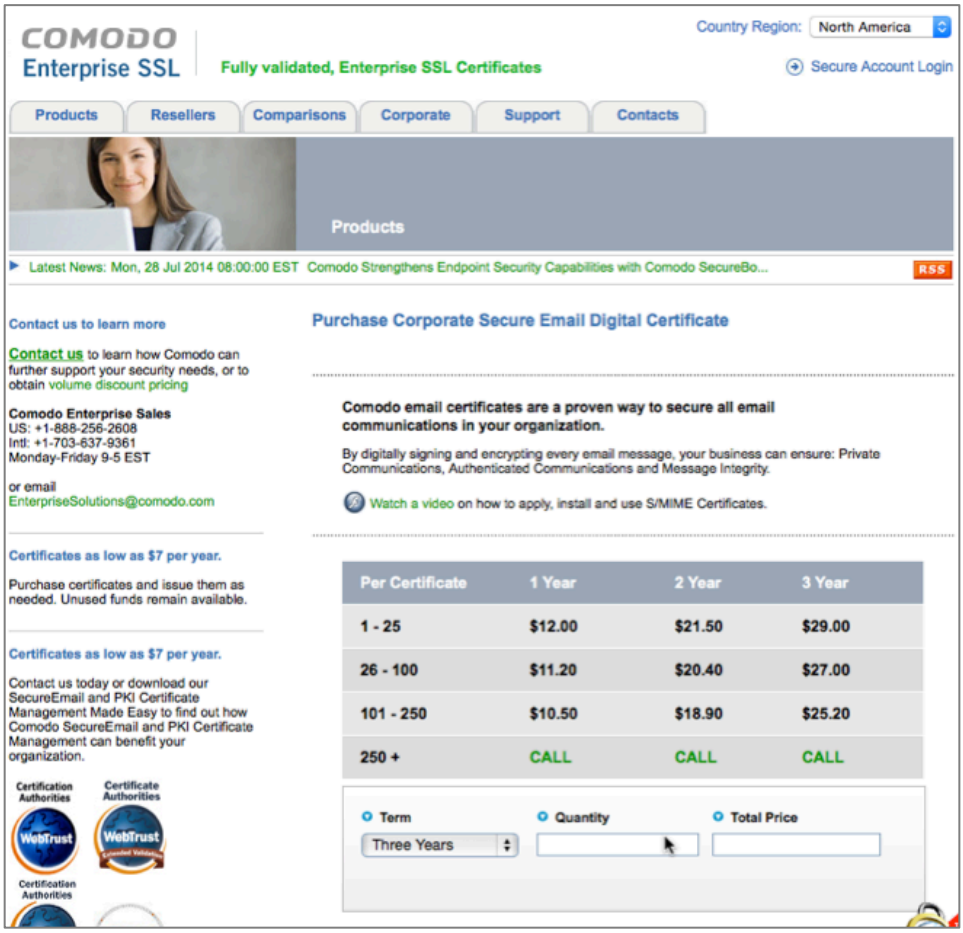
2. From the Navigation bar, select *Enterprise* > *Secure Email Certificate*.



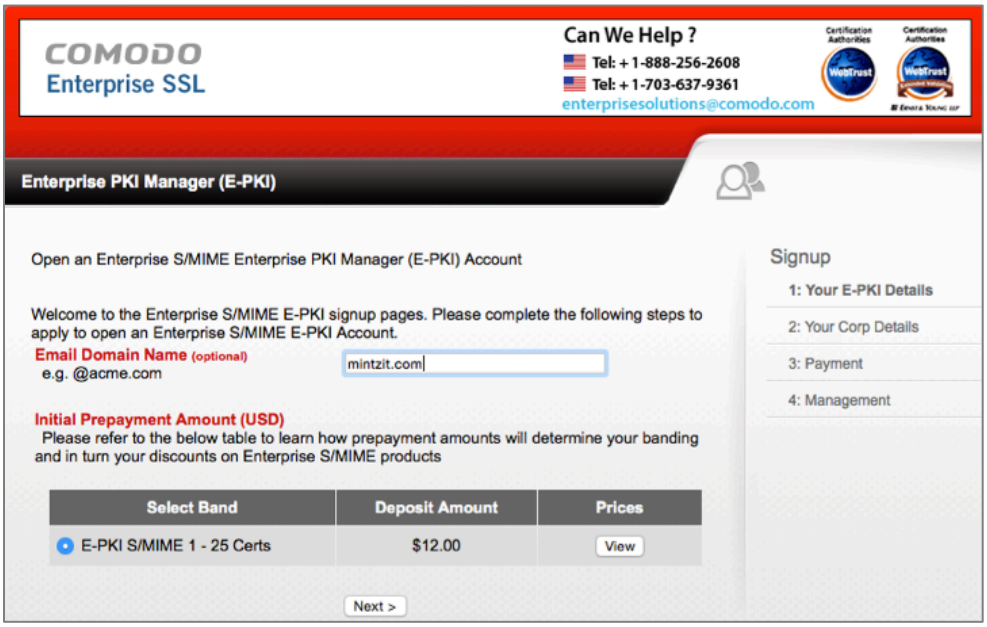
3. In the *Secure Email Certificates* page, select the *Buy Now button*.



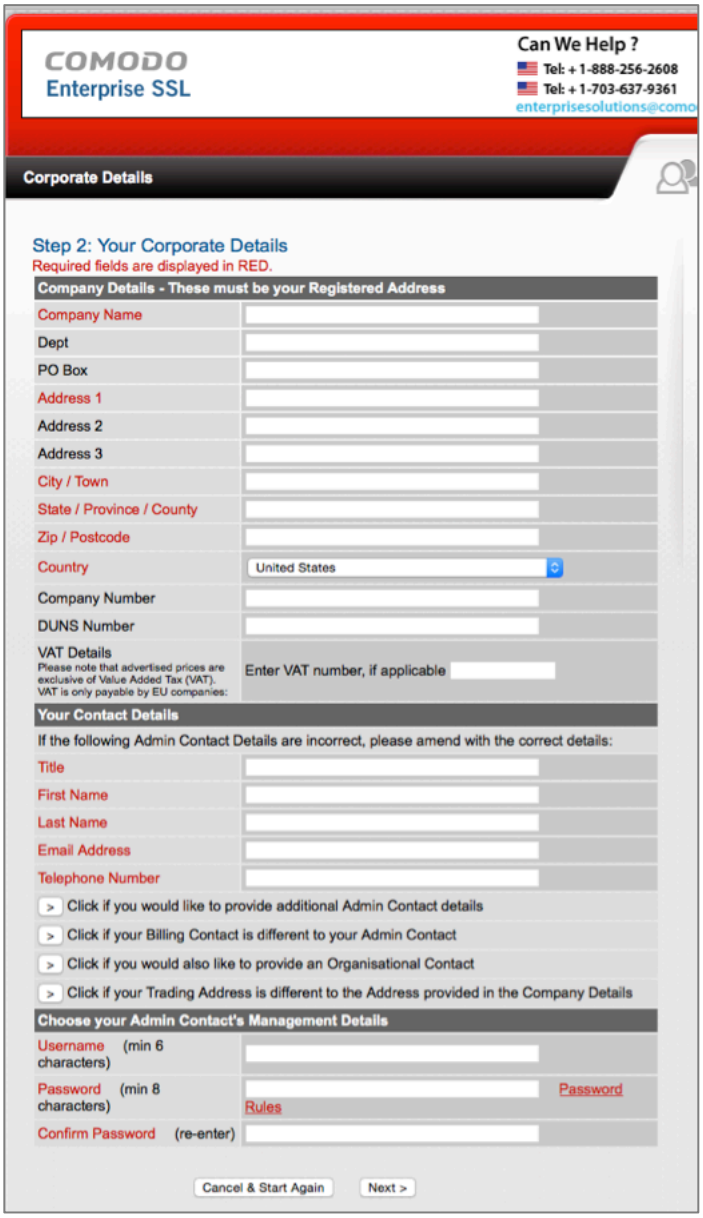
4. In the *Purchase Corporate Secure Email Digital Certificate* page, enter your desired *Term* and *Quantity*. And then select the *Next* button.



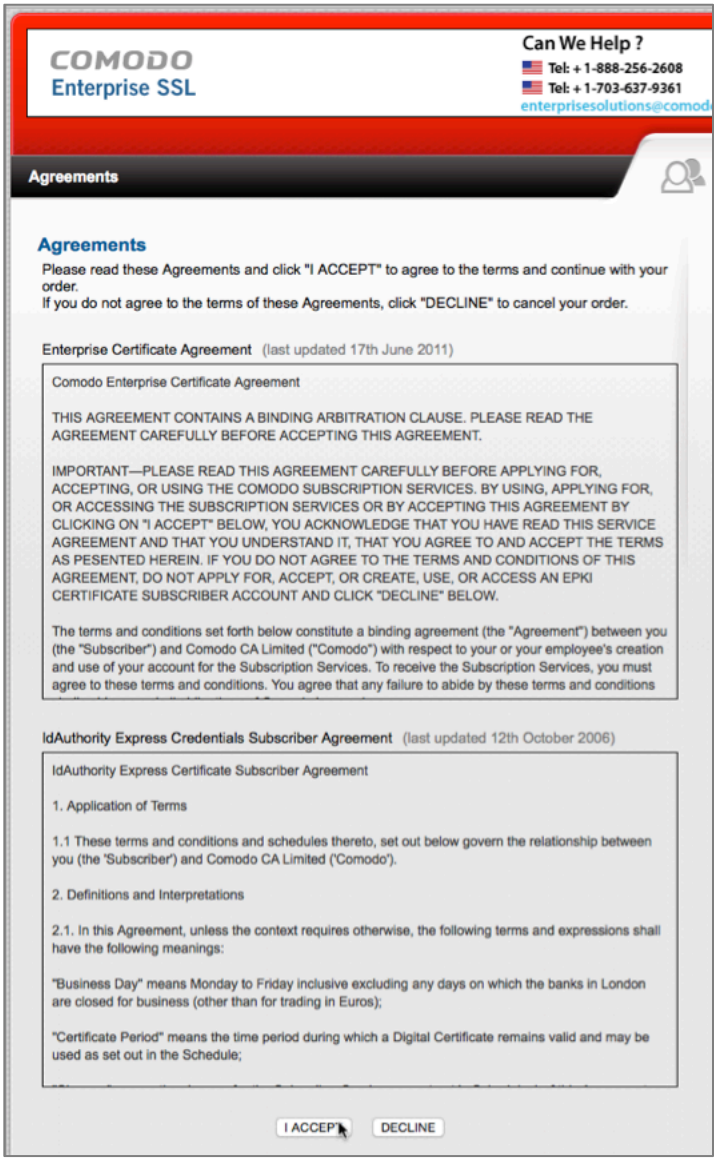
5. In the *Open an Enterprise S/MIME Enterprise PKI Manager (E-PKI) Account* window. Enter a domain name for your certificates, and then select the *Next* button.



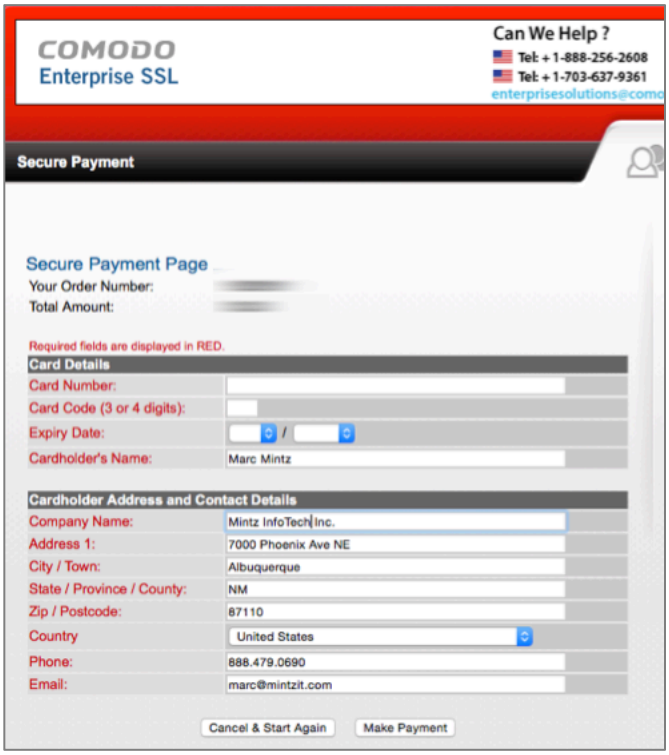
6. In the *Step 2: Your Corporate Details* page, enter all requested information, and then select the *Next* button.



