National Cyber Security Agency (NCSA)

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

การรักษาความปลอดภัยของอีเมลด้วย Pretty Good Privacy (PGP) โดยการใช้ Mailvelope

โปรโตคอลการเข้ารหัสแบบ PGP (Pretty Good Privacy) ใช้ในการเข้ารหัสข้อมูลที่มีชั้นความลับ เพื่อส่งผ่านช่องทางอีเมล์

สารบัญ

1. หลักการขั้นพื้นฐาน

Pretty Good Privacy : (PGP) เป็นวิธีเข้ารหัสและยืนยันตัวตน โดยมากนิยมใช้เข้าและถอดรหัส และลงลายมือชื่อในการส่งอีเมล เริ่มสร้างโดย Phil Zimmermann เมื่อปี ค.ศ. 1991 มีหลักการทำงาน คือ อาศัยการเข้ารหัสแบบกุญแจสาธารณะ (public-key) ที่รวมถึงระบบที่รวมกุญแจไว้กับชื่อผู้ใช้ ในรุ่นแรกๆ นั้น PGP เป็นที่รู้จักในฐานะ web of trust ซึ่งแตกต่างจากระบบ X.509 ที่เป็นแบบโครงสร้างลำดับชั้น (hierarchical) ซึ่ง PGP ได้นำมาประยุกต์ใช้และปรับปรุงในภายหลัง

PGP ทำให้การสื่อสารมีความปลอดภัย ด้วยวิธีการให้เข้ารหัสข้อความโดยใช้กุญแจสาธารณะของผู้รับ ซึ่งสามารถเข้าถึงได้ด้วยกุญแจส่วนตัวเท่านั้น นอกจากนี้ยังสามารถใช้เพื่อยืนยันว่ามีการส่งข้อความโดยบุคคลนั้นเป็นผู้ส่งจริง, ป้องกันผู้โจมตีจากการส่งข้อความหลอกลวงและสามารถป้องกันข้อความไม่ให้ถูกแก้ไขโดยบุคคลที่สาม

2. รู้จัก Mailvelope

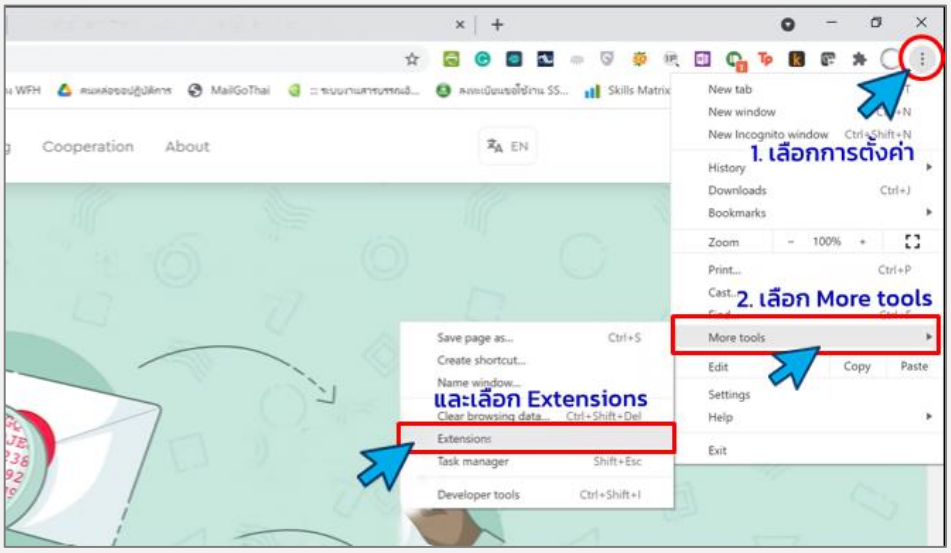
Mailvelope เป็นโปรแกรมเสริมของเบราว์เซอร์หรือปลั๊กอิน ที่เพิ่มขีดความสามารถในการเข้าถึงรหัสและเนื้อหาของอีเมล ซึ่งเป็นไปตามมาตรฐานการเข้ารหัส OpenPGP เพื่อให้สามารถ ส่ง รับ หรือเซ็นชื่ออีเมลแบบดิจิทัลได้อย่างปลอดภัย โดยการใช้บริการ OpenPGP เช่น Mailvelope นั้น ผู้ใช้จำเป็นจะต้องสร้างคู่กับกุญแจรหัสที่เป็นส่วนตัว และแชร์กุญแจรหัสสาธารณะก่อน

3.การใช้งานเบื้องต้น

ในการจะใช้งาน Mailvelope ได้นั้น จะต้องทำการติดตั้งตัวโปรแกรมลงบนเว็บเบราว์เซอร์ของเครื่องคอมพิวเตอร์ที่เราใช้งานเสียก่อน โดยตัวอย่างวิธีการติดตั้งนี้จะทำการติดตั้งลงบนเบราว์เซอร์ google chrome ซึ่งเป็นที่นิยม และมีผู้ใช้งานเป็นจำนวนมาก

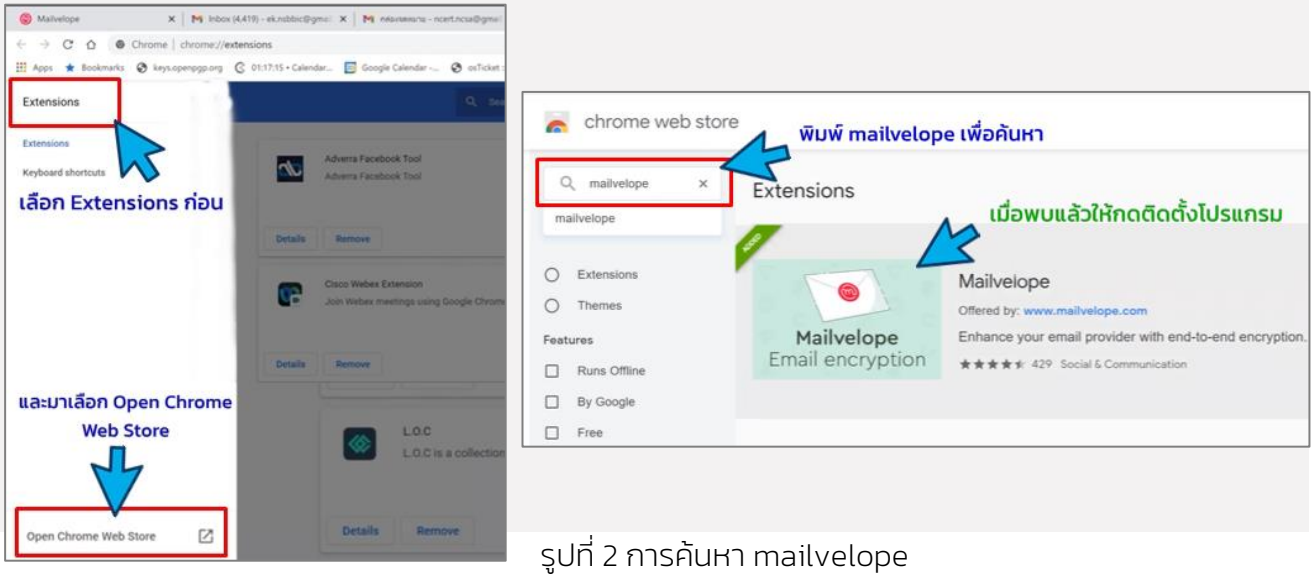
3.1 การติดตั้งบน Chrome

1. ไปที่แท็บตั้งค่าทางขวามือบนของ Chrome Chrome
2. เลือกเมนู More tools แล้วมาทำการเลือกที่เมนู Extensions ดังรูปที่ 1



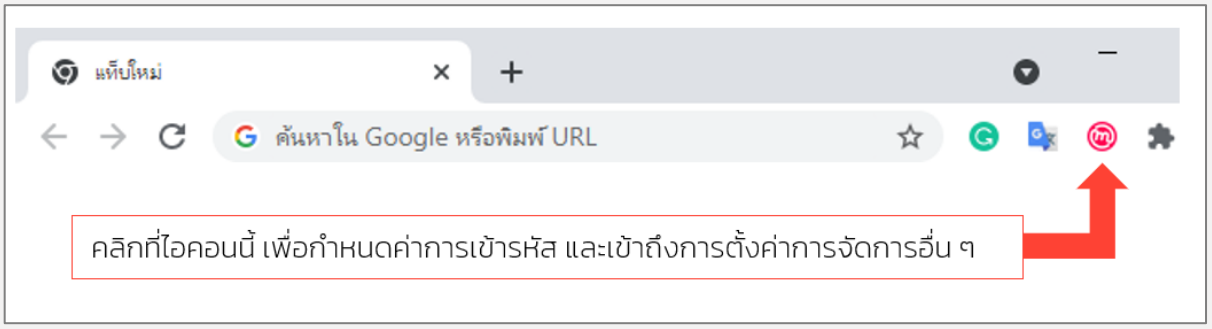
รูปที่ 1 การเข้าสู่เมนู Extensions

3. ไปทางซ้ายบนเลือก Extensions และไปด้านล่างเลือก Open Chrome Web Store
4. ในช่องค้นหา ใส่คำค้นว่า mailvelope และเมื่อพบโปรแกรม mailvelope แล้ว ให้ทำการติดตั้งลงบน Chrome ดังรูปที่ 2



