

คู่มือ

การตั้งค่าการยืนยันตัวตนแบบสองปัจจัย (Two-Factor Authentication : 2FA)

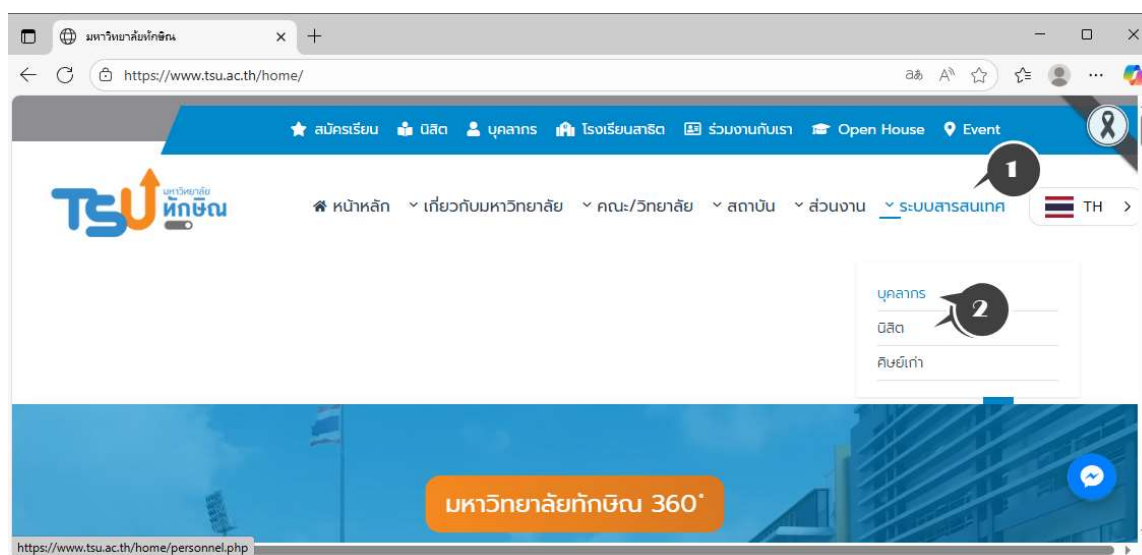
สำหรับระบบอีเมล TSU Mail (@tsu.ac.th) มหาวิทยาลัยทักษิณ

Two-Factor Authentication หรือเรียกย่อ ๆ ว่า 2FA เป็นวิธีการในการยืนยันตัวตนแบบหลายปัจจัย เพื่อให้เกิดความปลอดภัยในการใช้งานระบบมากยิ่งขึ้น สำหรับระบบ Google Workspace ใช้วิธีการยืนยันตัวตนแบบ 2 ขั้นตอน โดยจะใช้โทรศัพท์มือถือหรืออีเมลส่วนตัวสำหรับการยืนยันตัวตนอีกขั้นตอนหลังจากใส่รหัสผ่าน ซึ่งจะช่วยให้สามารถป้องกันการบุกรุกเข้าใช้งานบัญชีอีเมลของผู้ใช้จากผู้ไม่ประสงค์ดี อีกทั้งยังสามารถช่วยให้เกิดความปลอดภัยกับผู้ใช้งานอีเมลมหาวิทยาลัยในภาพรวมได้

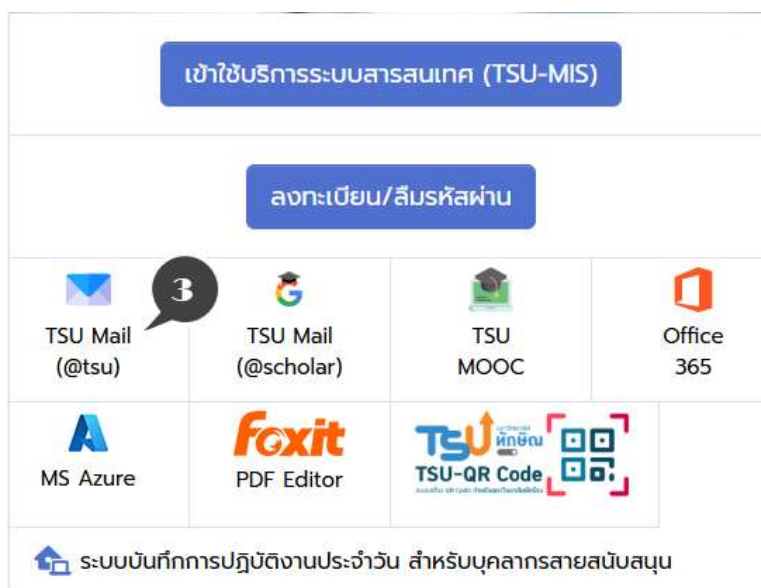
กุเกิ้ลซึ่งเป็นผู้ให้บริการอีเมลมหาวิทยาลัยภายใต้โดเมน @tsu.ac.th กำลังจะบังคับใช้งานการยืนยันตัวตนแบบ 2 ขั้นตอน ภายในวันที่ 15 ธันวาคม 2568 นี้ ดังนั้นผู้ใช้งานจึงต้องดำเนินการตั้งค่า 2FA ให้เสร็จสิ้นก่อนถึงกำหนดเวลาดังกล่าวเพื่อหลีกเลี่ยงปัญหาการเข้าใช้งานระบบอีเมลมหาวิทยาลัยไม่ได้ ซึ่งการดำเนินการดังกล่าวนี้ ผู้ใช้จะต้องเตรียมเครื่องมือ 2 อย่าง คือ โทรศัพท์มือถือ และอีเมลส่วนตัว เพื่อนำมาใช้สำหรับสร้างทางเลือกการใส่รหัสผ่านร่วมกับเครื่องมือที่กุเกิ้ลได้เตรียมไว้ เช่น Google Authenticator เบอร์โทรศัพท์มือถือ หรืออีเมลส่วนตัวสำหรับการกู้คืนระบบ ซึ่งระบบจะบอกให้เจ้าของบัญชีไปเปิด OTP (One Time Password) บนโทรศัพท์มือถือของตนเพื่อนำรหัสดังกล่าวมากรอกในระบบอีกครั้งจึงจะสามารถเข้าใช้บริการได้สำเร็จ โดยการตั้งค่า 2FA มีขั้นตอนดังนี้