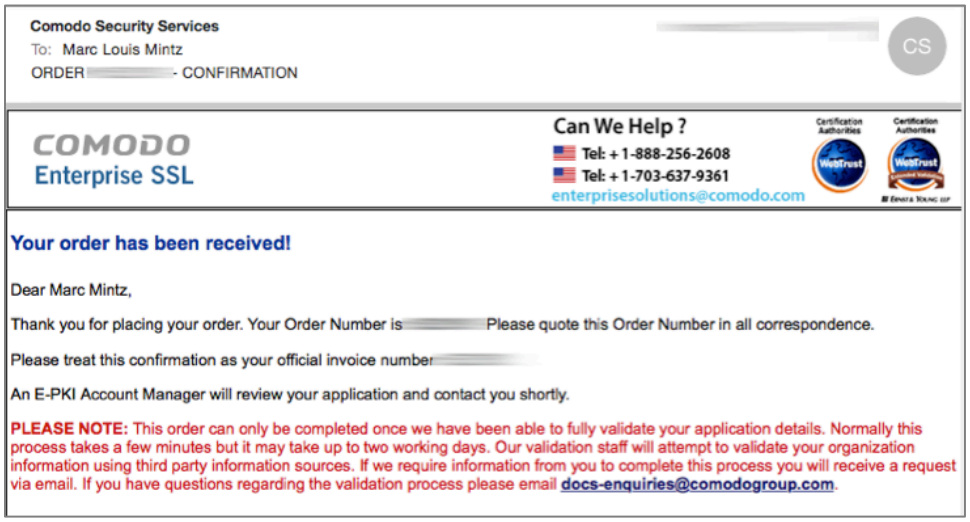
7. At the *Agreement* page, select the *I ACCEPT* button.



8. In the *Secure Payment Page,* enter your credit card information, and then select the *Make Payment* button.



9. You will receive an email from Comodo informing you of receipt of your order, and stating that you will soon be receiving another email requesting documents to validate your identity.



Comodo Security Services
To: Marc Louis Mintz
ORDER - CONFIRMATION

CS

COMODO
Enterprise SSL

Can We Help ?
Tel: + 1-888-256-2608
Tel: + 1-703-637-9361
enterprisesolutions@comodo.com

Your order has been received!

Dear Marc Mintz,

Thank you for placing your order. Your Order Number is Please quote this Order Number in all correspondence.

Please treat this confirmation as your official invoice number

An E-PKI Account Manager will review your application and contact you shortly.

PLEASE NOTE: This order can only be completed once we have been able to fully validate your application details. Normally this process takes a few minutes but it may take up to two working days. Our validation staff will attempt to validate your organization information using third party information sources. If we require information from you to complete this process you will receive a request via email. If you have questions regarding the validation process please email **docs-enquiries@comodogroup.com**.

10. Soon you will receive an email requesting the validation documents. Submit the requested documents and information.

COMODO Validation Team
To: Marc Louis Mintz
Information Required Order

CV

Thank you for your recent order.

We have begun validating your information so that we can issue your order. The following is the account information you submitted:

Company: Mintz InfoTech, Inc.
Domain Name: mintzit.com
Address 1: 7000 Phoenix Ave NE
Address 2: 310
Address 3:
City: Albuquerque
State: NM
Postal Code:87110
Country: United States of America

Although we have begun processing your order, we have been unable to complete validation for the following reasons:

In order to verify the existence of your organization we must be able to find it listed either in an official government database or a third party database such as Dunn & Bradstreet (www.dnb.com)

If the address on your account does not match the database record we may use one of the following documents for verification of the address. Please provide us with one of the following documents so we may complete your validation:

A. Articles of Incorporation (with address)
B. Government Issued Business License (with address)
C. Copy of a recent company bank statement (you may blacken out the Account Number)
D. Copy of a recent company phone bill
E. Copy of a recent major utility bill of the company (i.e. power bill, water bill, etc.) or current lease agreement for the company

*Note:Recent=dated within the last 6 months

Please fax any validation documentation to 1-866-831-5837(U.S. and Canada) or +1 801-303-9291 (Worldwide). When faxing documents, please include the attached coversheet. You may also respond by going to https://support.comodo.com, registering, and opening a ticket and attaching the documents. Please be sure to include your name, order number, domain name, e-mail address, and phone number in either your fax or support ticket.

If you need assistance, or wish to speak to a Customer Service Representative, please contact us toll-free at anytime at 1-888-266-6361 (U.S.) and +1-206-203-6361 (Worldwide).

Regards,
COMODO Validation Team

11. You will receive an email informing you that your account has been created, with a link to their *Getting Started Guide*. Although the steps outlined in this book will take you through the process, it is not a bad idea to download and read the Guide as well. Download the *Getting Started Guide*.

12. Register for Comodo technical support by clicking the link provided in the email, and then follow the on-screen instructions. This will save you significant time and headache if you ever need technical support from Comodo.

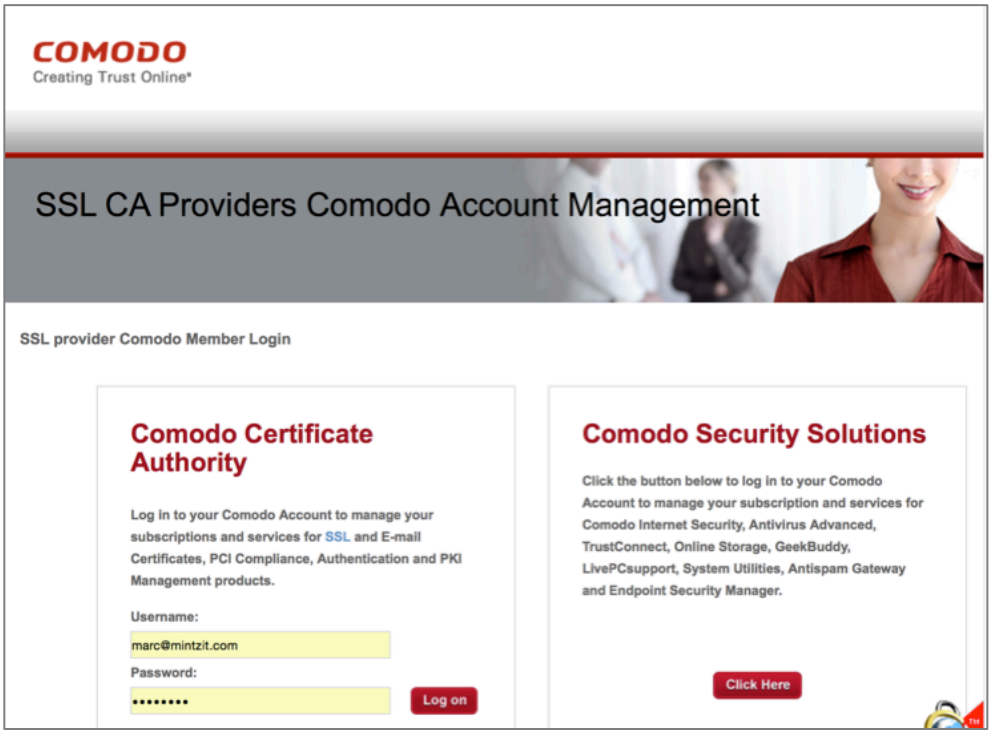
15.9.3 Assignment: Purchase a Class 3 S/MIME Certificate for Business Use

Once you have set up your Class 3 business account with Comodo, you are able to order S/MIME certificates for you and your staff at any time.

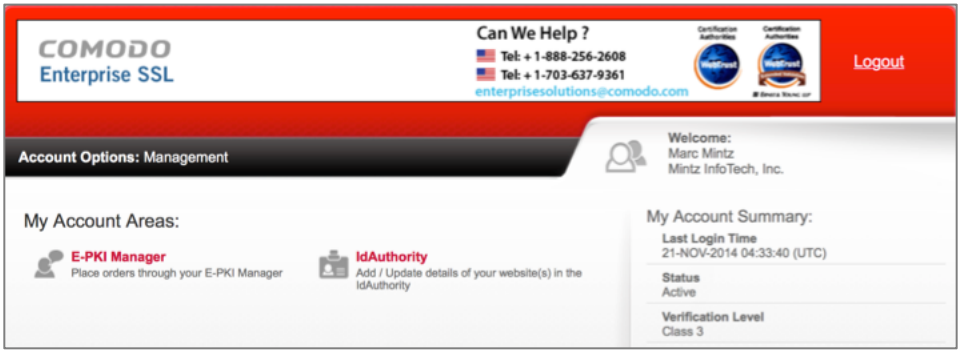
In this exercise, you purchase your first certificate.

1. From your web browser, go to the Comodo home page at *https://comodo.com*.
2. Select the *Login* link, and then login. This opens the *SSL CA Providers Comodo Account Management* page.

3. In the *Comodo Certificate Authority* area, enter your *Username* and *Password* used to start your account with Comodo, and then select the *Log on* button.

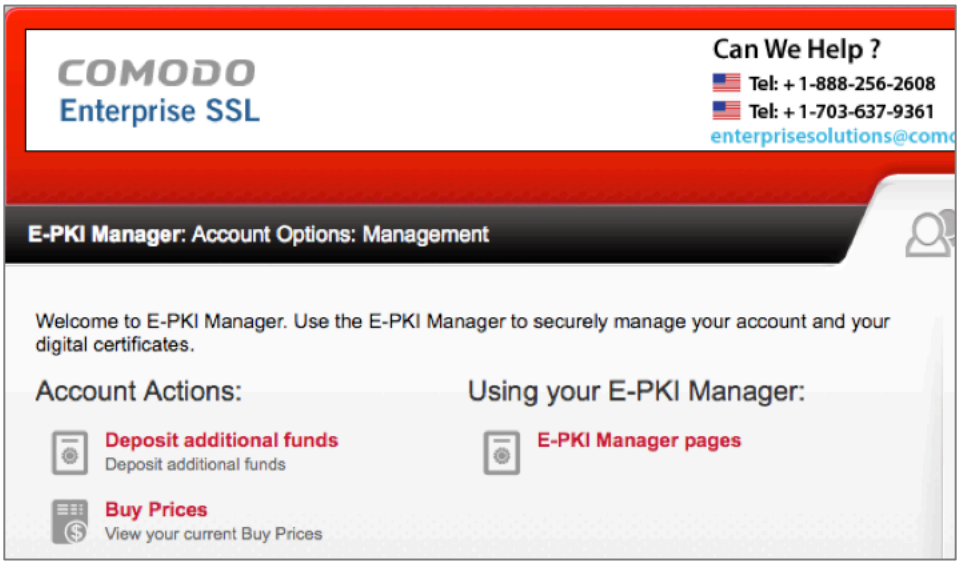


4. The *Account Options: Management* window opens. Select the *E-PKI Manager* link.



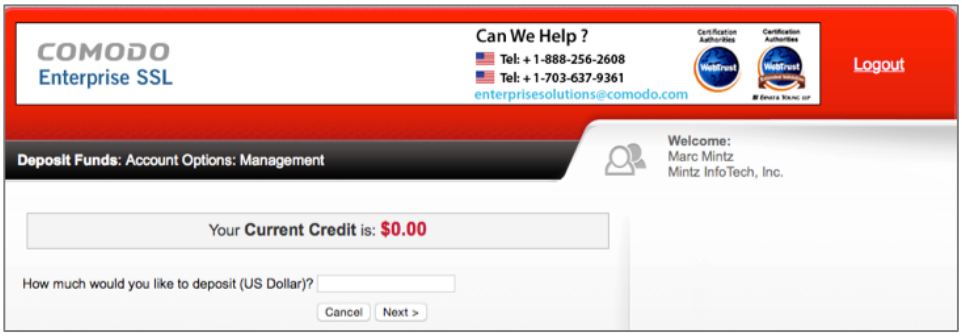
5. This will take you to the *E-PKI Manager: Account Options: Management* page. With Comodo, you pay for certificates not directly, but by pulling from

monies on deposit with Comodo. If there are inadequate funds on deposit, you will need to deposit money now. To do so, select the *Deposit additional funds* link.