รูปที่ 2 การค้นหา mailvelope

5. เมื่อดำเนินการตามขั้นตอนต่าง ๆ ให้เสร็จสิ้นแล้ว หากติดตั้ง Mailvelope สำเร็จ ไอคอน จะปรากฏขึ้นที่ใดที่หนึ่งในแถบเครื่องมือหลัก ดังรูปที่ 3



รูปที่ 3 ไอคอน Mailvelop บน Chrome

6. หากไม่มีไอคอน ปรากฏขึ้นมา ให้ไปเลือกที่ไอคอนจิ๊กซอว์ และเข้าไปเลือก Mailvelope เพื่อเพิ่มเป็นโปรแกรมส่วนขยาย

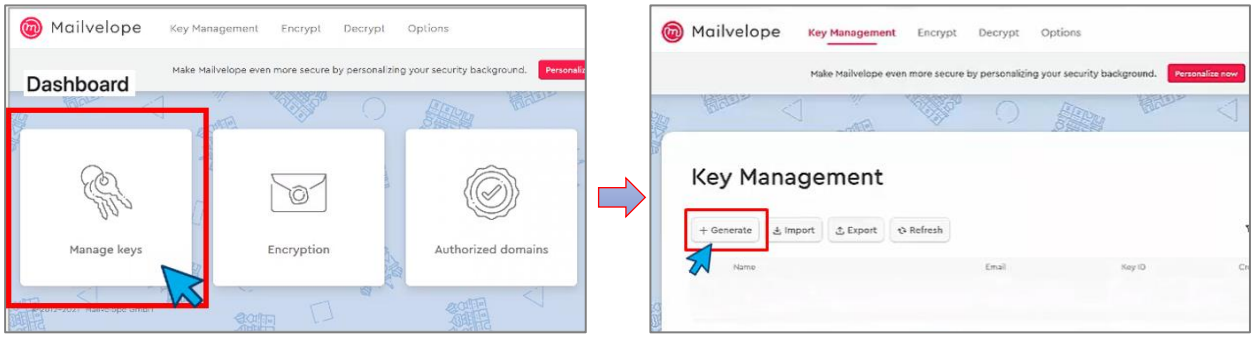
3.2 การจัดการกุญแจรหัส

ในการใช้งาน Mailvelope ครั้งแรก จะต้องทำการ การสร้างกุญแจรหัสขึ้นใหม่ และนำกุญแจรหัสนั้น ขึ้นประกาศบน Public Key Server เพื่อให้ผู้ที่ต้องการติดต่อกับเรามีกุญแจรหัสสาธารณะของเราเพื่อใช้ในการเข้ารหัสข้อความ

3.2.1 การสร้างกุญแจรหัส

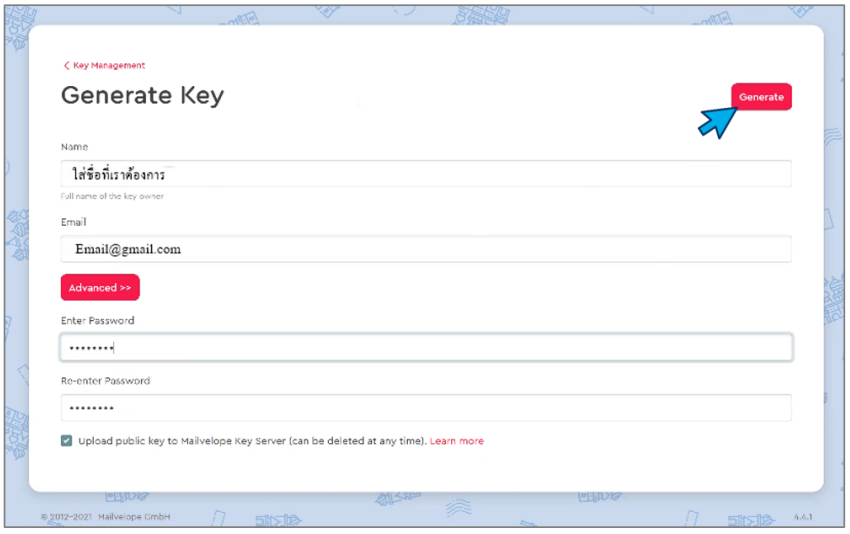
1. เลือก Mailvelope ที่เป็นสัญลักษณ์ตัวเอ็มสีแดง ที่อยู่ในแถบเครื่องมือหลักของ Chrome Chrome

2. ไปที่ key management ที่อยู่ในแถบเมนูด้านบน แล้วหน้า Dashboard จะปรากฏขึ้นมา จากนั้นเลือกที่ Manage Keys และกดเลือก +Generate เพื่อทำการสร้างกุญแจรหัสขึ้นใหม่ ตามรูปด้านล่างนี้



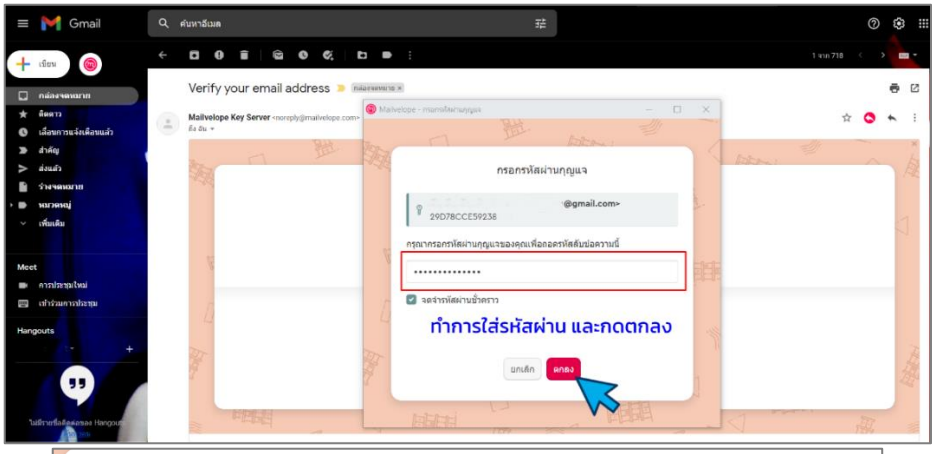
รูปที่ 4 การสร้างกุญแจรหัส

3. ใส่ข้อมูล name ที่ต้องการให้แสดง คู่กับ email ที่ต้องการใช้ เพื่อสร้างกุญแจรหัส ทำการใส่รหัสที่มีความปลอดภัย และใส่รหัสยืนยันให้ตรงกัน จากนั้นเลือก Generate ระบบจะส่งข้อมูลยืนยันไปที่ email ที่เราได้ให้ไว้ ดังรูปที่ 5



รูปที่ 5 การกรอกข้อมูลเพื่อสร้างกุญแจรหัส

4. ไปยังกล่องจดหมาย email ที่เราได้ทำการบันทึกไว้ โดยโปรแกรม Mailvelope จะส่งข้อความเข้ามาให้ทำการใส่รหัสที่บันทึกไว้ และคลิกกดตกลง จากนั้นทำการคลิกลิงก์ verify เป็นอันเสร็จขั้นตอน ดังรูปที่ 6