ส่วนที่ 1 การตั้งค่า Google Authenticator

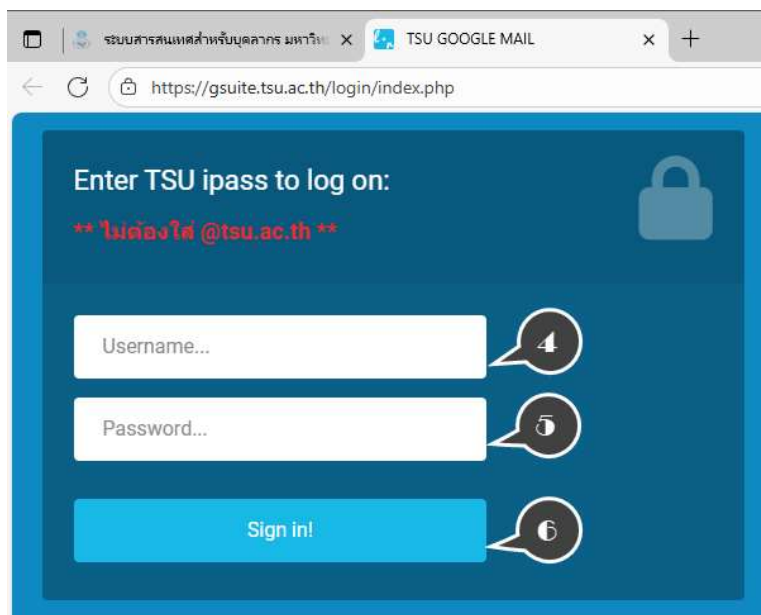
1. เปิดเว็บไซต์มหาวิทยาลัย (<https://www.tsu.ac.th>) คลิกเมนู “ระบบสารสนเทศ” เลือกเมนูย่อย “บุคลากร” หรือ “นิสิต”



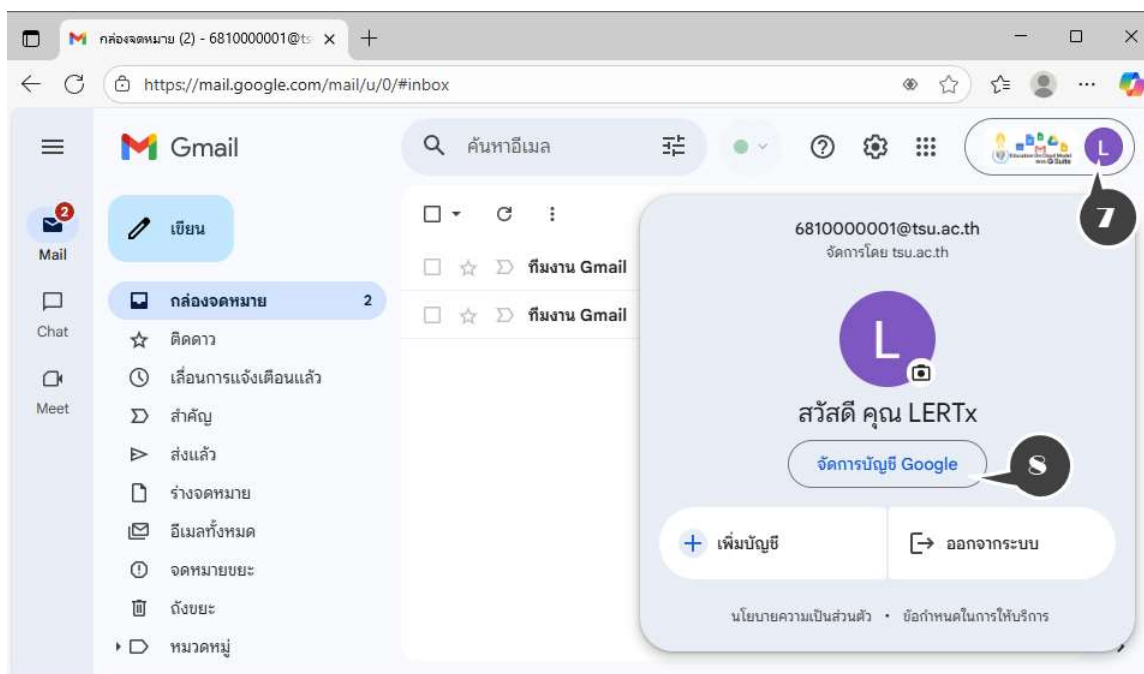
2. คลิกที่ “TSU Mail (@tsu)”



