Email Encryption 101 Workshop

Presented by: Matt Ward, CFSS, FIMS Computing Services – mward44@uwo.ca Office 281

Installing Thunderbird & Enigmail

1. Install Thunderbird email client: https://www.mozilla.org/en-US/thunderbird/
2. Install GPG4win and click the large green download button: https://www.gpg4win.org/ When installing GPG4, make sure each check box is selected in the "Choose Components" screen.
3. Open Thunderbird → skip integration.
4. Skip and choose "Use an existing email account."
5. Decide what email you want to use for encryption. (UWO, Gmail, Hotmail, etc.)
6. [If you are using your UWO email, follow this step.] You will need to enter these settings in the boxes below. Click manual configuration, and enter this info below. Once complete, hit done.

Incoming Settings	Outgoing Settings
Type: IMAP *Server Hostname* – outlook.office365.com *Port* – 993 *SSL Type* – SSL/TLS *Authentication* – Normal Password	*Server Hostname* – smtp.office365.com *Port* – 587 *SSL Type* – STARTTLS *Authentication* – Normal Password

7. Click on your inbox and you will see your email's inbox start to show up.
8. Right click on the top bar in the Thunderbird program. This will open a drop down menu. Click the "menu bar."
9. Once the menu bar has appeared: click on tools then add-ons.
10. Search for Enigmail → click add to Thunderbird → click install now.
11. Once it has installed, a restart now button should appear on the top right corner. Click that to restart Thunderbird.

Creating a Passphrase

1. Open up Thunderbird once more.
2. Enigmail mail setup wizard should pop up.
3. Start setup → click next.

4. Choose standard configuration.
5. Now, it will prompt you to create a passphrase.
6. Once you have entered your passphrase twice, click next.
7. This will create your key pair for email encryption. Ensure your passphrase is never compromised or shared!!
8. Create revocation certificate → save it on your computer. Try to not lose this.
9. Once the wizard is complete, click finish or close the window. You have now created a private and public key.

Creating a passphrase is an extremely important step. **If lost, there is no way to retrieve the passphrase**. It is gone forever. This is why we recommend you write it out on a piece of paper. A secure passphrase should contain 3-4 words.

Examples:

Good passphrase:MunchingTorsoWishingCabbage

Bad passphrase: HarryPotterForever

Your passphrase: _____

Never give your private key to anyone. If you suspect your private has been compromised, you can generate a new key pair by running this wizard over again

Sending an Encrypted Email

1. Click on the Thunderbird tab towards the top of your screen to get back to your inbox.
2. In order to send encrypted emails to your friends, you need each other's public key. Pick a partner and email them your key by clicking "attach my public key." Hit send.
3. Save your friends public key on your computer. Click on Engimail tab on the menu at the top of the screen and select "Key Management."
4. Choose "File" → "Import Key from File" → choose your friends public key you have saved to your computer. If prompted, click yes.
5. To send an encrypted email in Thunderbird compose a message as any other email. Choose "Write mail," → Fill other sections, such as the body and subject of the email
6. Before clicking send, click on the lock icon to ensure encryption is on and then send the email.
7. To decrypt your email from your friend, you must enter in your passphrase that you created earlier.
8. Voila. Welcome to secure PGP encrypted email!