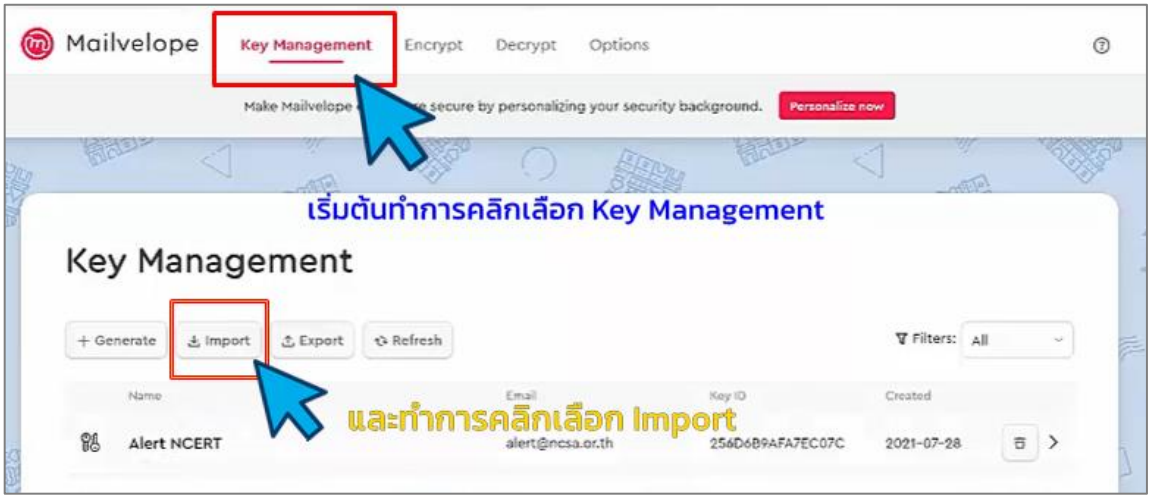
รูปที่ 6 การ verify ผ่าน Email

5. ทำซ้ำขั้นตอนเดิม สำหรับบัญชีอีเมลอื่น ๆ ที่เราต้องการสร้างกุญแจรหัสเพิ่มขึ้น

3.2.2 การนำเข้ากุญแจรหัส

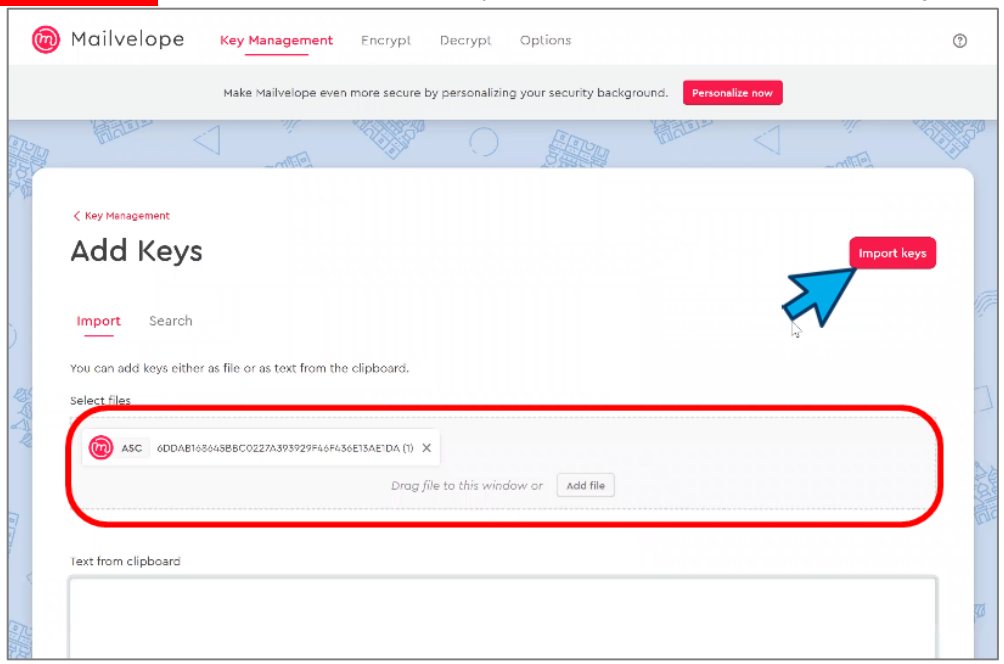
หากต้องการนำเข้ากุญแจรหัสของผู้อื่น ที่เราต้องการติดต่อสื่อสารด้วย โดยมีวิธีการและขั้นตอนการดำเนินการ ดังนี้

1. ให้ทำการคลิกเลือก Key Management ในแถบตัวเลือกด้านบนก่อน และทำการคลิกเลือกที่ Import ด้านล่าง ตามรูปที่ 7



รูปที่ 7 การเข้าเมนูนำเข้ากุญแจรหัส

2. ให้ทำการนำเข้ากุญแจรหัสของผู้ที่เราต้องการติดต่อสื่อสารด้วย ที่ได้มาจากไฟล์ข้อความที่ผู้ติดต่อส่งมาให้ หรือได้มาจากผู้เป็นเจ้าของกุญแจรหัส ได้ประกาศไว้บน Public Key Server โดยให้ทำการวางข้อความลงไปในช่อง Select files เสร็จแล้วให้คลิกเลือก Import Keys หลังจากนั้น เราก็จะมีกุญแจรหัสของเขามาเก็บไว้ ดังรูปที่ 8

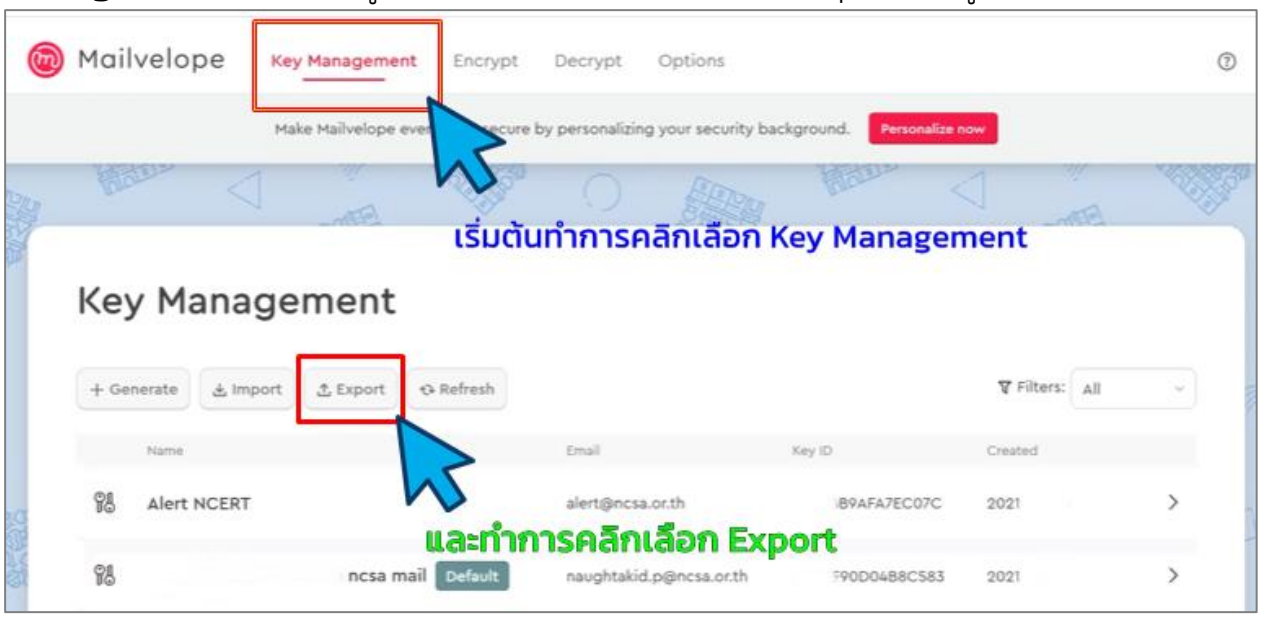


รูปที่ 8 การเลือกและกดยืนยันเพื่อนำเข้ากุญแจรหัส

3.2.3 การส่งออกกุญแจรหัส

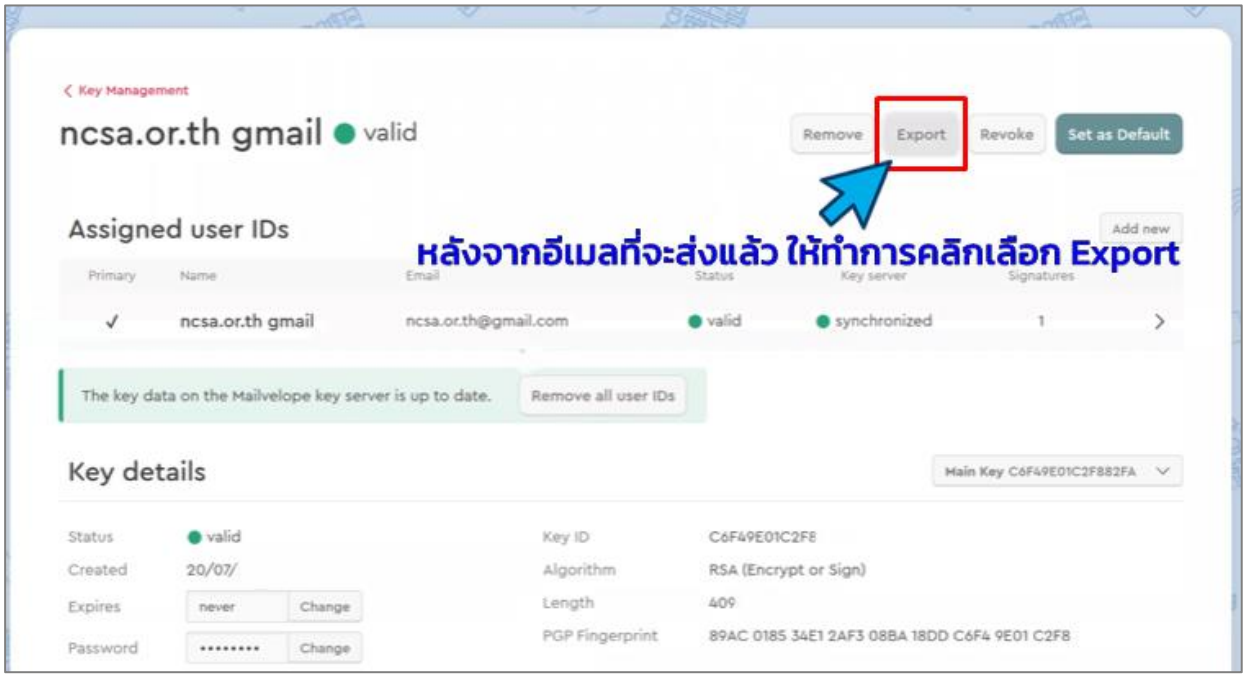
หากต้องการส่งออกกุญแจรหัสของเรา ส่งไปให้กับผู้ที่เราต้องการติดต่อสื่อสารด้วย เพื่อเขาได้ทำการนำเข้ากุญแจรหัสของเรานั้น มีวิธีการและขั้นตอนการดำเนินการ ดังนี้

1. หากต้องการส่งออกกุญแจรหัสของเราทั้งหมดทีเดียว ให้เริ่มคลิกเลือกที่ Key Management ในแถบเมนูด้านบน แล้วทำการคลิกเลือก Export ดังรูปที่ 9