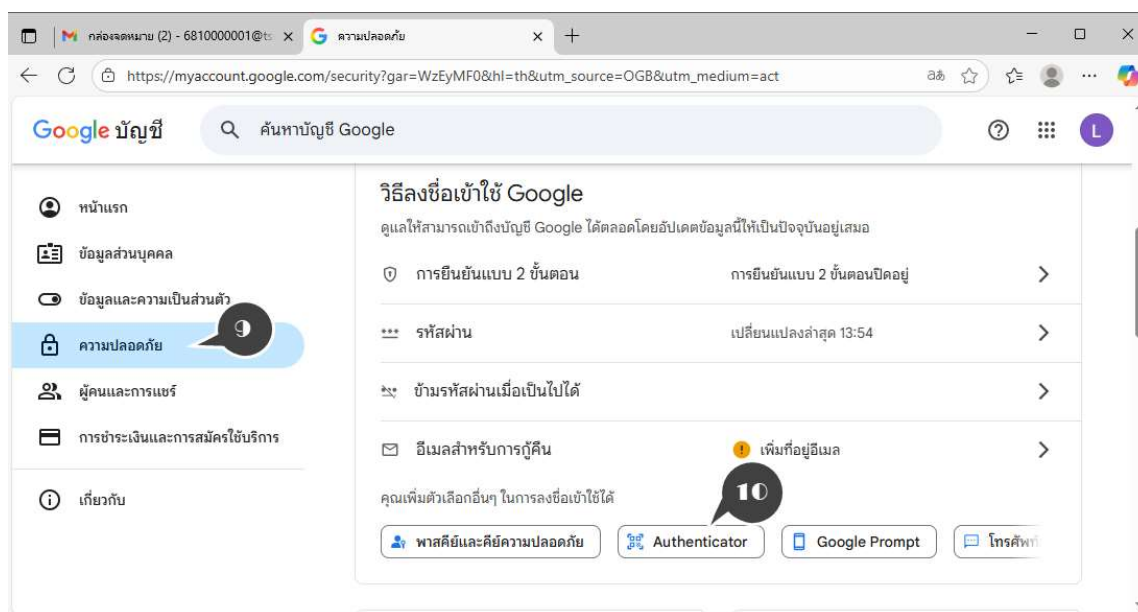
3. เข้าสู่ระบบอีเมลมหาวิทยาลัย โดยกรอกรหัสผู้ใส่ และรหัสผ่าน แล้วคลิกปุ่ม “Sign in”



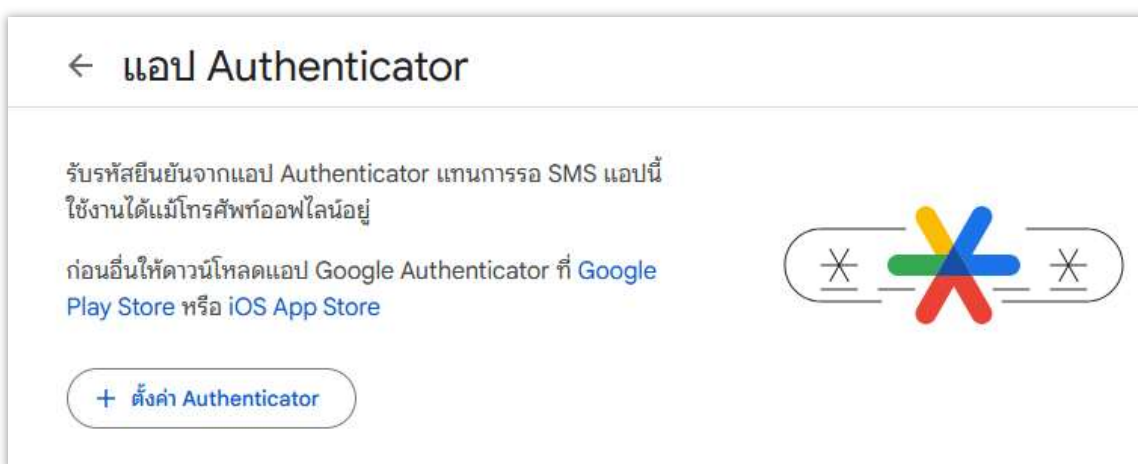
4. คลิกที่ “รูปโปรไฟล์” มุมบนขวา แล้วคลิกที่ “จัดการบัญชี Google”



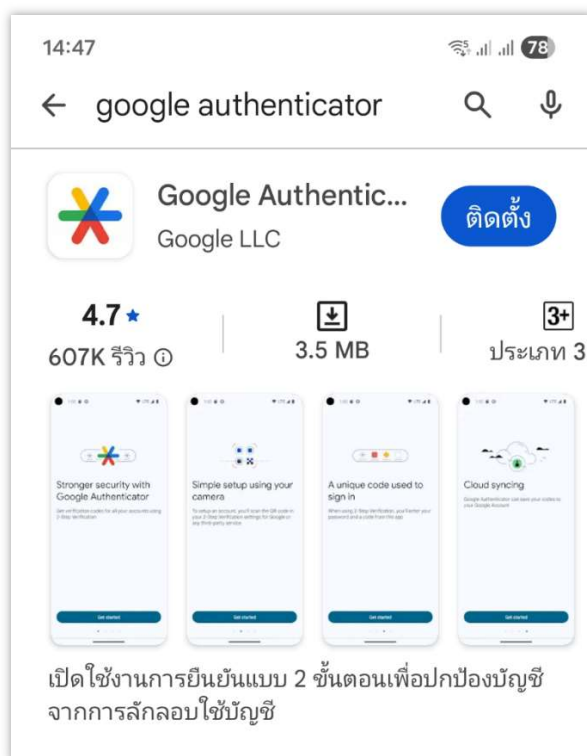
5. สำหรับการตั้งค่าของส่วนที่ 1 เป็นการเปิดใช้แอปพลิเคชันสำหรับรหัสผ่านแบบใช้งานได้ครั้งเดียว (One-time Password) ให้ผู้ใช้คลิกที่ “ความปลอดภัย” และคลิกที่ “Authenticator”