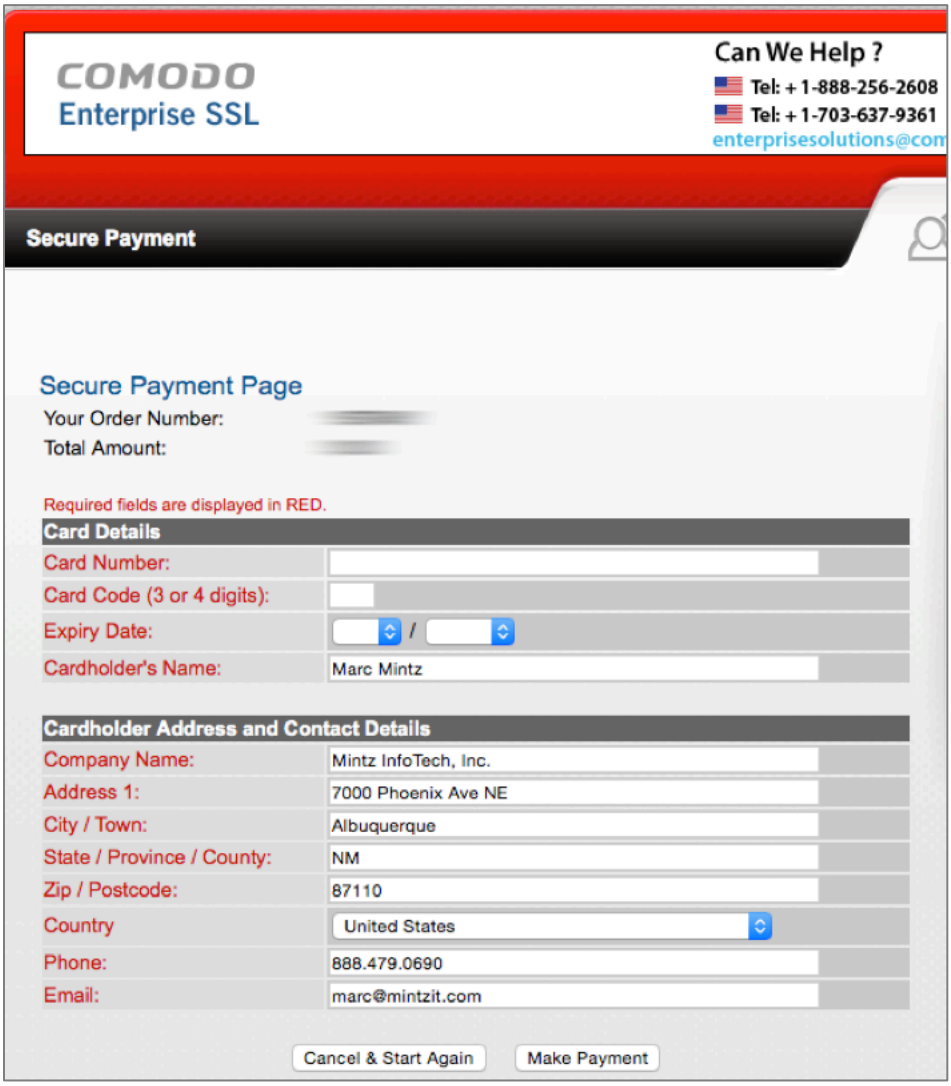


6. In the *Deposit Funds: Account Options: Management* page, enter at least the amount needed to purchase your S/MIME certificates. Rates per certificate as of this writing are.

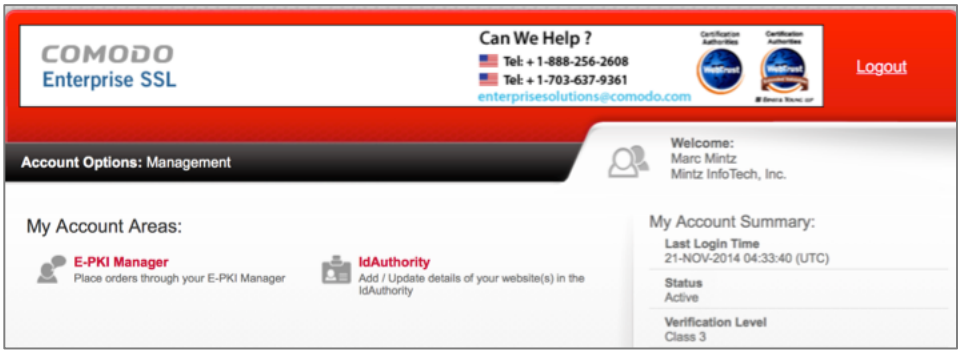
Per Certificate	1 Year	2 Year	3 Year
1 - 25	$12.00	$21.50	$29.00
26 - 100	$11.20	$20.40	$27.00
101 - 250	$10.50	$18.90	$25.20
250 +	CALL	CALL	CALL


COMODO
Enterprise SSL
Can We Help ?
Tel: + 1-888-256-2608
Tel: + 1-703-637-9361
enterprisesolutions@comodo.com
Logout
Deposit Funds: Account Options: Management
Welcome:
Marc Mintz
Mintz InfoTech, Inc.
Your Current Credit is: $0.00
How much would you like to deposit (US Dollar)?
Cancel
Next >

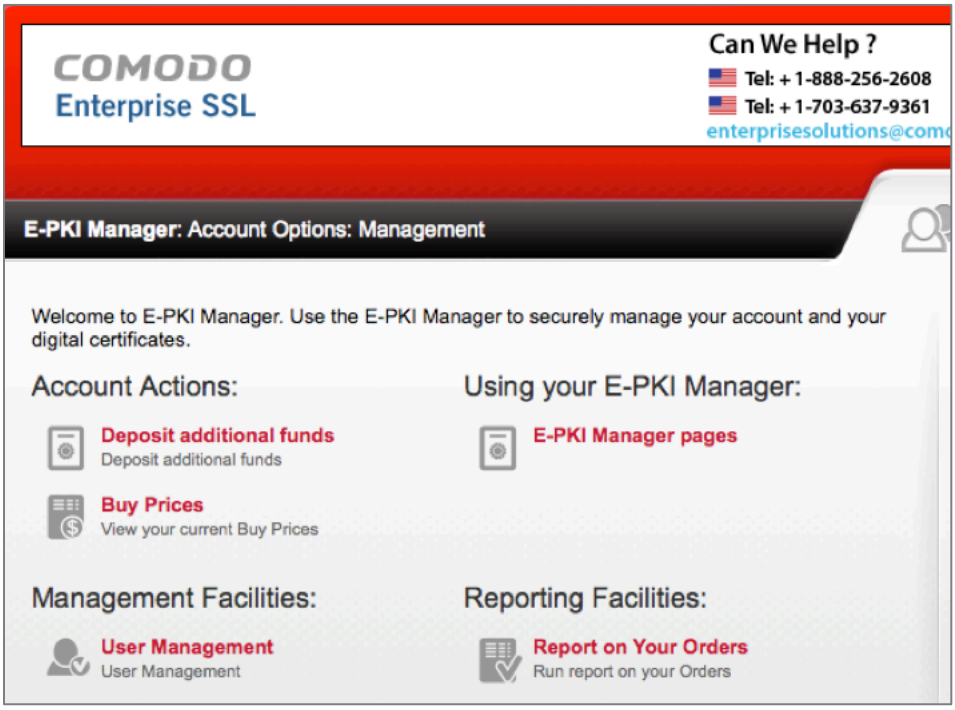
7. In the *Secure Payment* page enter your credit card information, and then select the *Make Payment* button.



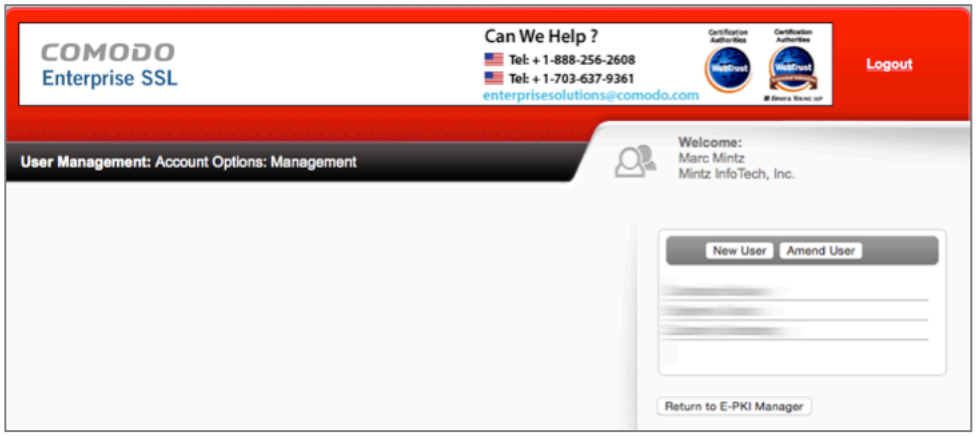
8. Return to the *Account Options: Management* page, and then select the *E-PKI Manager* link.



9. In the E-*PKI Manager: Account Options: Management* page, select the *User Management* link.



10. In the *User Management: Account Options: Management* page, select the *New User* button.



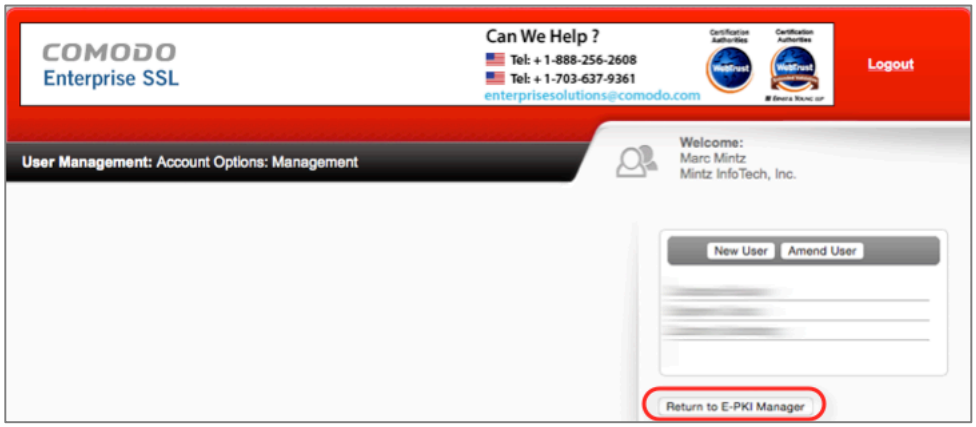
11. In the *New User* window, enter all information for your new user, and then select the *Save Changes* button.