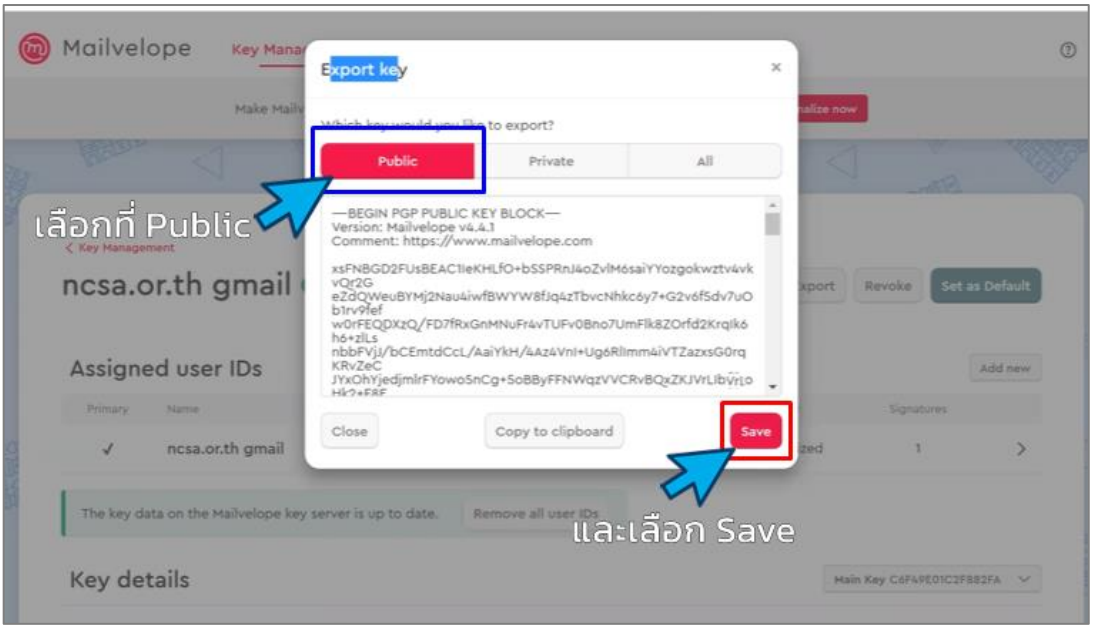
รูปที่ 9 การเข้าเมนูการส่งออกกุญแจรหัส

2. หากต้องการส่งออกกุญแจรหัสของเราเพียงอีเมลใดอีเมลหนึ่ง ให้ทำการคลิกเลือกเฉพาะที่อีเมลนั้น แล้วทำการคลิกเลือก Export ทางด้านบนขวามือ ดังรูปที่ 10

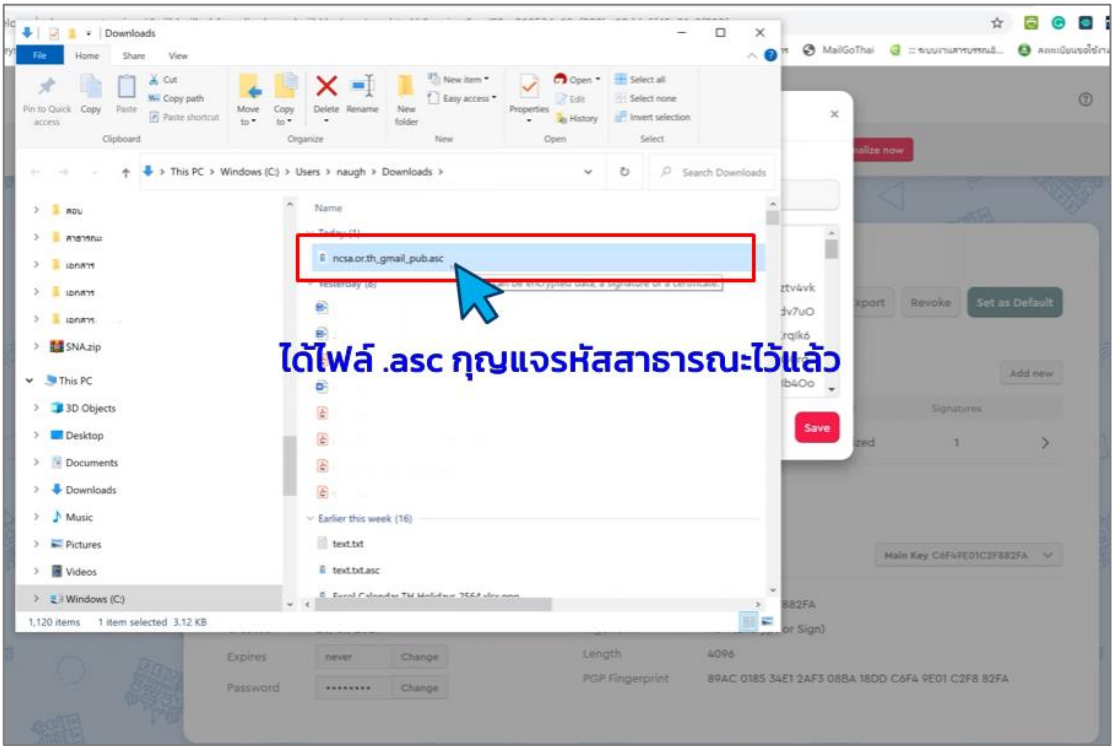


รูปที่ 10 การส่งออกกุญแจรหัส

3. จากนั้นให้ไปเลือกที่แท็บ Public และคลิกเลือก Save จะมีการดาวน์โหลดไฟล์ กุญแจรหัสสาธารณะ (public key) ที่เป็นไฟล์นามสกุล .asc มาเก็บไว้ที่เครื่องคอมพิวเตอร์ของเรา โดยเราจะใช้ไฟล์นี้ ส่งให้กับผู้ที่เราต้องการติดต่อสื่อสารด้วย นอกจากนี้เราต้องไม่บอกให้ใครรู้ถึงกุญแจรหัสส่วนตัวของเรา ซึ่งจะเก็บกุญแจรหัสส่วนตัวดังกล่าว ไว้เป็นความลับ ดังรูปที่ 11 -12 หรือคลิกที่ copy to clipboard เพื่อส่งกุญแจรหัสเป็นข้อความ ให้ผู้ที่ต้องการติดต่อสื่อสารได้อีกวิธีหนึ่งด้วย



รูปที่ 11 การ save public key



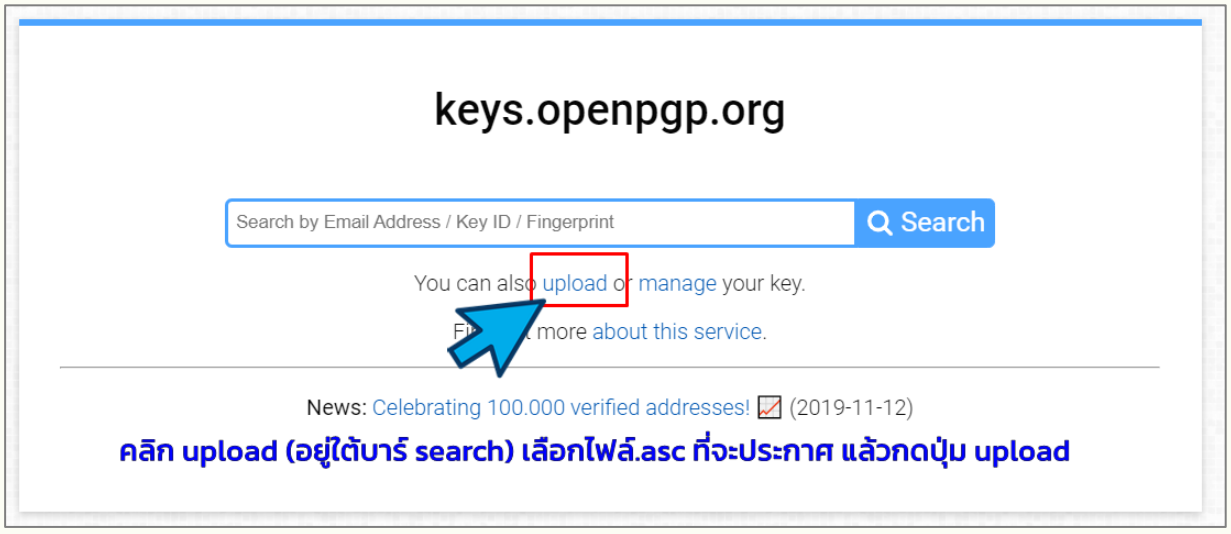
รูปที่ 12 ตรวจสอบ ไฟล์ .asc ของ public key ที่ได้ทำการ save

3.2.4 การนำกุญแจรหัสขึ้นประกาศบน Public Key Server

เป็นการแจ้งให้บุคคลอื่นทราบว่าเราใช้ PGP อยู่ เพื่อให้บุคคลอื่น ๆ สามารถส่งข้อความแบบเข้ารหัสติดต่อสื่อสารกันได้ โดยนำกุญแจรหัสของเรา ประกาศไว้เป็นสาธารณะบน Public Key Server พร้อมรายละเอียดอื่น ๆ ที่บุคคลทั่วไปสามารถค้นหา และตรวจสอบได้ คือ Key ID , PGP Fingerprint และสามารถดาวน์โหลด กุญแจรหัสของเรา ไปเพิ่มเพื่อติดต่อกับเราได้ทันที มีวิธีการและขั้นตอนการดำเนินการ ดังนี้