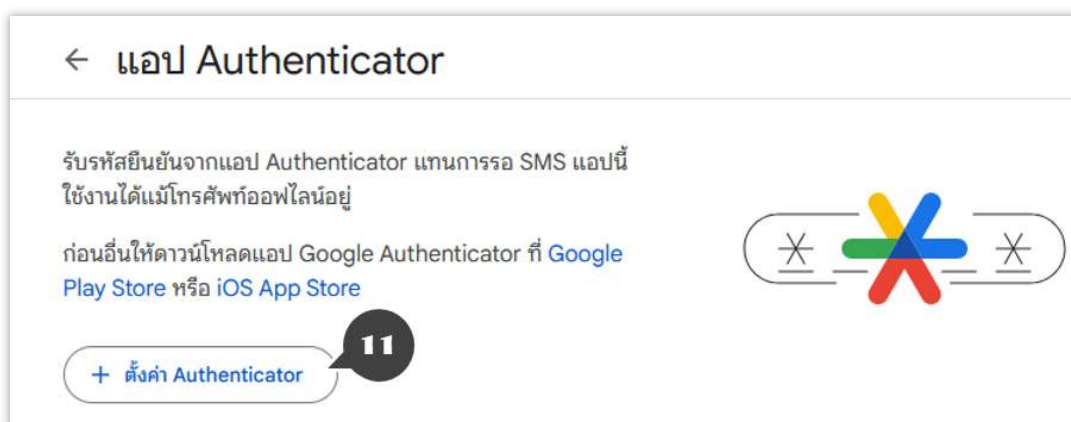
6. ต่อไประบบจะแนะนำให้ติดตั้งโปรแกรม “Google Authenticator” บนโทรศัพท์มือถือของผู้ใช้ (สามารถติดตั้งได้ทั้งบนระบบปฏิบัติการ Android และ iOS)

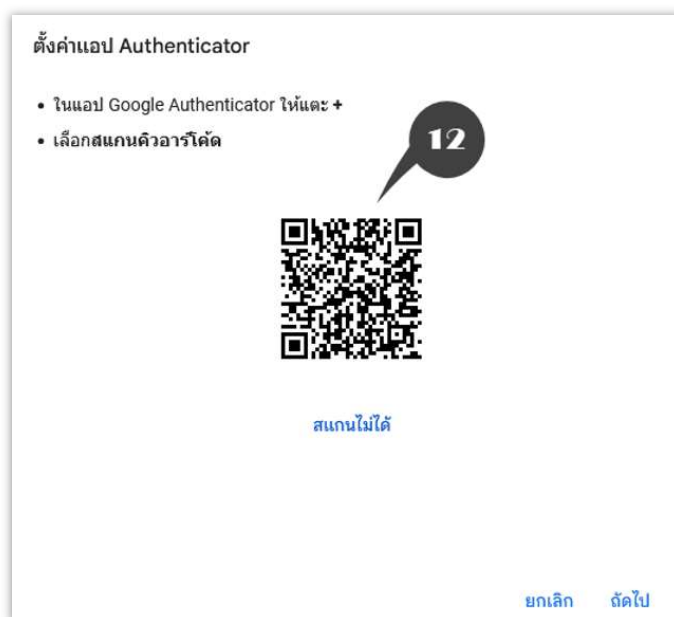


7. บนโทรศัพท์มือถือของผู้ใช้ให้ค้นหาโปรแกรม “Google Authenticator” ใน Play Store แล้วกดปุ่ม “ติดตั้ง”

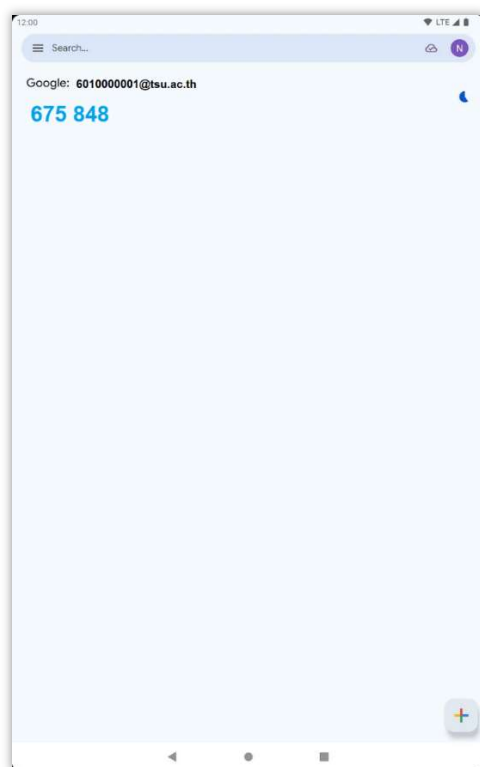


8. เมื่อติดตั้งโปรแกรม “Google Authenticator” บนโทรศัพท์เสร็จแล้ว ให้กลับไปหน้าเว็บไซต์ระบบอีเมลอีกครั้ง ซึ่งได้ดำเนินการตั้งค่าถึงข้อที่ 6 ค้างเอาไว้ ให้คลิกที่ปุ่ม “ตั้งค่า Authenticator” ระบบจะสร้าง QR Code ขึ้นมา