User Details	
Title	
First Name	
Surname	
Email Address	
Telephone No.	
Fax No.	
Is Active?	☑
Login Name	
Password	
Password Confirmation	
Is Api User? Enabling this will disable the users Order Management Link.	☐
User Address	
Department	
PO Box	
Street Address 1	7000 Phoenix Ave NE
Street Address 2	310
Street Address 3	
City	Albuquerque
State / Province / County	NM
Postal / Zip Code	87110
Country	United States

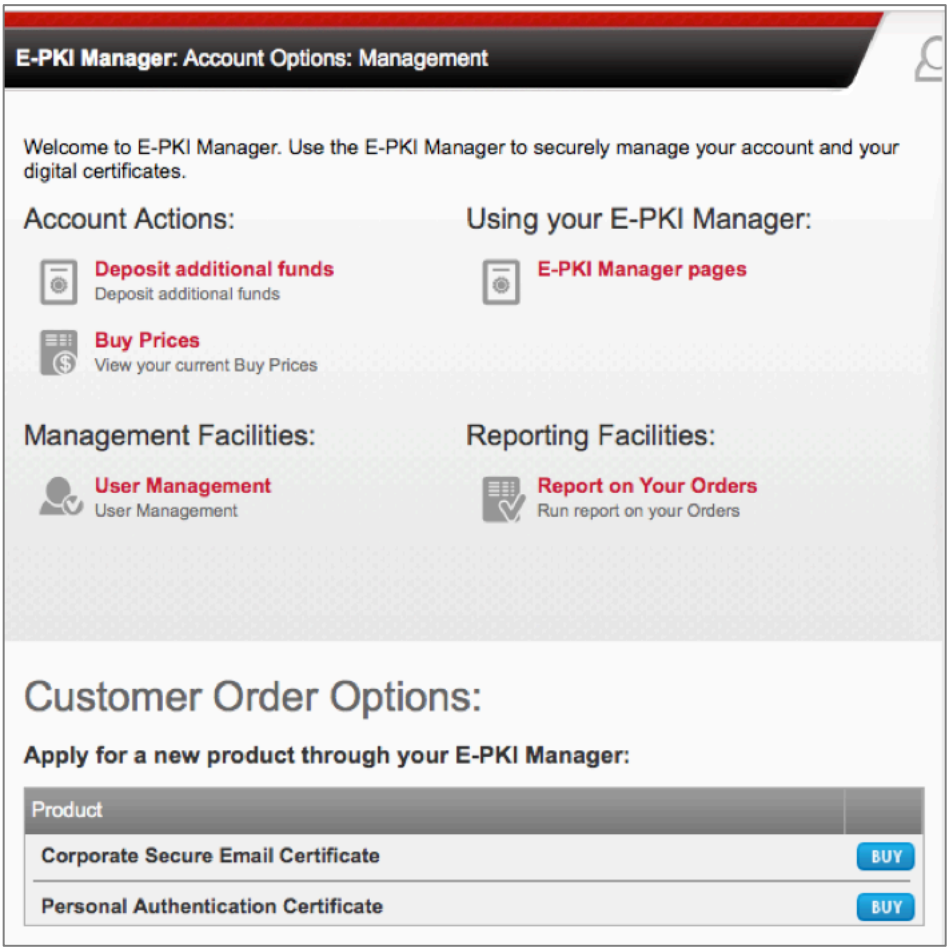
Cancel Save Changes

12. Repeat steps 7-10 to enable each user/email account to have an S/MIME certificate.

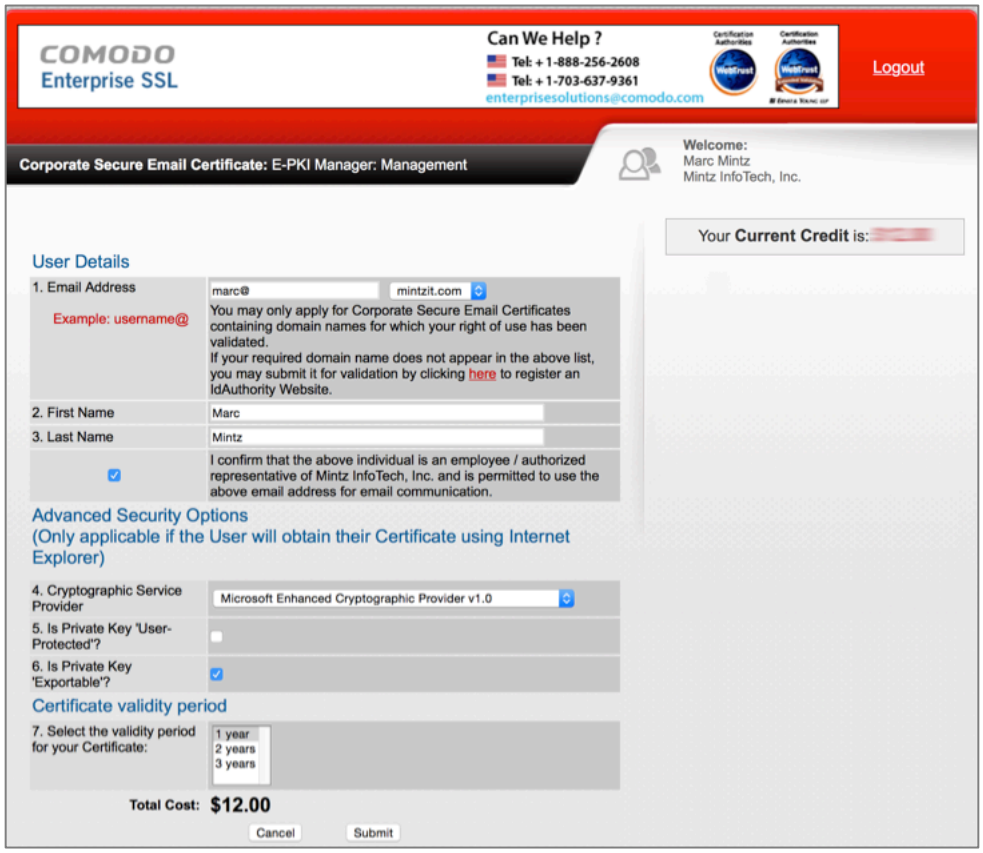
13. When all certificates have been requested, return to the *User Management: Account Options: Management* window, and then select the *Return to E-PKI Manager* button.



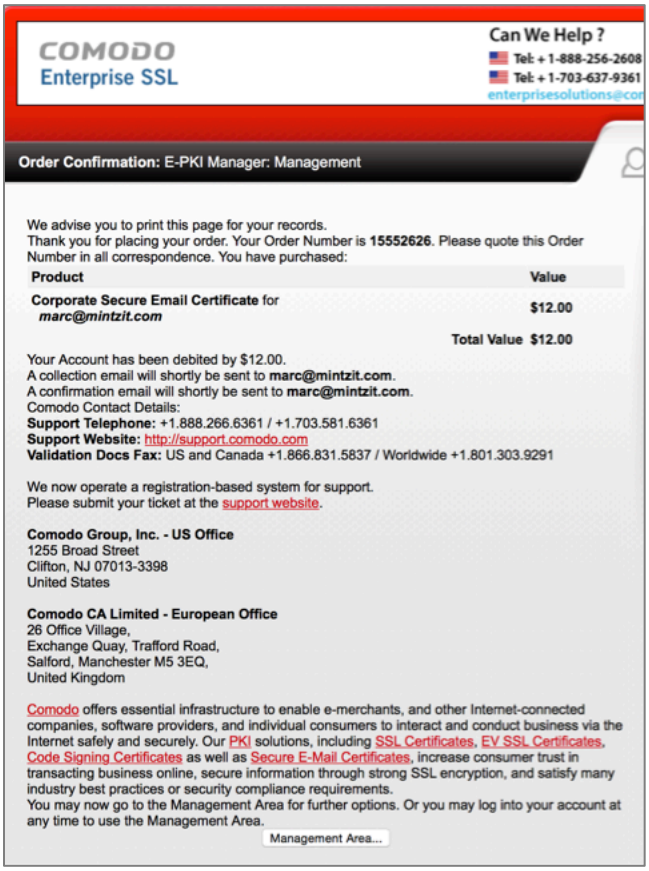
14. In the E-*PKI Manager: Account Options: Management* page, scroll to the bottom, and then select the *Corporate Secure Email Certificate Buy* button.



15. In the *Corporate Secure Email Certificate: E-PKI Manager: Management* page, complete the information for the user/email address you wish to assign an S/MIME certificate, and then select the *Submit* button.



16. At the *Order Confirmation: E-PKI Manager: Management* page, print your receipt, and then select the *Management Area…* button.



COMODO
Enterprise SSL

Can We Help ?
Tel: + 1-888-256-2608
Tel: + 1-703-637-9361
enterprisesolutions@co

Order Confirmation: E-PKI Manager: Management

We advise you to print this page for your records.
Thank you for placing your order. Your Order Number is **15552626**. Please quote this Order Number in all correspondence. You have purchased:

Product	Value
Corporate Secure Email Certificate for ***marc@mintzit.com***	**$12.00**
Total Value	**$12.00**

Your Account has been debited by $12.00.
A collection email will shortly be sent to **marc@mintzit.com**.
A confirmation email will shortly be sent to **marc@mintzit.com**.
Comodo Contact Details:
Support Telephone: +1.888.266.6361 / +1.703.581.6361
Support Website: http://support.comodo.com
Validation Docs Fax: US and Canada +1.866.831.5837 / Worldwide +1.801.303.9291

We now operate a registration-based system for support.
Please submit your ticket at the support website.

Comodo Group, Inc. - US Office
1255 Broad Street
Clifton, NJ 07013-3398
United States

Comodo CA Limited - European Office
26 Office Village,
Exchange Quay, Trafford Road,
Salford, Manchester M5 3EQ,
United Kingdom

Comodo offers essential infrastructure to enable e-merchants, and other Internet-connected companies, software providers, and individual consumers to interact and conduct business via the Internet safely and securely. Our PKI solutions, including SSL Certificates, EV SSL Certificates, Code Signing Certificates as well as Secure E-Mail Certificates, increase consumer trust in transacting business online, secure information through strong SSL encryption, and satisfy many industry best practices or security compliance requirements.
You may now go to the Management Area for further options. Or you may log into your account at any time to use the Management Area.

Management Area...

17. Repeat steps 13-15 for each user/email account to be assigned an S/MIME certificate.

15.9.4 Assignment: Install a Business S/MIME Certificate

In this assignment, you download and install a Class 3 S/MIME Certificate.

1. At the user's computer, check email for a message from Comodo, select and copy the *Your Certificate Password*, and then select the *Begin Corporate Secure Email Certificate Application* button.

Comodo Security Services

To: Marc Louis Mintz

Collecting your Corporate Secure Email Certificate

CS

Dear Marc Mintz,

Your Corporate Secure Email Certificate has now been issued and is ready to be collected.

Please click the button below to begin collection.

Begin Corporate Secure Email Certificate Collection

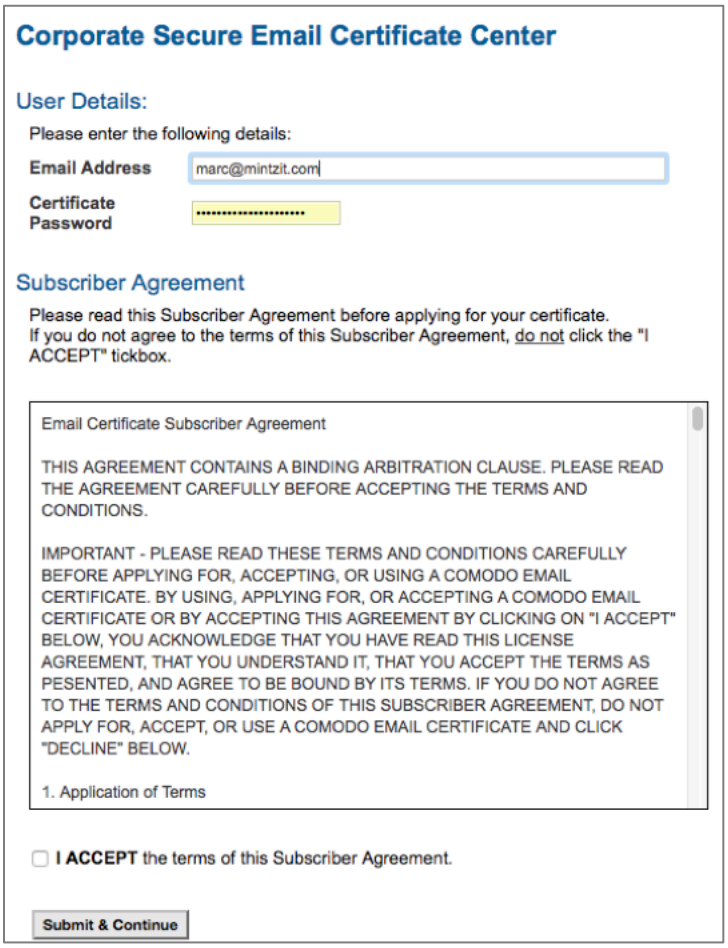
If the above button does not work, please navigate to
https://secure.comodo.com/products/CorporateSecureEmail.
Your Certificate Password is:

This email message was sent on behalf of your System Administrator. Should you have any questions regarding your Corporate Secure Email Certificate application, please contact your System Administrator.