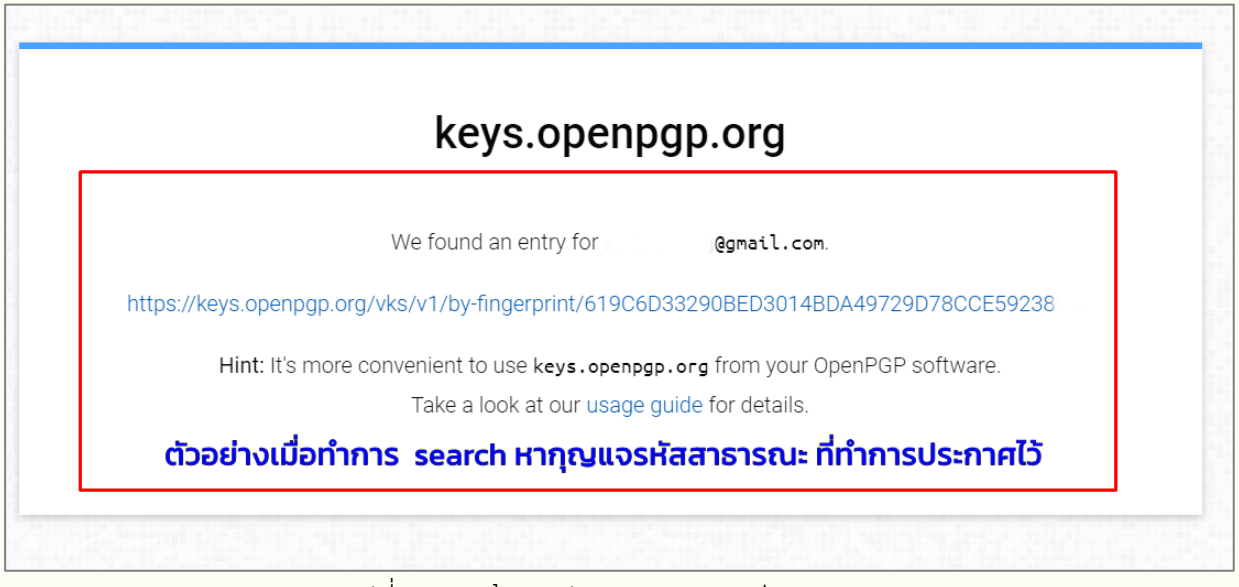
1. ให้ทำการหาเว็บไซต์ที่ให้บริการ Public Key Server โดยในคู่มือฉบับนี้ จะแนะนำเว็บไซต์ชื่อว่า https://keys.openpgp.org/

2. ทำการคลิกเลือก upload (อยู่ใต้บาร์ search) และเลือกไฟล์ กุญแจรหัสสาธารณะ (public key) ที่เป็นไฟล์นามสกุล .asc ที่เก็บไว้ในเครื่องเรา แล้วกดปุ่ม upload



รูปที่ 13 การ upload กุญแจรหัสสาธารณะ ขึ้น Public Key Server

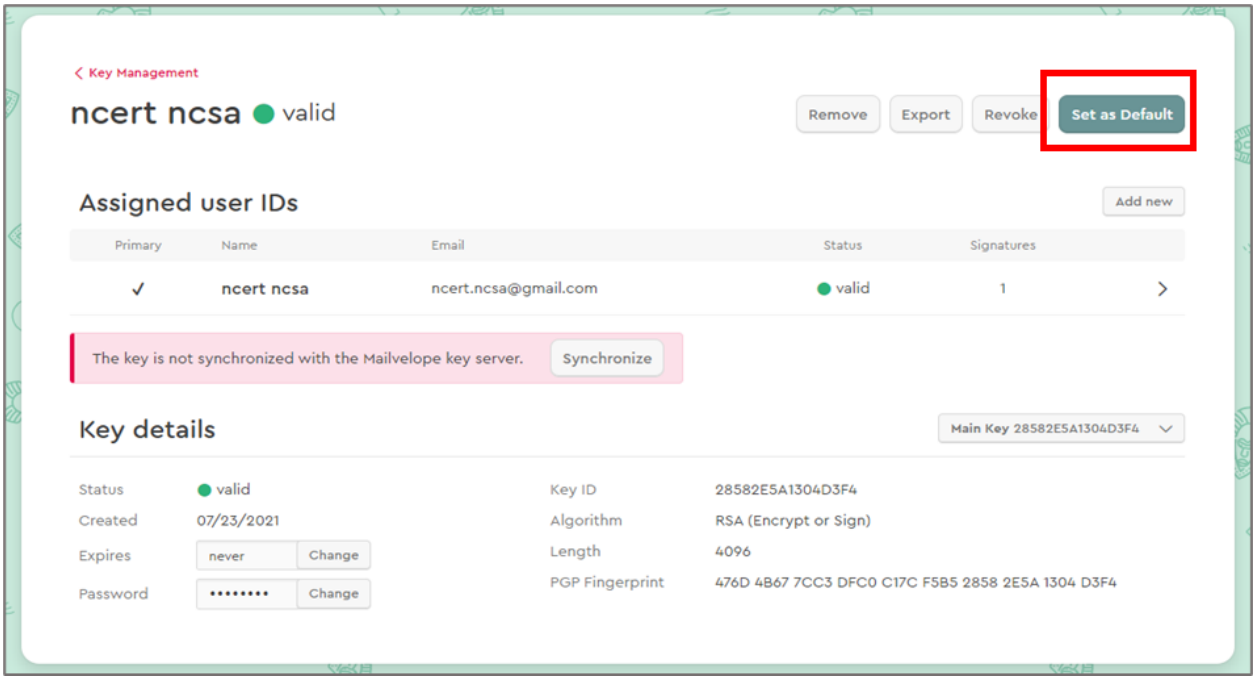
3. เมื่อทำการ upload ไฟล์กุญแจรหัสสาธารณะ ของเราสำเร็จแล้ว ให้ไปเข้า email เพื่อทำการคลิกลิงก์ verify เป็นอันเสร็จขั้นตอน



รูปที่ 14 การค้นหาประกาศกุญแจรหัสสาธารณะ

3.2.5 การกำหนดกุญแจรหัสหลัก

หากต้องการกำหนดกุญแจรหัสใด เป็นกุญแจรหัสหลัก/กุญแจรหัสเริ่มต้น ให้คลิกเลือก Key Management ในเมนูตัวเลือก หลังจากนั้น กดเลือกกุญแจรหัสที่ต้องการ แล้วคลิก Set as Default โดยปกติแล้ว กุญแจรหัสหลัก/กุญแจรหัสเริ่มต้นจะถูกเลือกใช้ก่อนเสมอ เว้นแต่จะมีการเลือกกุญแจรหัสอื่นไว้แทน ดังรูปที่ 15

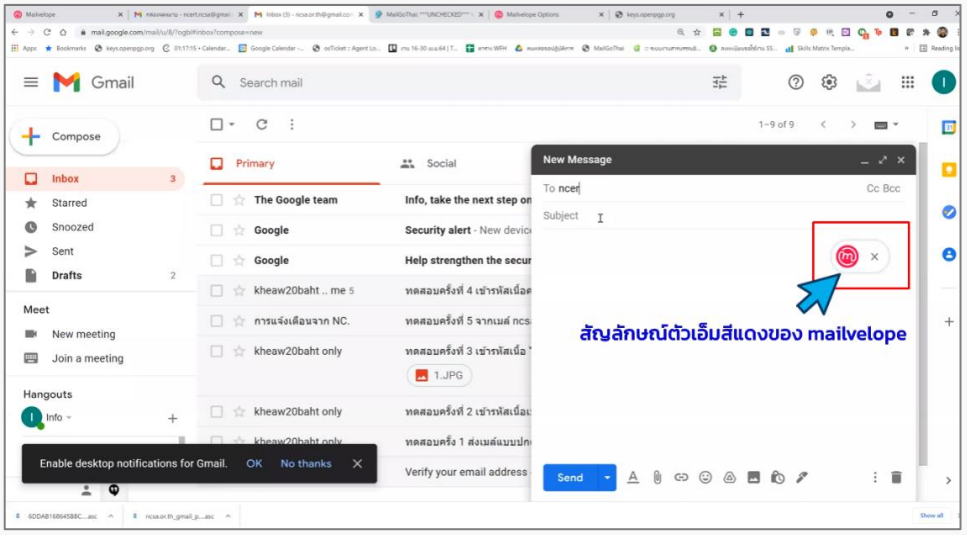


รูปที่ 15 การกำหนดกุญแจรหัสหลัก

4. ตัวอย่างการใช้งาน Mailvelope

4.1 การใช้งาน email และการลงชื่อยืนยัน

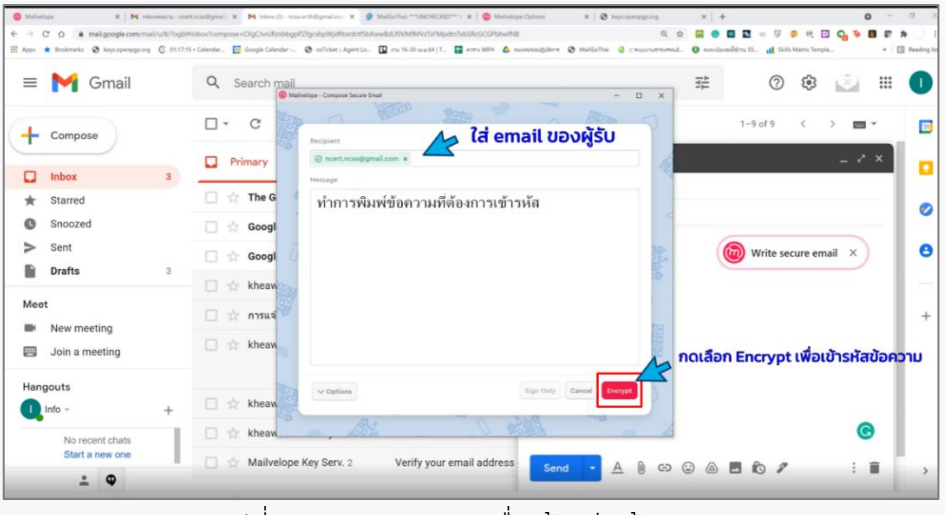
1. การใช้ mailvelope กับ free email ยอดนิยมส่วนมาก เช่น gmail จะสามารถใช้งานได้ทันที โดยให้เลือกเขียน email ใหม่ จะพบสัญลักษณ์ตัวเอ็มสีแดงของ mailvelope ปรากฏอยู่ในช่องเขียนข้อความ