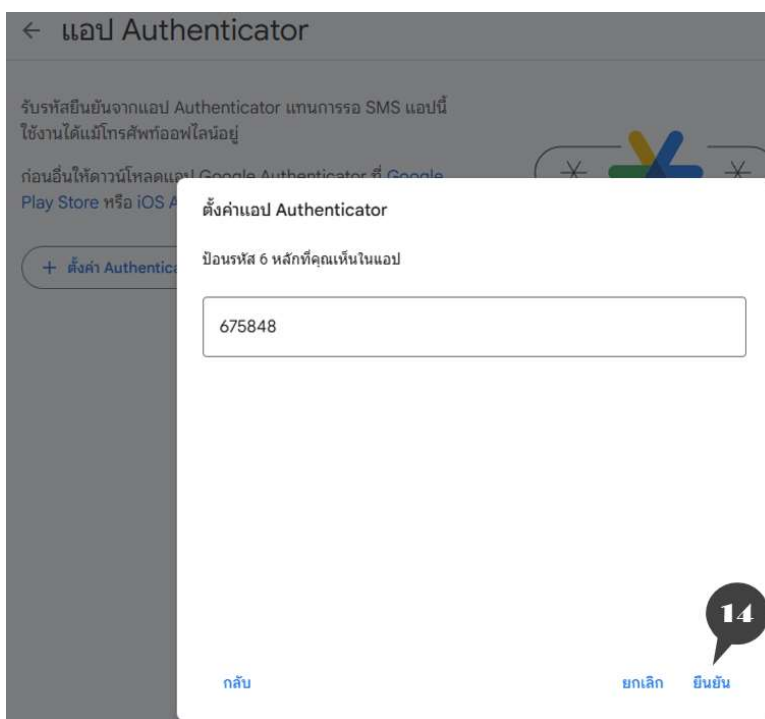
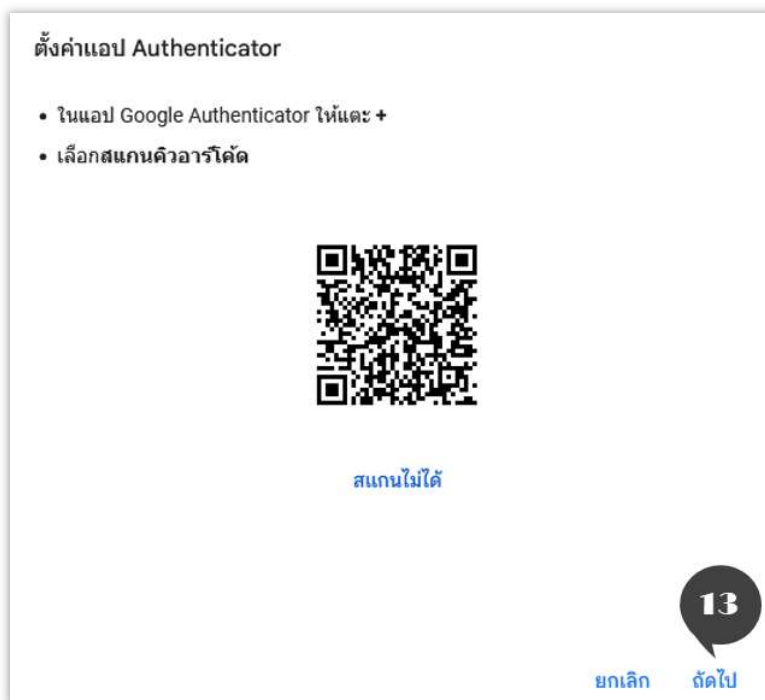




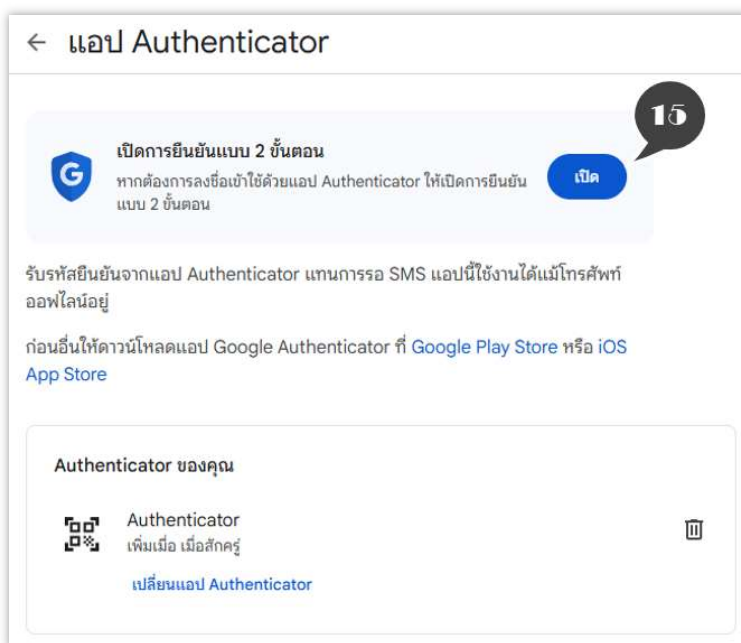
9. บนโทรศัพท์มือถือของผู้ใช้ให้เปิดโปรแกรม “Google Authenticator” แล้วสแกน QR Code ดังกล่าว ซึ่งจะ
ทำให้ได้ชุดตัวเลข 6 หลัก ดังภาพ



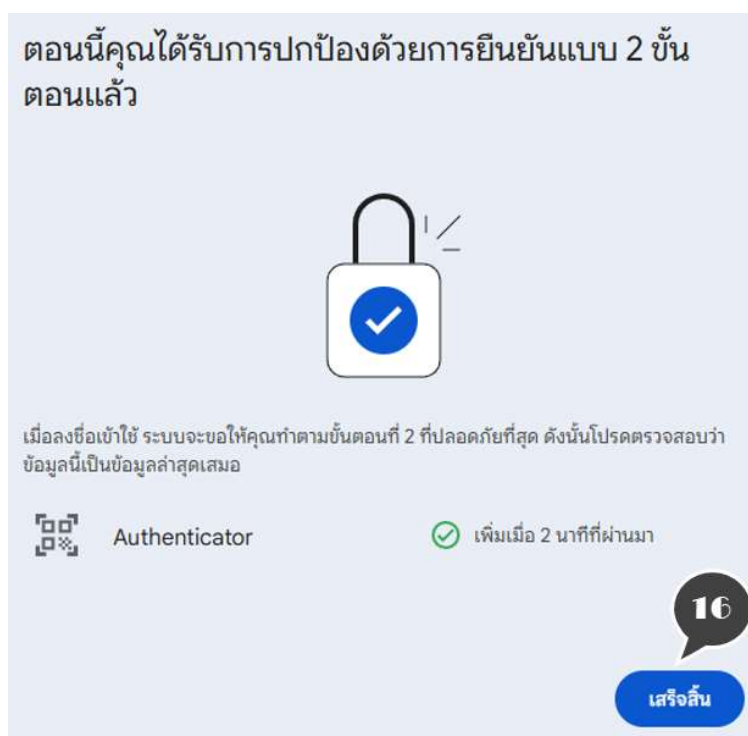
10. กลับมาที่หน้าเว็บไซต์ระบบอีเมลอีกครั้ง ให้คลิกที่ปุ่ม “ถัดไป” แล้วนำรหัส 6 หลักบนโทรศัพท์มือถือกรอกลงไป แล้วกดปุ่ม “ยืนยัน”