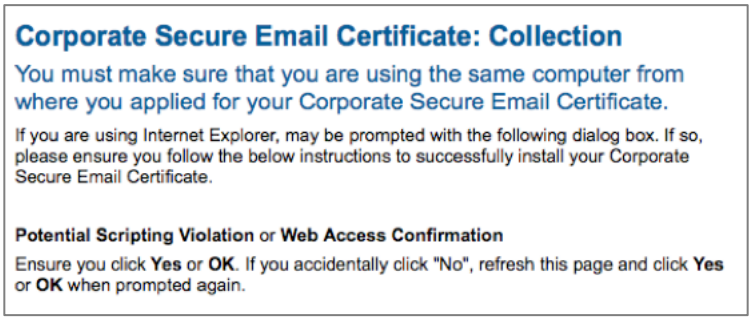
Kind Regards,

Comodo Security Services
noreply_support@comodo.com

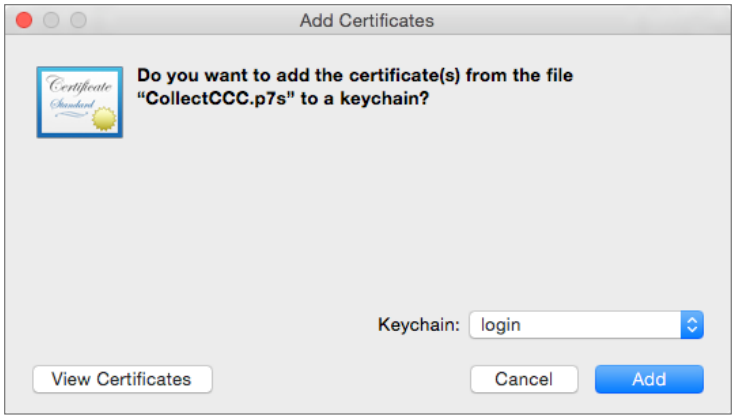
2. In the *Corporate Secure Email Certificate Center*:
   - Enter the **exact same email address** as used during the certificate creation.
   - Paste in the *Certificate Password* that was included in the Comodo email sent to the email address.
   - Enable the *I Accept* checkbox.
   - Select the *Submit & Continue* button.



3. The *Corporate Secure Email Certificate: Collection* page will open; your certificate will be generated and begin to download.



4. When the certificate has been generated, it will start downloading. When downloaded, you will find it in your *Downloads* folder named something like *CollectCCC.p7s*.
5. Open your *Downloads* folder and locate the *CollectCCC.p7s* file.
6. To install your S/MIME certificate into the *Keychain Access.app*, double-click on the *CollectCCC.p7s* file.
7. The *Add Certificates* window opens. Select *Keychain: login*, and then select the *Add* button.



8. *Quit* Keychain Access.
9. Quit the Mail.app.

10. *Open* the *Mail.app*. This forces the Mail application to search for new certificates.
11. If you use multiple computers, place a copy of your *CollectCCC.p7s* file on each of your computers, and repeat steps 6-10.

Your S/MIME certificate, which includes both your *Public Key* (used by others to encrypt email to you) and *Private Key* (used by you to decrypt email received by you) is now installed.

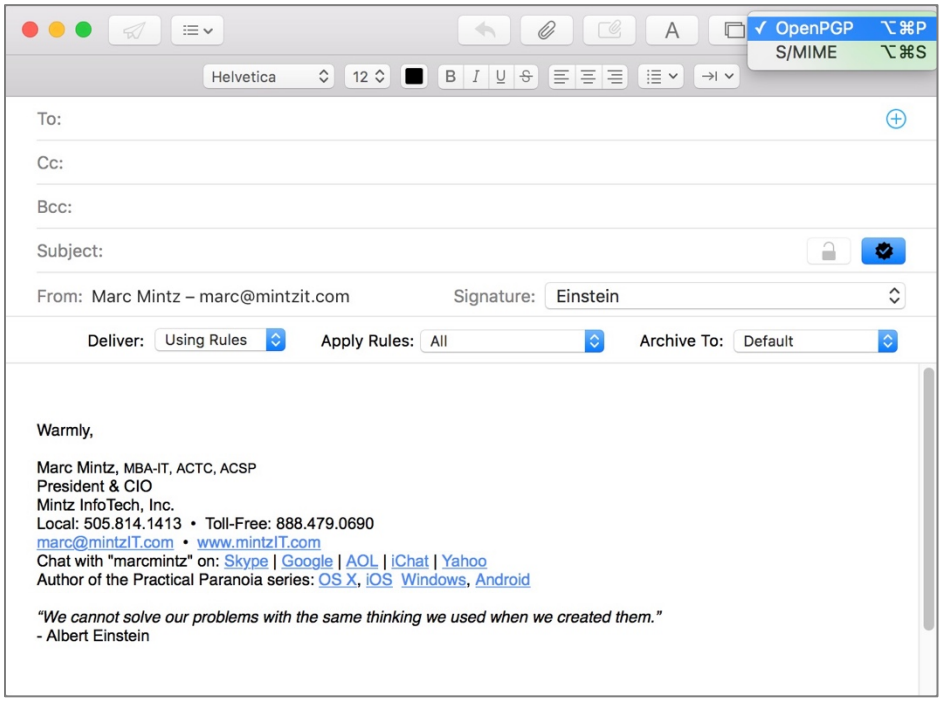
15.9.5 Assignment: Exchange Public Keys with Others

Before you can send or receive encrypted email with others, you need to exchange Public Keys with each other. This is as simple as sending a signed email to each other. To start, you send a signed email to a friend. This gives this recipient your Public Key, as well as instructions for the recipient to set up S/MIME on their own system.

In this assignment, you send a friend your public key.

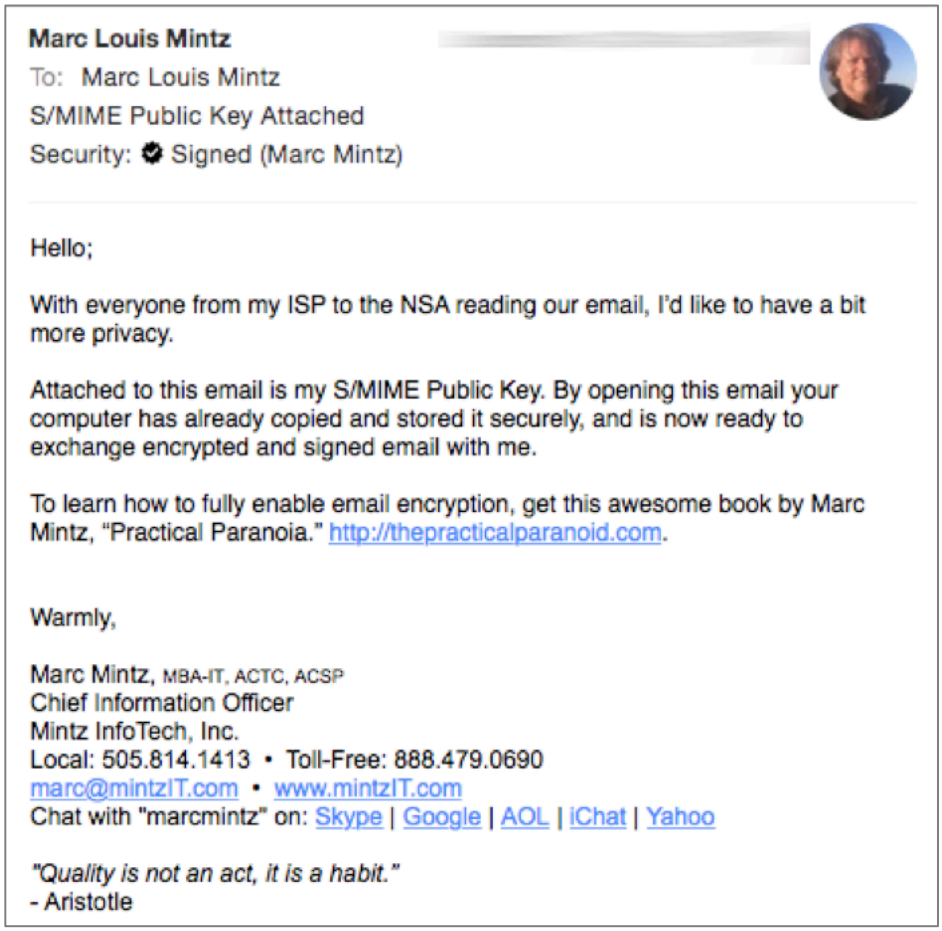
1. From a computer that now has your newly acquired email certificates, *Open* the *Mail.app*. This process forces *Mail.app* to look for new certificates.
2. Select the *File* menu > *New Message*.
3. From the *From:* pop-up menu, select the email account with the new certificates. (If you have only one email account, the *From* field typically does not appear.)
4. At the bottom right of the header area, note the two new icons–an encryption lock and signed check. If you have performed the earlier GPG assignments, these are the same and are shared between the two systems. The lock becomes available when you have the Public Key of the recipient, allowing for encryption. The check is available for anyone once you have your certificate. It will verify that the sender (you) are who you say you are.
5. If you have performed the earlier GPG assignments, the drop-down menu at the top right corner allows you to select either GPG or S/MIME as your

encryption protocol. If you have not performed the earlier GPG assignments, this menu is absent.



6. Address your email to an associate with whom you would like to be able to exchange encrypted email. Feel free to address the email to me at *marc@mintzit.com*.
7. If you have installed both PGP and S/MIME, ensure the *S/MIME* is the selected protocol, and that the *S/MIME signed check* is enabled (it should be by default.) This will ensure your Public Key is sent to your designated recipient.
8. In the Subject line, be clear about the intent of the email by noting something like: *S/MIME Public Key Attached.*
9. In the body area, you may want to include instructions for how to acquire an email certificate–or better yet–point to this book at its website *http://thepracticalparanoid.com*.

10. When the recipient receives and opens the email, that recipient now has your Public Key and can determine that the email truly did come from you due to your signing the email with your certificate.



Marc Louis Mintz
To: Marc Louis Mintz
S/MIME Public Key Attached
Security: Signed (Marc Mintz)

Hello;

With everyone from my ISP to the NSA reading our email, I'd like to have a bit more privacy.

Attached to this email is my S/MIME Public Key. By opening this email your computer has already copied and stored it securely, and is now ready to exchange encrypted and signed email with me.

To learn how to fully enable email encryption, get this awesome book by Marc Mintz, "Practical Paranoia." http://thepracticalparanoid.com.

Warmly,

Marc Mintz, MBA-IT, ACTC, ACSP
Chief Information Officer
Mintz InfoTech, Inc.
Local: 505.814.1413 • Toll-Free: 888.479.0690
marc@mintzIT.com • www.mintzIT.com
Chat with "marcmintz" on: Skype | Google | AOL | iChat | Yahoo

"Quality is not an act, it is a habit."
- Aristotle

11. The recipient then needs to repeat the steps in this and the previous assignments to acquire an email certificate, and then send a signed email to you. Once this is done, the two of you may exchange encrypted email.

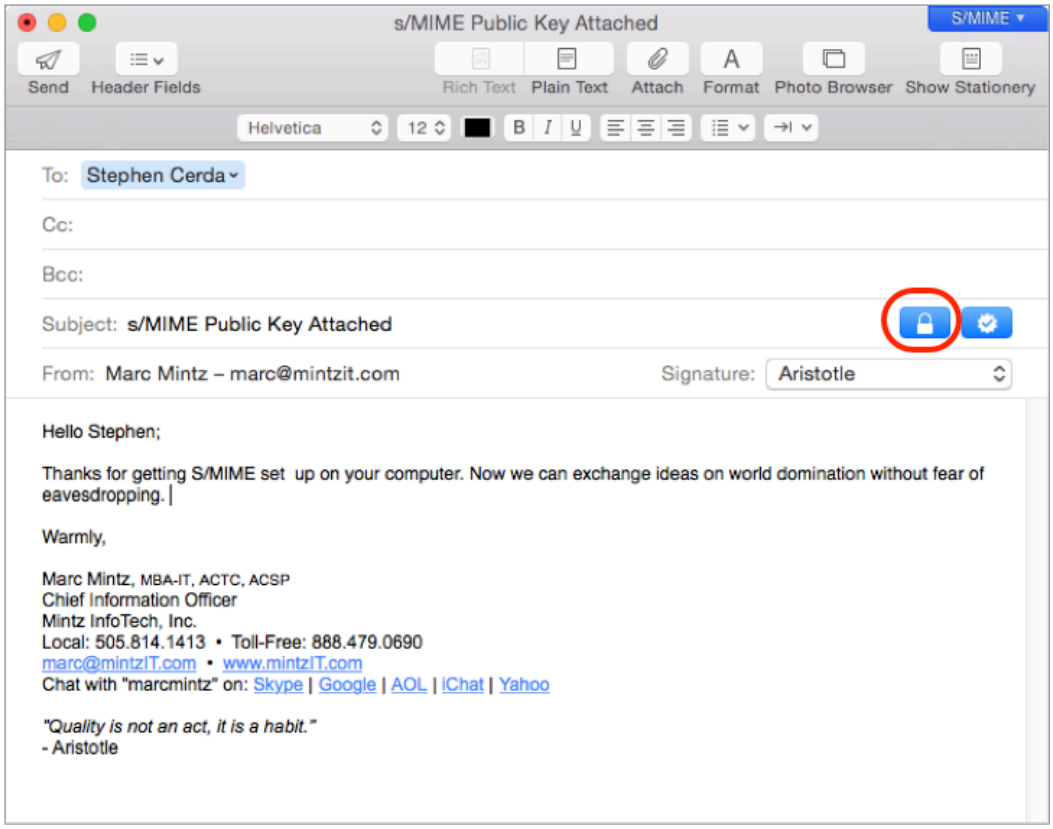
15.9.6 Assignment: Send S/MIME Encrypted Email

To exchange encrypted email using S/MIME, the previous assignments must be completed by yourself and at least one other person with whom you wish to have secure communication. Once done, each has an email certificate, a private key, and a public key that is embedded in the other's computer.