รูปที่ 16 การเข้าใช้งาน Mailvelope ในการส่ง email บน Gmail

2. ผู้ใช้งานสามารถคลิกสัญลักษณ์ดังกล่าว และระบุชื่อรายละเอียดผู้รับ (Recipient) เป็น email หากผู้รับมีกุญแจรหัสอยู่แล้ว จะแสดงเป็นตัวอักษรสีเขียว ยืนยันได้ว่าเป็น email ที่มี PGP หากพบว่า เป็นตัวอักษรสีแดง ให้ตรวจสอบความถูกต้องของ email หรือสันนิษฐานว่าอาจยังไม่มีกุญแจรหัส

3. ในช่อง Message สามารถพิมพ์ข้อความใด ๆ ซึ่งจะถูกเข้ารหัสไว้ ในกรณีที่ต้องการลงชื่อผู้ส่ง (Sign) สามารถกดเลือก option ด้านล่างซ้าย และเลือก Sign message แล้วเลือก key ที่จะใช้ลงชื่อได้ ทั้งนี้ สามารถเลือกเฉพาะการลงชื่อเพื่อส่งเท่านั้น หรือจะเลือกเฉพาะเข้ารหัสเนื้อความโดยไม่ลงชื่อ หรือจะเลือกทั้ง 2 อย่างก็ได้ ขึ้นอยู่กับวัตถุประสงค์การใช้งาน

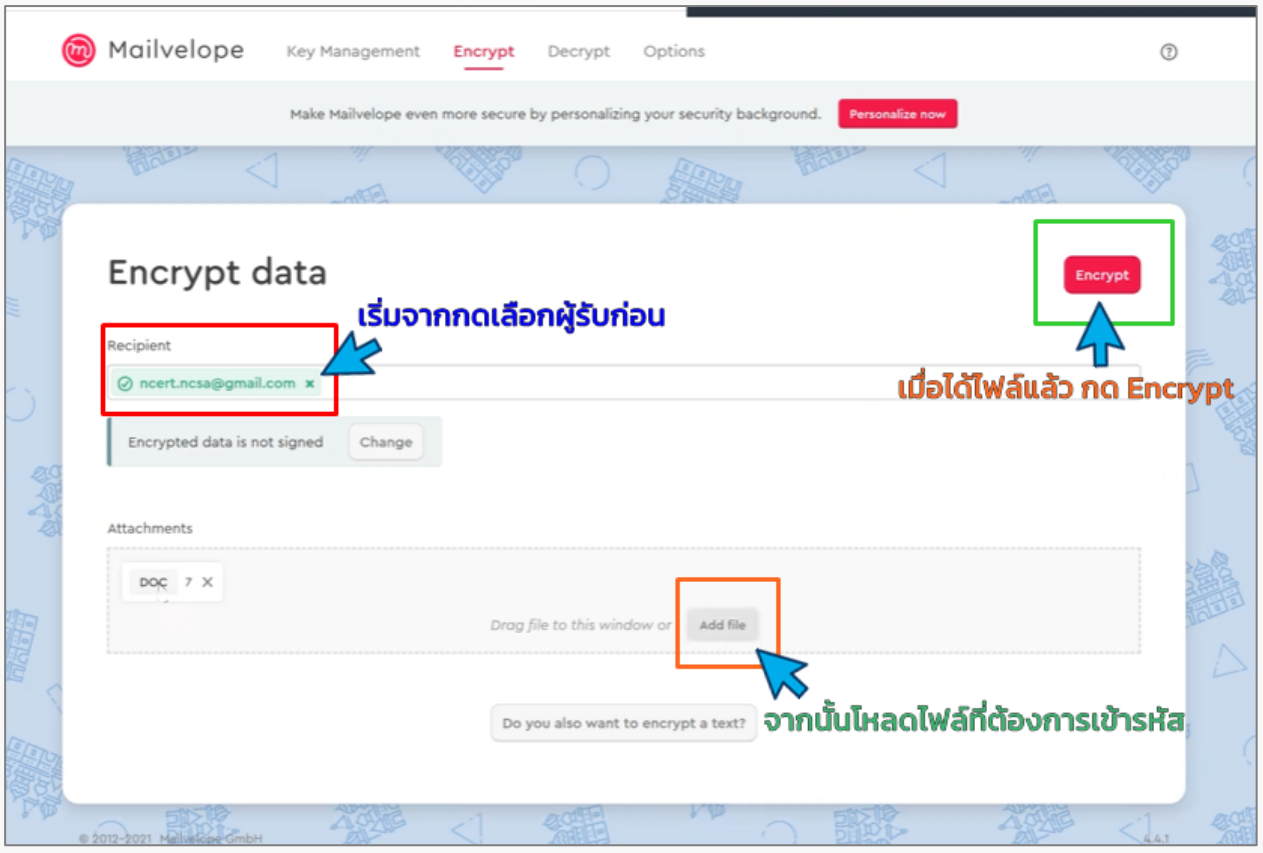


รูปที่ 17 การ Encrypt เพื่อเข้ารหัสข้อความ

4.2 การเข้ารหัส และถอดรหัสไฟล์

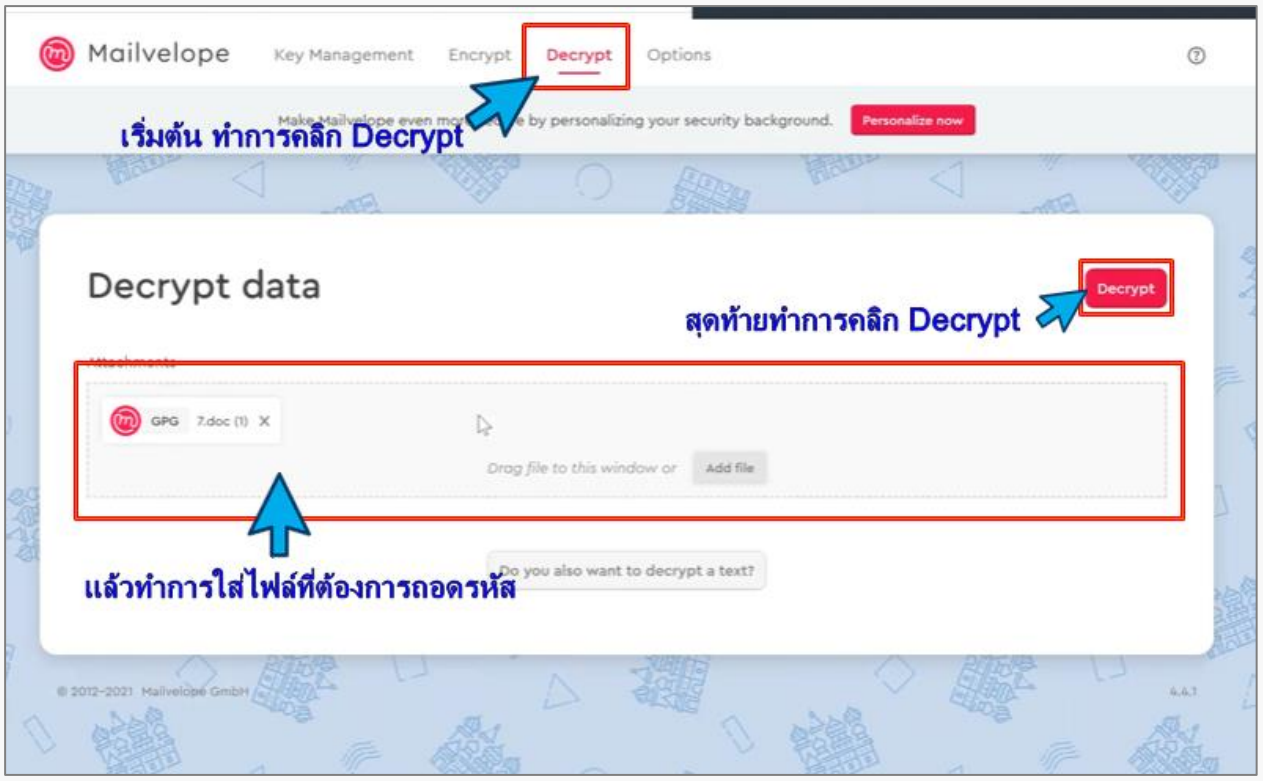
การส่ง email ด้วย PGP จะเป็นการลงชื่อ หรือเข้ารหัสข้อความเนื้อหาใน email เพียงเท่านั้น จะไม่มีการเข้ารหัสไฟล์แนบใน email ที่ส่งไป ซึ่งในการเข้ารหัส และถอดรหัสไฟล์มีวิธีการและขั้นตอนการดำเนินการ ดังนี้