11. ให้คลิกที่ปุ่ม “เปิด” เพื่อเปิดการใช้งานแบบ 2 ขั้นตอนด้วย Google Authenticator



12. ระบบจะแสดงข้อความการปกป้องด้วยการยืนยันแบบ 2 ขั้นตอน ให้คลิกที่ “เสร็จสิ้น”



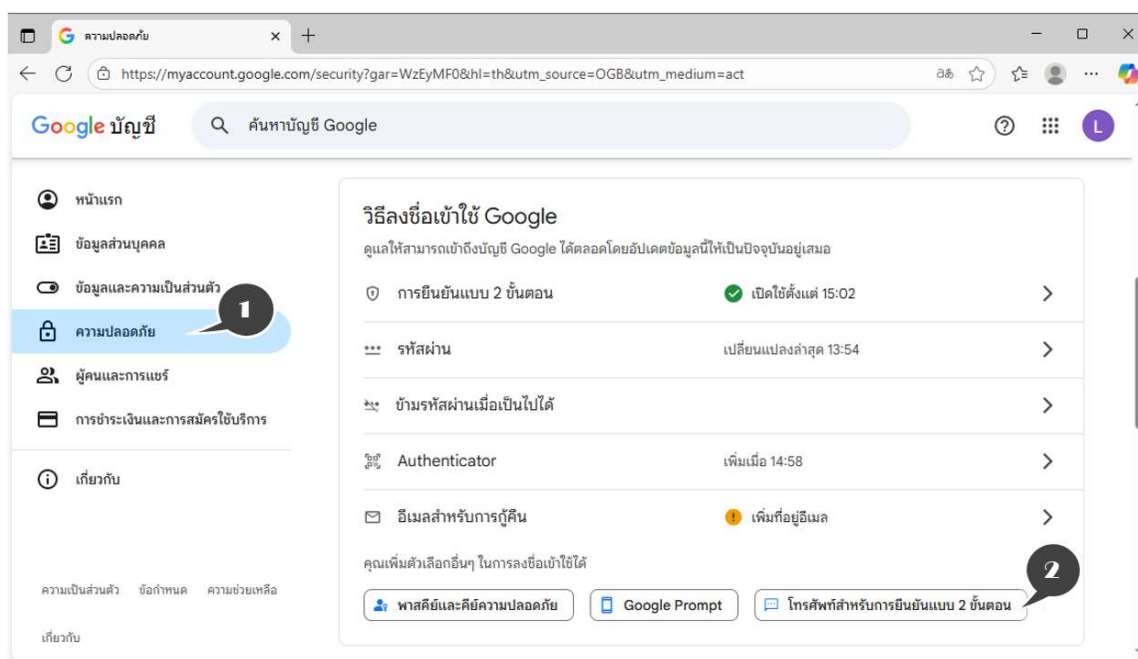
13. จะมีอีเมลส่งถึงผู้ใช้ 1 ฉบับ แจ้งการเปิดการยืนยันแบบ 2 ขั้นตอนแล้ว



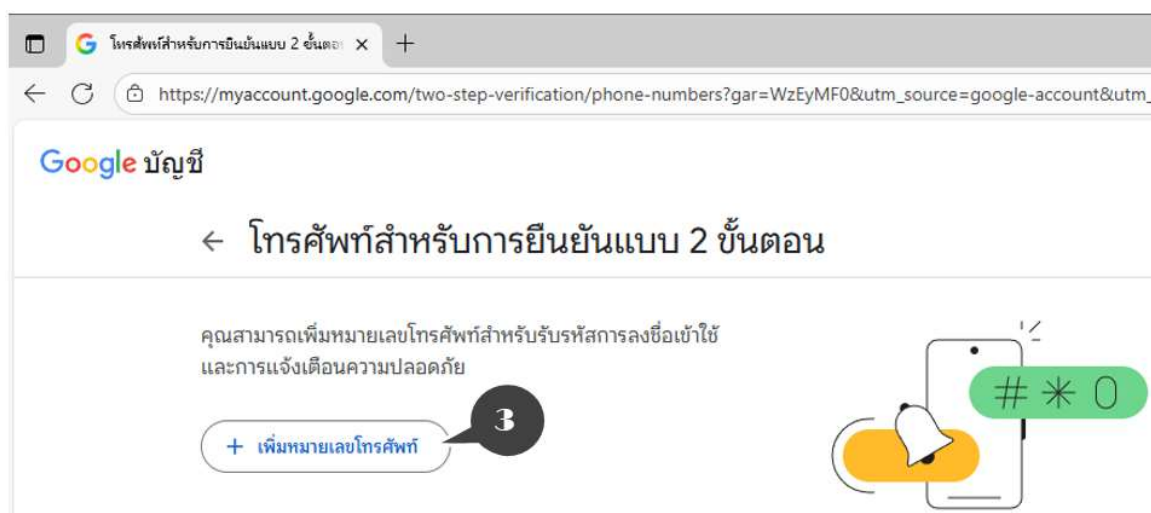
คุณได้รับอีเมลนี้เพื่อแจ้งให้ทราบเกี่ยวกับการเปลี่ยนแปลงสำคัญในบัญชี Google และบริการต่างๆ ของคุณ
© 2025 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