In this assignment, you send your first S/MIME encrypted email.

1. Open your *Mail.app*.
2. Create a new message, addressed to someone with whom you share public keys.
3. If you have also installed GPG, set the *GPG-S/MIME* menu in the top right corner of the message to *S/MIME*.

4. Enable the *encrypted* lock icon in the bottom right area of the message header.



5. Send the message. When received by the recipient, the message is instantly and automatically decrypted, and the recipient gets a notice that the message is encrypted as well as signed.

Congratulations! You are now able to send and receive securely encrypted email using the S/MIME protocol.

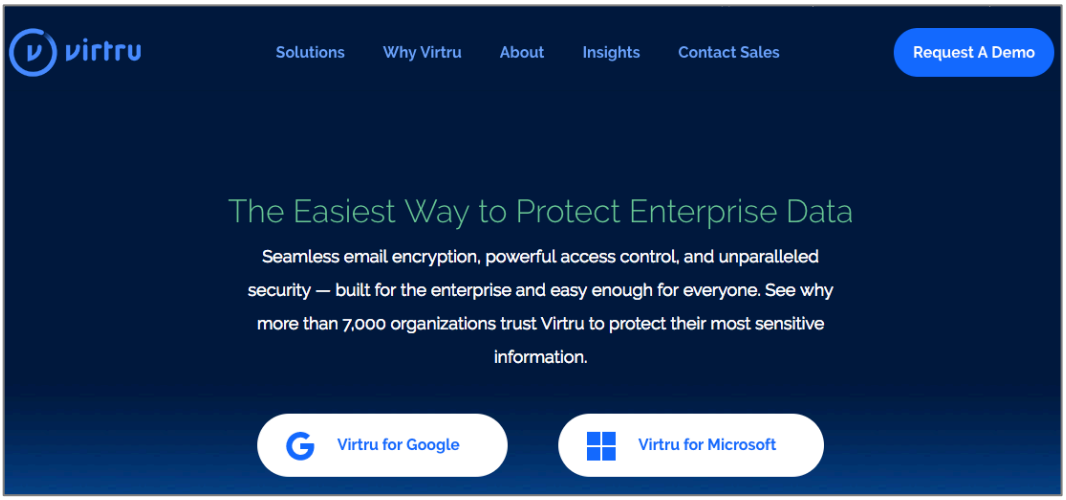
15.10 Virtru Email Encryption

Although PGP/GPG and S/MIME are excellent, highly secure options, they do need some expertise and time to install and configure, and require that both the sender and recipient have the same protocol installed.

For many businesses, that is simply a deal breaker.

If you or your organization use Gmail, Google G-Suite (previously Google Apps for Work) or Microsoft Outlook (currently Windows only), another excellent, highly secure option is *Virtru*[15]. Virtru only requires that the sender have a Virtru account, the recipient still can read the encrypted email, as well as any attached encrypted documents.

Virtru offers free accounts for personal use, and for-fee business accounts. The free account works with Gmail and G-Suite mail through the web interface. The business accounts work with Gmail, Google mail, and Microsoft Outlook.



[15] *https://virtru.com/*

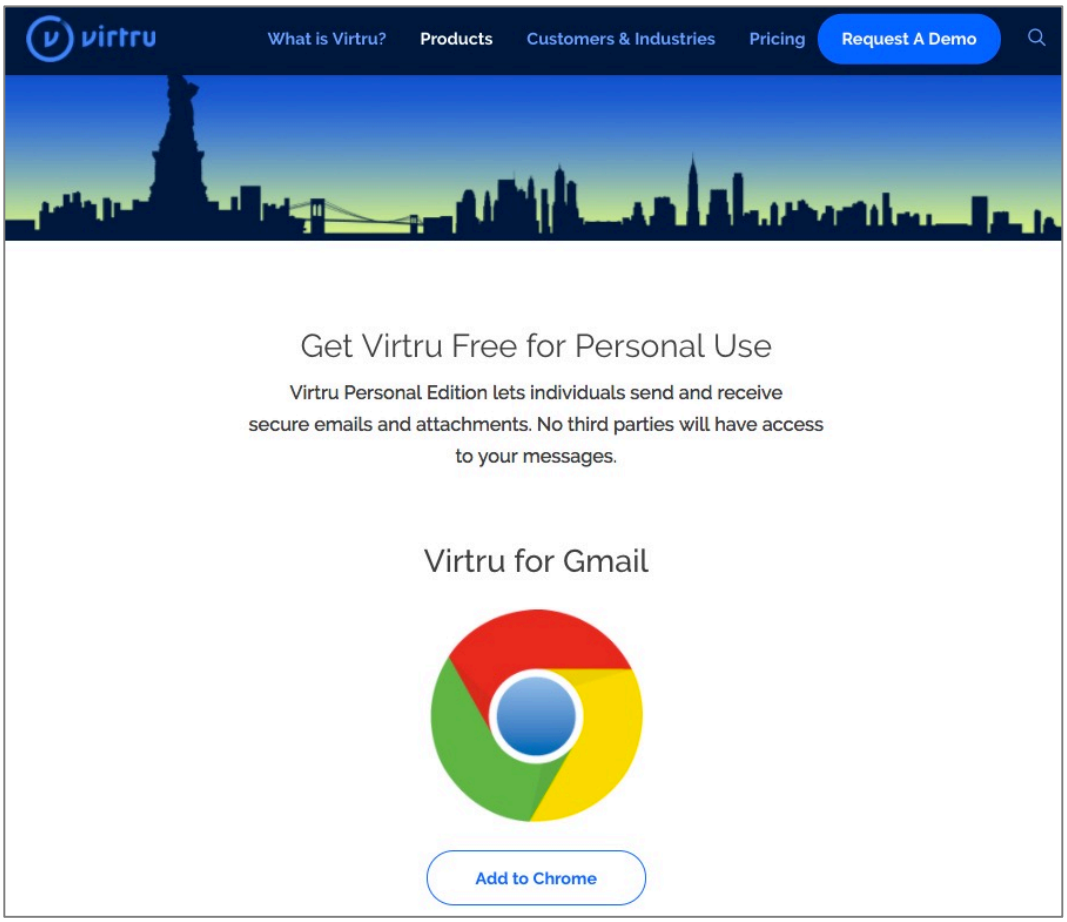
15.10.1 Assignment: Create a Free Virtru for Gmail Account

A free Virtru account is perfect for personal use with your existing Gmail account. You will immediately be able to send fully encrypted email and attachments to friends and family, without a need for them to do any additional work!

In this assignment, you create a free Virtru account.

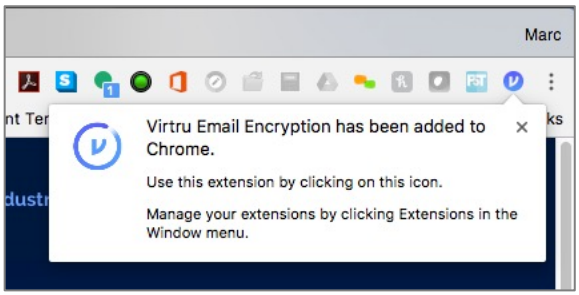
- Prerequisite: Must have a Gmail or Google G-Suite account, and use Google web mail.

1. Open Google Chrome, and visit *https://www.virtru.com/secure-email/*.



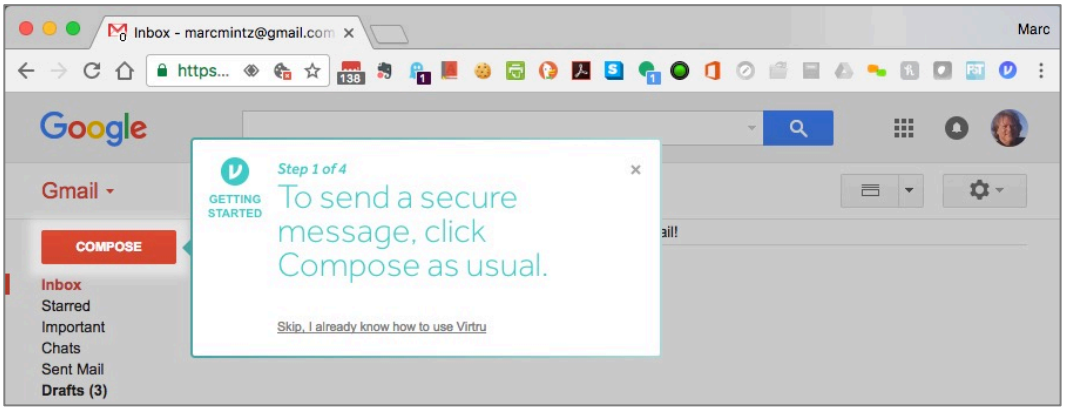
2. Click the *Add to Chrome* button.
3. The *Add "Virtru Email Encryption"* window appears. Click the *Add extension* button.