1. เราสามารถแนบไฟล์ที่เข้ารหัสได้ โดยไปที่แถบเมนู Encrypt ที่อยู่ด้านบน แล้วทำการเลือกชื่อผู้รับ จากนั้นเลือกไฟล์ที่ต้องการเข้ารหัส ที่มีขนาดไม่เกิน 50 MB แล้วกด Encrypt จะได้ไฟล์ชื่อเดิมแต่มีนามสกุลต่อท้ายเพิ่มเป็น GPG กดโหลดไฟล์ที่เข้ารหัสแล้วมาไว้ที่เครื่องคอมพิวเตอร์ของเรา แล้วนำไปส่งต่อ ยังปลายทางที่ต้องการ ดังรูปที่ 18



รูปที่ 18 การเข้ารหัสไฟล์

2. ผู้ใช้งานสามารถส่งไฟล์นี้ให้กับผู้รับที่ถูกระบุได้ โดยอาจใช้ช่องทางอื่น ๆ ไม่จำเป็นต้องส่งผ่าน email ก็ได้ ทั้งนี้ ผู้รับสามารถนำไฟล์ที่ได้รับไปทำการถอดรหัส โดยไปที่เมนู Decrypt เลือกไฟล์ที่ได้รับมา แล้วกด Decrypt จะได้ไฟล์ที่ถอดรหัสแล้ว โหลดมาใช้งานได้ทันที ดังรูปที่ 19

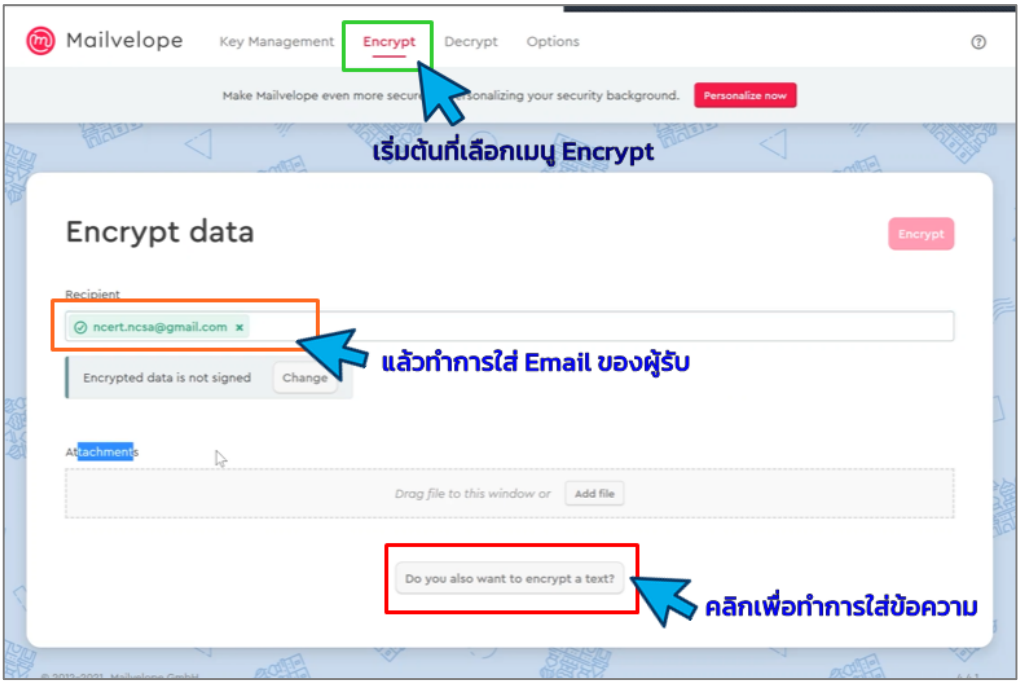


รูปที่ 19 การถอดรหัสไฟล์

4.3 การเข้ารหัสข้อความ (text)

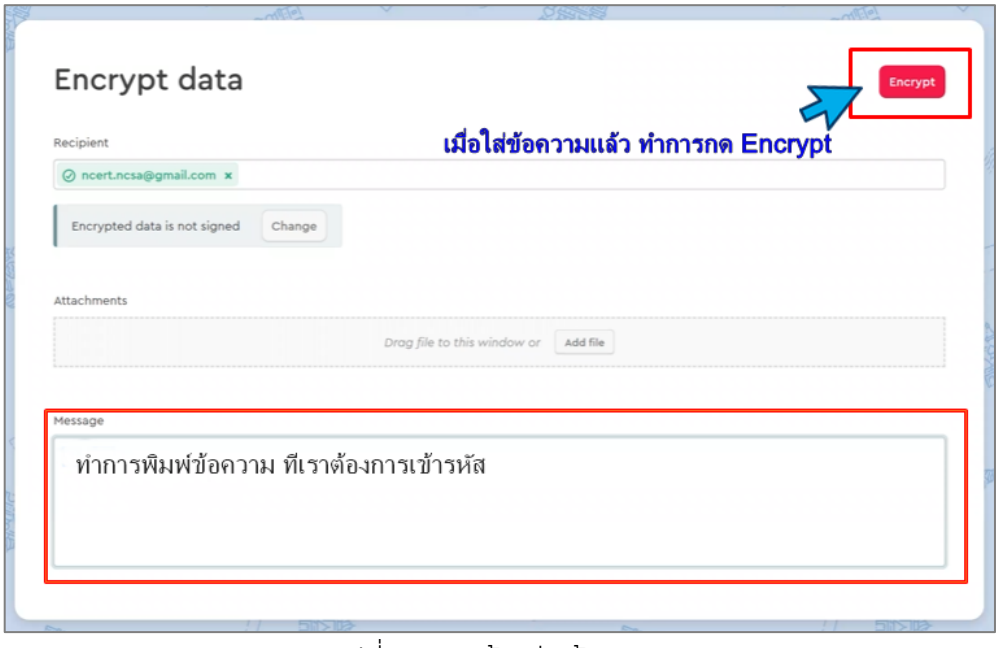
นอกจากนี้ ผู้ใช้งานยังสามารถเลือก สร้างข้อความ (text) ที่เข้ารหัส เพื่อส่งให้กับผู้รับปลายทางได้ มีวิธีการและขั้นตอนการดำเนินการ ดังนี้

1. โดยเข้าไปที่แถบเมนู Encrypt แล้วทำการใส่ Email ของผู้รับข้อความ และไปเลือกเลือกบรรทัดล่างสุด Do you also want to encrypt a text? ดังรูปที่ 20



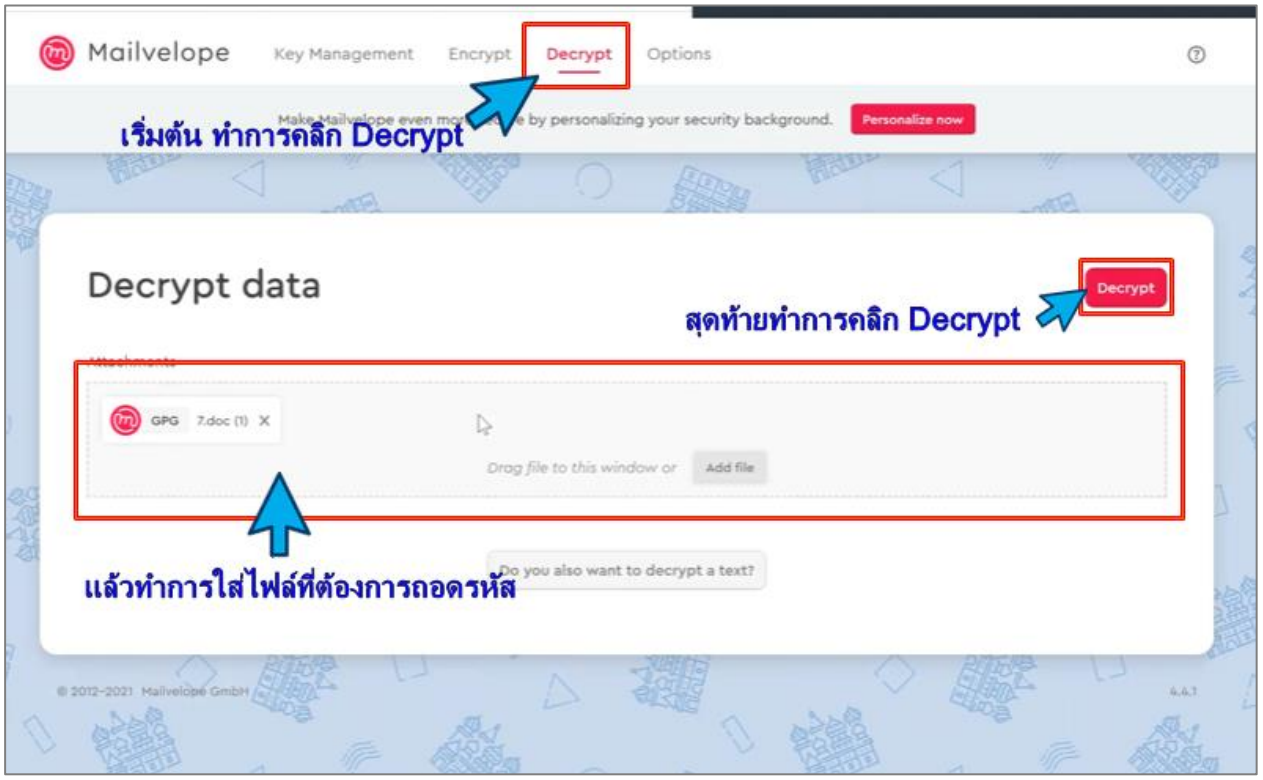
รูปที่ 20 การเข้าเมนูสำหรับเข้ารหัสข้อความ (text)