ส่วนที่ 2 การตั้งค่าเบอร์โทรศัพท์มือถือส่วนตัว

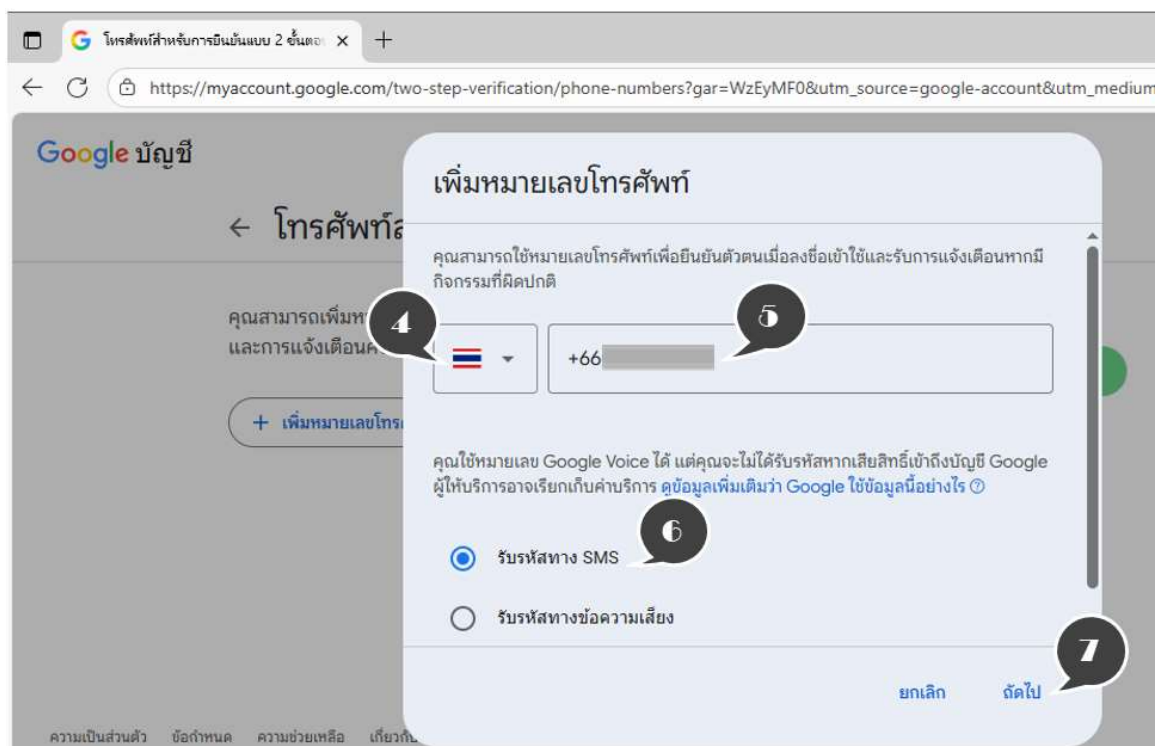
- ต่อไปจะเป็นการใช้เบอร์มือถือในการตั้งค่า 2FA ให้คลิกที่ “รูปโปรไฟล์” มุมบนขวา คลิกที่ “จัดการบัญชี Google” คลิกที่เมนู “ความปลอดภัย” แล้วคลิกที่ “โทรศัพท์สำหรับการยืนยันแบบ 2 ขั้นตอน”



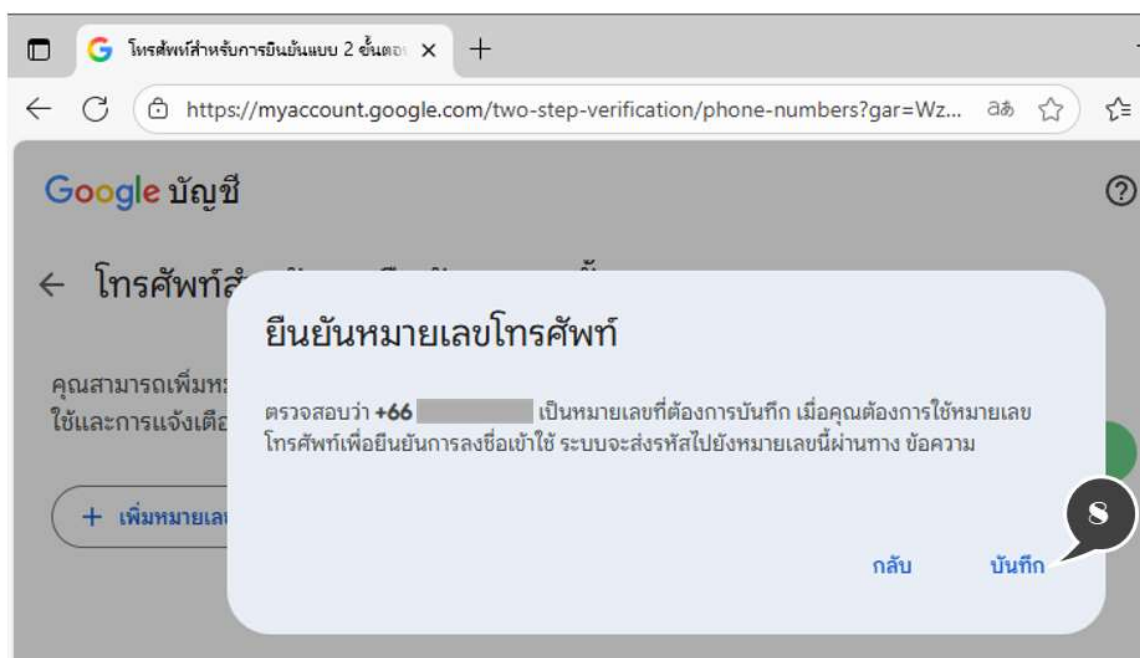
- คลิกที่ “เพิ่มหมายเลขโทรศัพท์”