4. A pop-up will appear, showing the new Virtru Chrome icon.

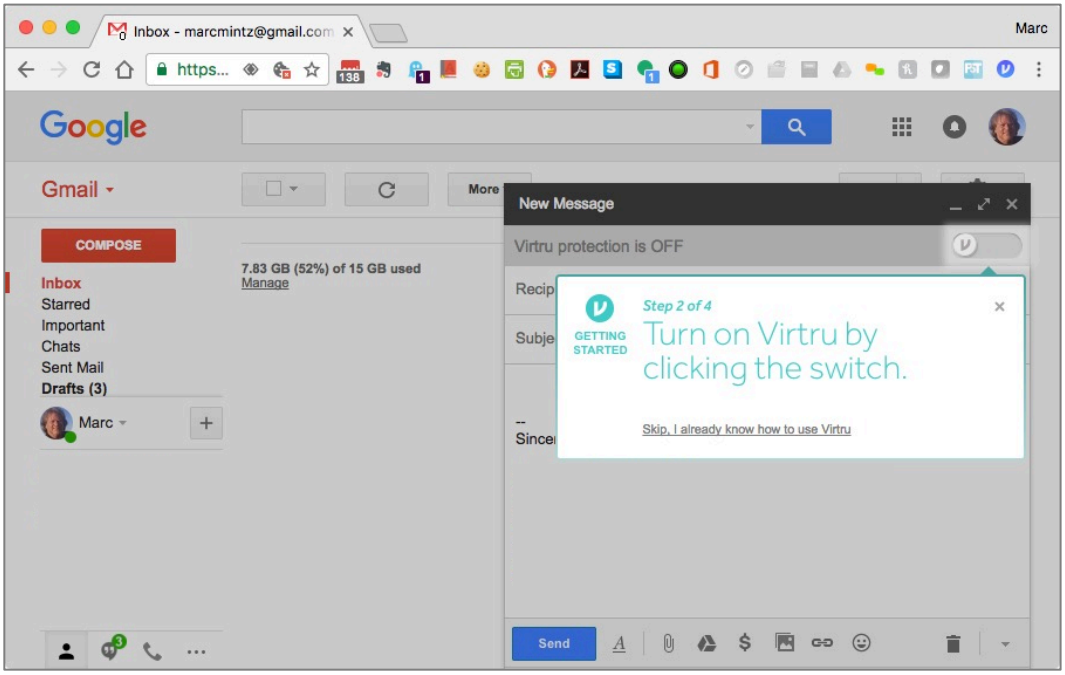


5. In Chrome, go to your Gmail account at *https://mail.google.com,* and then sign in.

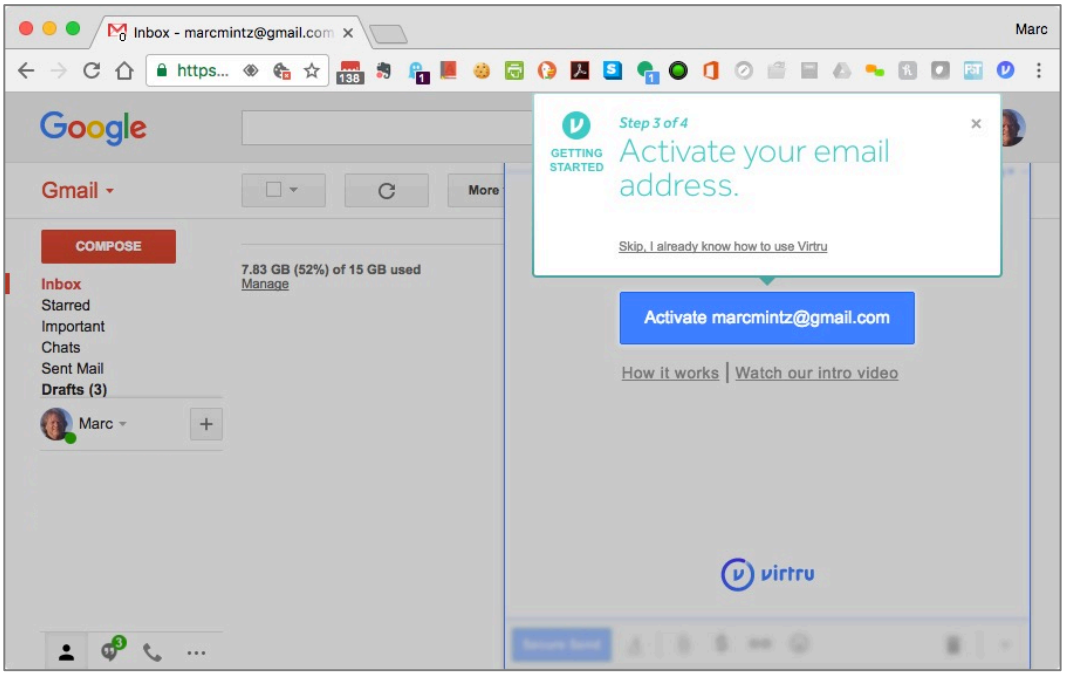
6. You will see a *Step 1 of 4* alert. Following the instructions of the alert, click the *Compose* button.



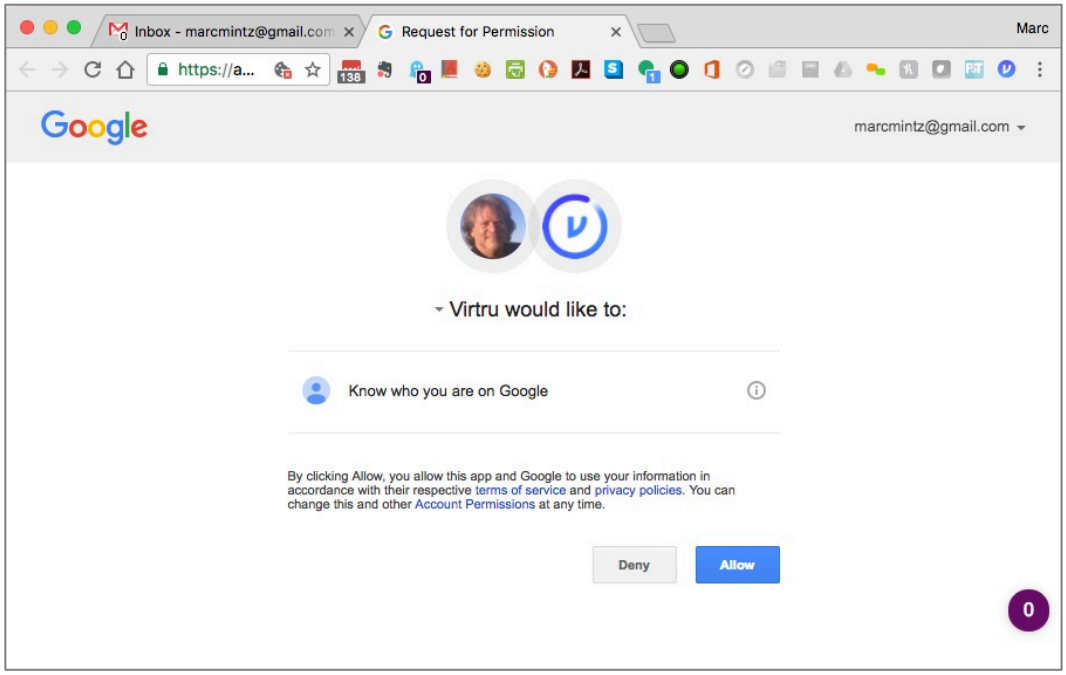
7. The *Step 2 of 4* alert appears. Following the instructions, click the Virtru switch to enable Virtru encryption.



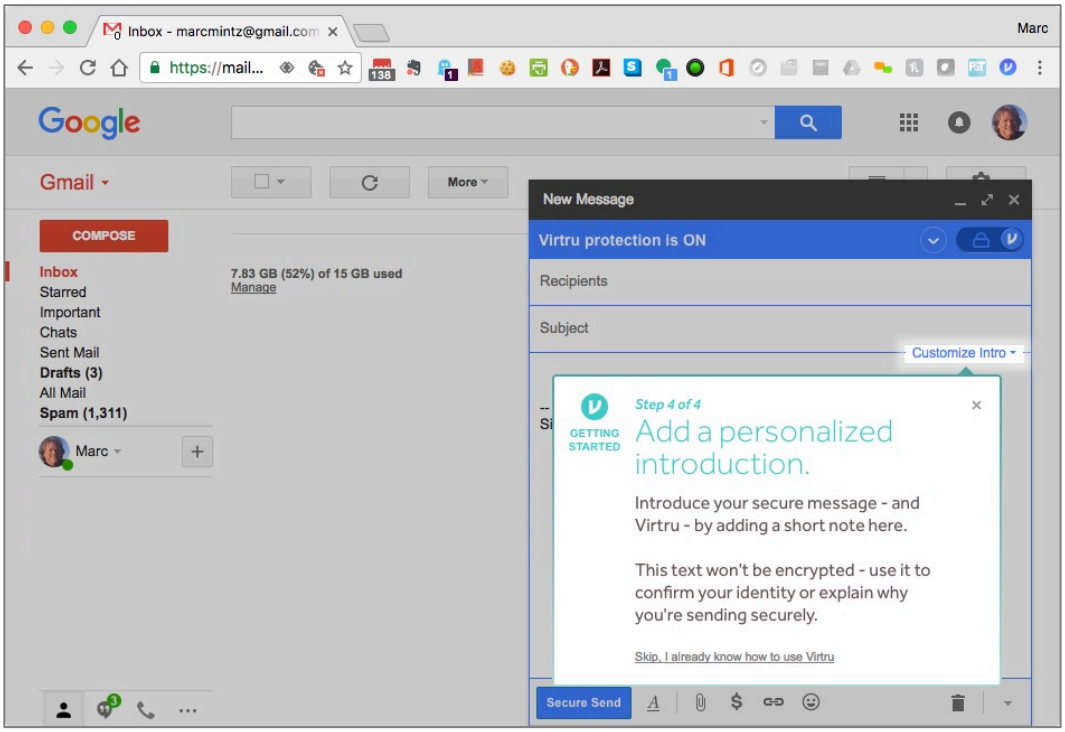
8. The *Step 3 of 4* alert appears. Following the instructions, click the *Activate <your email address>* button.



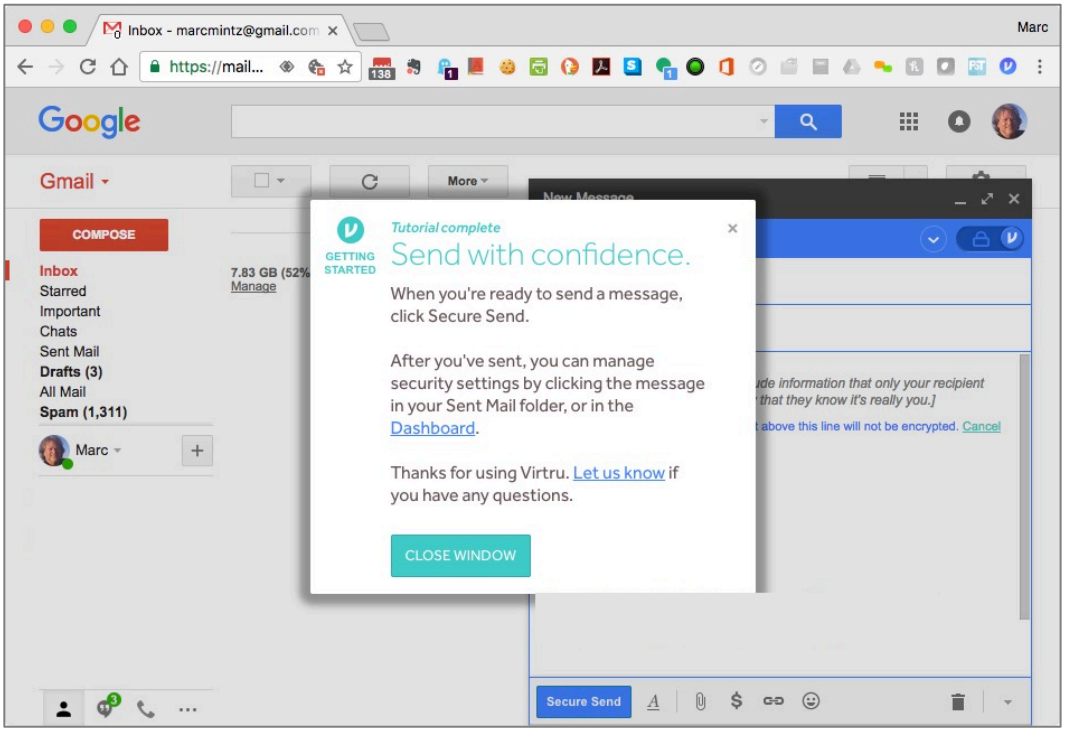
9. In the *Virtru would like to:* window, click the *Allow* button.



10. The *Step 4 of 4* alert appears. As you aren't really sending an email yet, click the *Customize Intro* button to move to the last alert.



11. The *Send with confidence* alert appears. Click the *Close Window* button.



You are now read to send your first Virtru encrypted email.

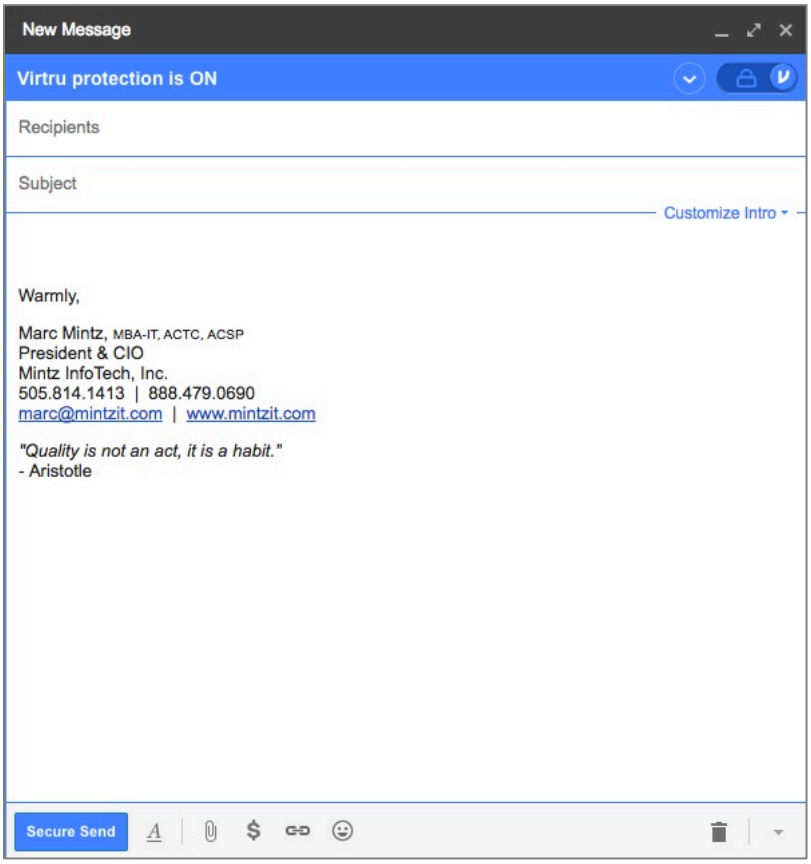
15.10.2 Assignment: Send Encrypted Gmail With Virtru

In this assignment, you send your first encrypted Gmail or G-Suite email with Virtru.