2. จากนั้น ให้พิมพ์ข้อความที่ต้องการเข้ารหัส ในช่อง message แล้วกด Encrypt จะได้ข้อความที่เข้ารหัสแล้ว สามารถคัดลอกไปใช้ส่งถึงผู้รับโดยตรง หรือจะกดดาวน์โหลดเป็นไฟล์ text ที่มีนามสกุลต่อท้าย .asc มาใช้ส่งให้กับผู้รับก็ได้ ดังรูปที่ 21



รูปที่ 21 การเข้ารหัสข้อความ

3. ส่วนผู้รับสามารถทำการถอดรหัสโดย Decrypt ข้อความ หรือไฟล์ดังกล่าวมาใช้ โดยใช้เมนู Decrypt เช่นเดียวกับการถอดรหัสไฟล์ที่กล่าวมาแล้ว ดังรูปที่ 22

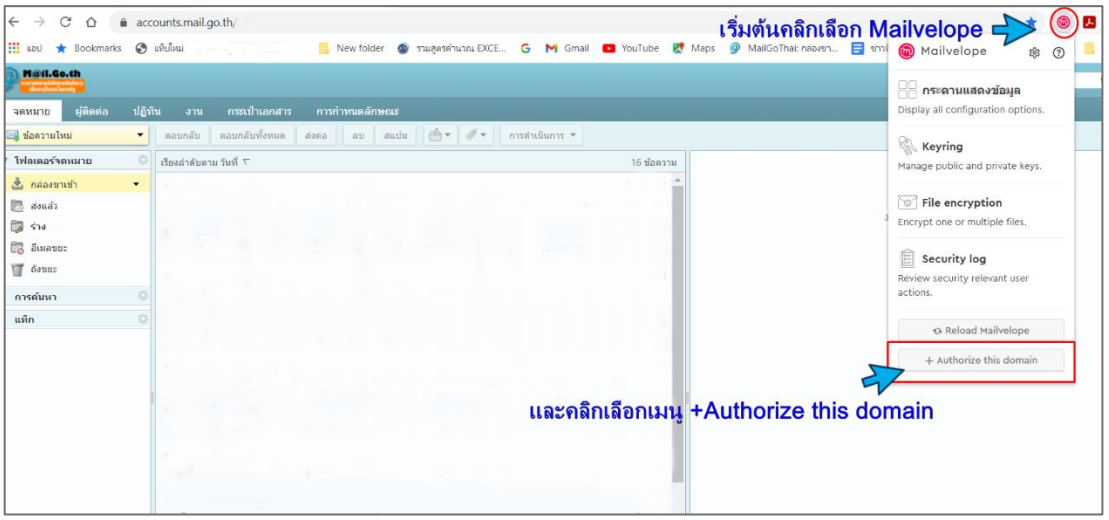


รูปที่ 22 การเข้ารหัสข้อความ

4.4 การใช้งาน mailvelope กับ อีเมล์ _@ncsa.or.th

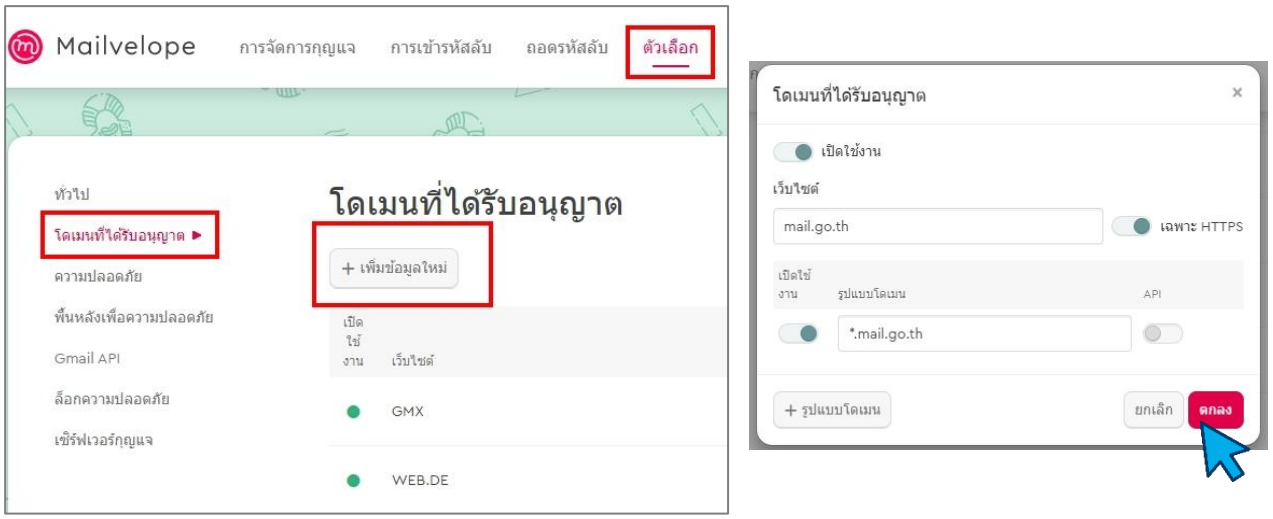
การใช้งาน mailvelope กับอีเมล์ของ ncsa.or.th ก็สามารถทำได้เช่นเดียวกัน โดยมีขั้นตอนและวิธีการดังนี้

1. เมื่อทำการเข้าสู่ระบบของอีเมล์ _@ncsa.or.th แล้วนั้น ให้คลิกเลือก Mailvelope ที่เป็นสัญลักษณ์ตัวเอ็มสีแดง ที่อยู่ในแถบเครื่องมือหลัก จะมีเมนูปรากฏขึ้นมา ให้ทำการคลิกเลือกเมนู +Authorize this domain ดังรูปที่ 23



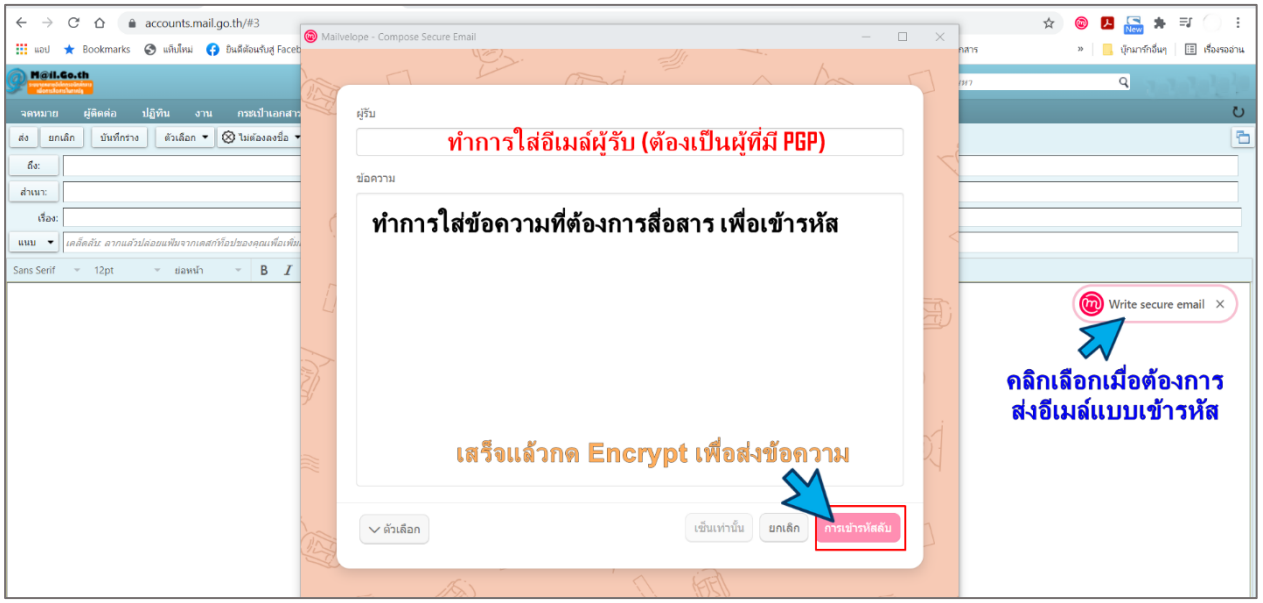
รูปที่ 23 การเริ่มต้นการใช้งานกับอีเมล์ ncsa.or.th

2. mailvelope จะอนุญาตให้ใช้งานกับโดเมน mail.go.th หรือให้ทำการพิมพ์ mail.go.th ลงไปในช่องว่าง เสร็จแล้วให้ทำการคลิกเลือก ตกลง ก็จะสามารถใช้งานการรับ-ส่งอีเมล์เข้ารหัส กับอีเมล์ _@ncsa.or.th ได้ทันที ดังรูปที่ 24



รูปที่ 24 อนุญาตการใช้งาน

3. เมื่อต้องการส่งอีเมล์แบบเข้ารหัส ให้ไปที่เมนู ข้อความใหม่ และไปคลิกเลือกที่สัญลักษณ์ตัวเอ็มสีแดงของ mailvelope ที่อยู่ด้านข้าง ก็จะปรากฏกล่องข้อความ เพื่อทำการใส่ข้อความเพื่อเข้ารหัสไปยังผู้ที่เราต้องการติดต่อสื่อสารด้วย เสร็จแล้วกด Encrypt เพื่อส่งข้อความ ดังรูปที่ 25



รูปที่ 25 การส่งอีเมล์_@ncsa.or.th แบบเข้ารหัส