- Prerequisite: A Gmail or G-suite account.

1. Open Google Chrome to *http://mail.google.com*.
2. Click the *Compose* button to create a new email.

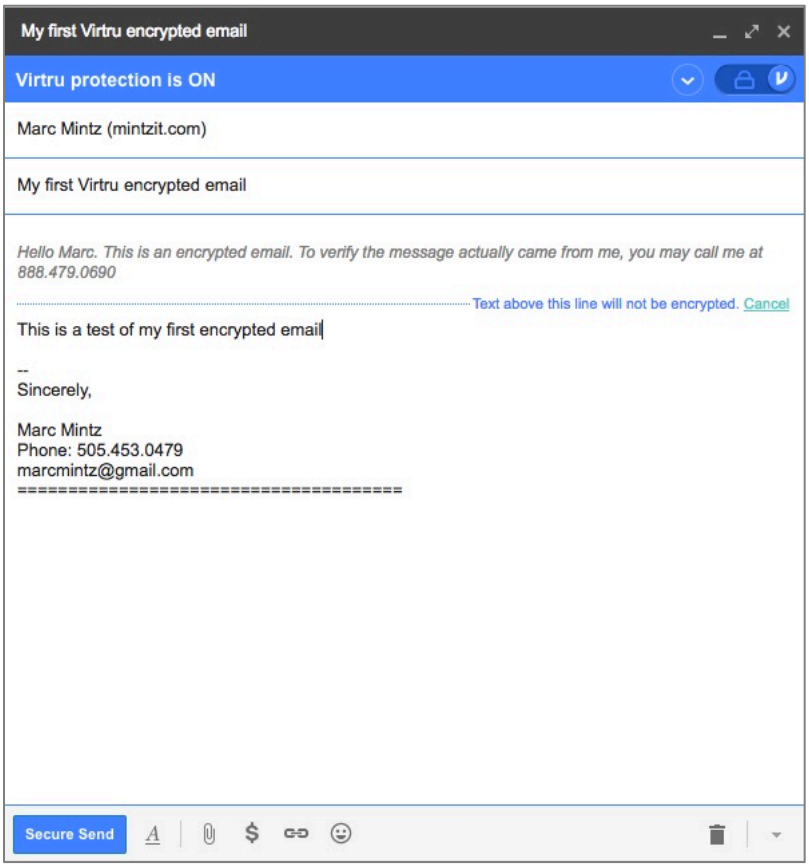
3. A *New Message* window appears. Click the *Virtru* switch in the top right corner to enable Virtru encryption.



- Enter the name of a friend in the *Recipients* field. If you are in a classroom, send to your classmate. If you are self-study, either send to one of your other email account, or to a friend.
- Enter a subject in the *Subject* field.
- Enter some text in the *Message* area.

4. Click the *Customize Intro* button.
5. Enter a way that the recipient may verify the email is from you.

6. Click the *Secure Send* button to send the email.



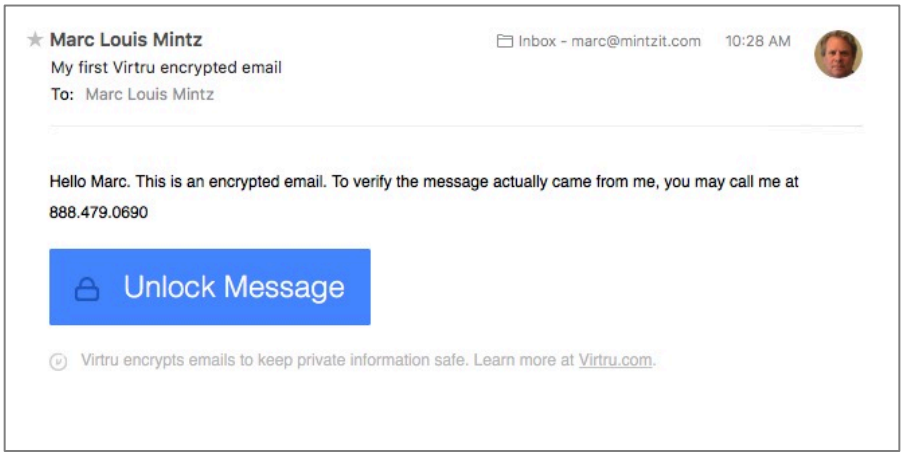
Your Virtru-encrypted email is on its way!

15.10.3 Receive and Reply to a Virtru-Encrypted Email

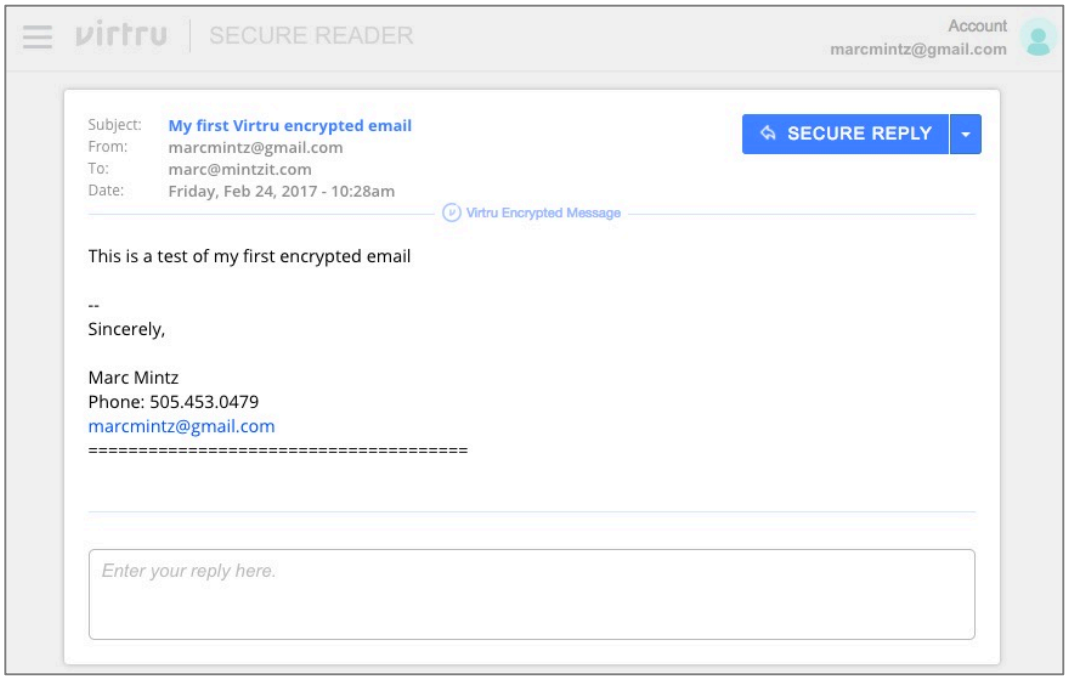
In this assignment, you receive and reply to a Virtru-encrypted email.

- Prerequisite: Completion of the previous assignment.

1. As the recipient of a Virtru-encrypted email, open your email to find the encrypted message sent from the previous assignment. Click the *Unlock Message* button.



2. A browser will open to the *Virtru Secure Reader* site, with the message decrypted.



3. To send an encrypted reply to the original sender (from the previous assignment), click the *Secure Reply* button.
4. Within the same window, a *Reply* field will appear. Enter your message, and then click *Send Secure*. The encrypted reply is on its way.

Revision Log

20180420, v2.0

- The majority of chapters have been edited for updated information.
- *Chapter 2.6 renumbered for readability.*
- *Chapter 4.5.1 Assignment: Harden the Keychain with a Different Password* removed. As of macOS 10.13.4 the login keychain password cannot be changed from the user account login password.
- Chapter *19.3 NordVPN* revised to create a free trial account.
- *Chapter 20.3 Facebook* heavily edited to reflect the revised privacy and timeline settings.
- *Chapter 20.4 LinkedIn* heavily edited to reflect the revised privacy settings.
- *Chapter 20.5 Google* heavily edited to reflect the revised privacy and Takeout options.

20180325, v 1.3

- *Chapter 4.8 Password Policies* added.
- *Chapter 12.1 Find My Mac* has been slightly edited.
- *Chapter 14.8 Do Not Track* has been edited to reflect changes in Ghostery, and the Chrome extension installation process.
- *Chapter 15.7 End-To-End Secure Email With GNU Privacy Guard* rewritten to reflect the major update of GPGTools.
- *Chapter 19.3 NordVPN* is rewritten from scratch from our previous recommended VPN host.

20171022, v1.2

- *Chapter 14 Web Browsing* is rewritten.

- *Chapter 15 Email,* added *hacked-emails.com* for checking if your email account was included in site breaches.
- *Chapter 16 Apple ID and iCloud*, added that Two-Factor Authentication can use either text messaging or voice call.
- *Chapter 19 Internet Activity,* changed the recommended VPN provider to *Perfect-Privacy.com.*

20171001, v1.1

- Updated chapter *Documents > Encrypt A Folder for Cross Platform Use With Zip* to use Keka, instead of the depreciated macOS built-in tools.

20170923, v1.01

- Updated chapter *When It Is Time To Say Goodbye*

20170918, v1.0

Initial release

Index

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.

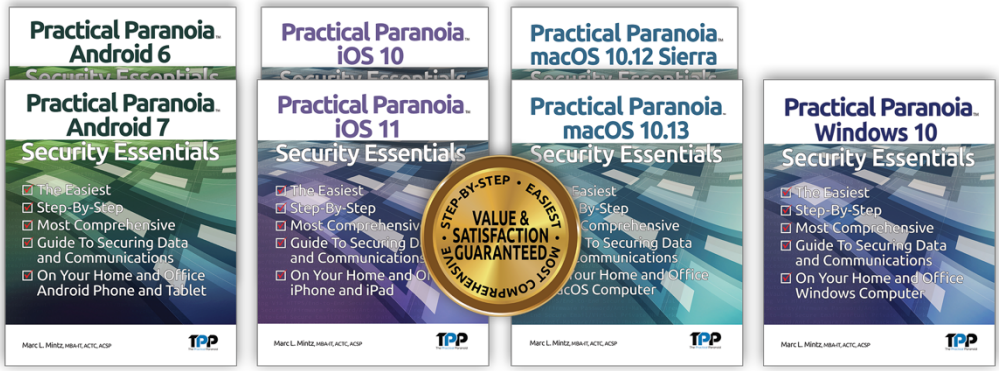
Let us contribute to your success.

Mintz InfoTech, Inc. is uniquely positioned to be your Virtual CIO and provide you and your organization comprehensive technology support. With the only MBA-IT consultant and 100% certified staff in New Mexico, our mission is to provide small and medium businesses with the same Chief Information and Security Officer resources otherwise only available to large businesses.

Mintz InfoTech, Inc.
Toll-free: +1 888.479.0690 • Local: 505.814.1413
info@mintzIT.com • https://mintzit.com

Practical Paranoia Workshops & Books

4 Years Undisputed #1 Best, Easiest, & Most Comprehensive Cybersecurity Series



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, everyone 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 macOS 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 classroom, workshop, and self-study. Includes all instructor presentations, hands-on assignments, software links, and security checklist. 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!

The Practical Paranoid, LLC
+1 888.504.5591 • info@thepracticalparanoid.com
https://thepracticalparanoid.com