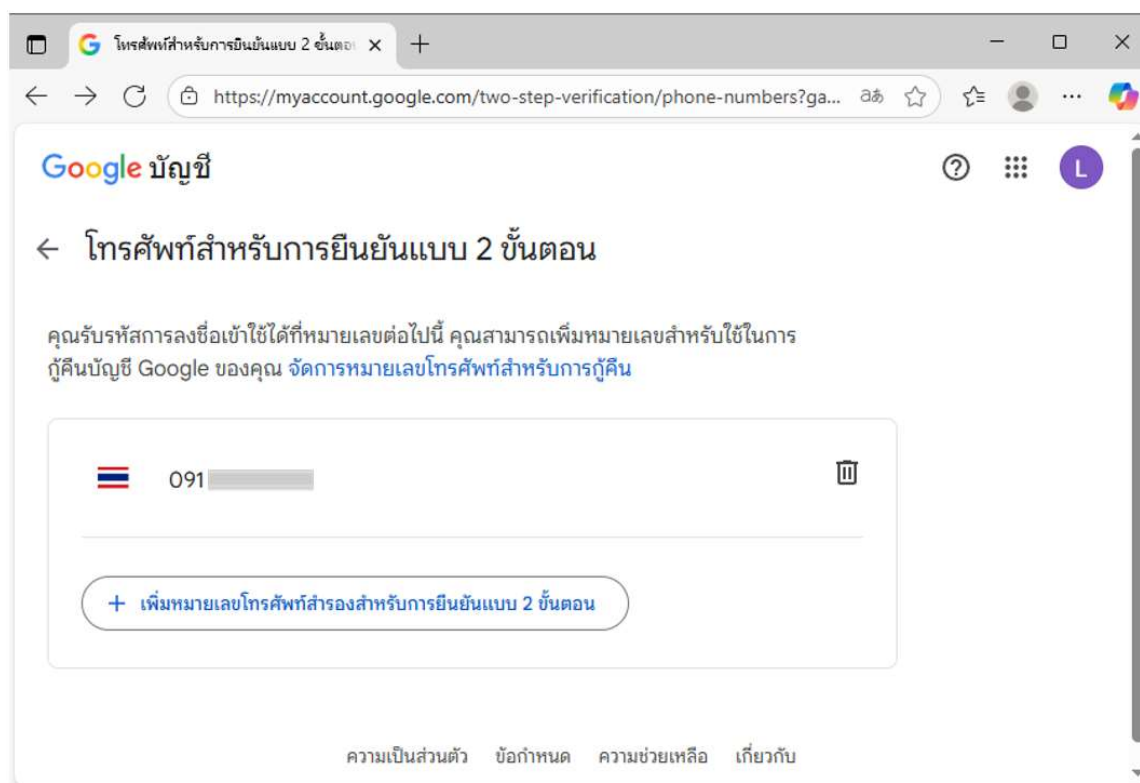
3. คลิกที่รูปธงชาติไทย แล้วกรอกหมายเลขโทรศัพท์ คลิกเลือก “รับรหัสทาง SMS” จากนั้นคลิกที่ “ถัดไป”



4. ตรวจสอบความถูกต้องของหมายเลขโทรศัพท์ที่ได้กรอกไว้ แล้วคลิกที่ “บันทึก”

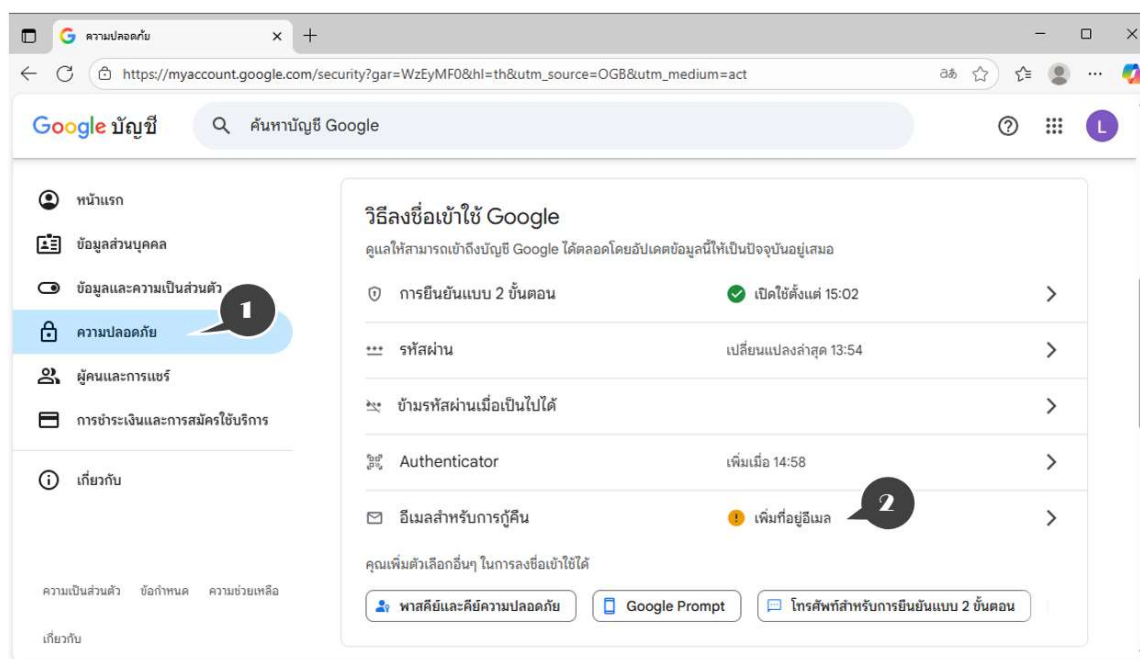


5. เมื่อเสร็จสิ้นขั้นตอนนี้ ระบบจะแสดงหมายเลขโทรศัพท์ส่วนตัวของผู้ใช้ที่ได้ยืนยันสำหรับการยืนยันแบบ 2 ขั้นตอนไว้

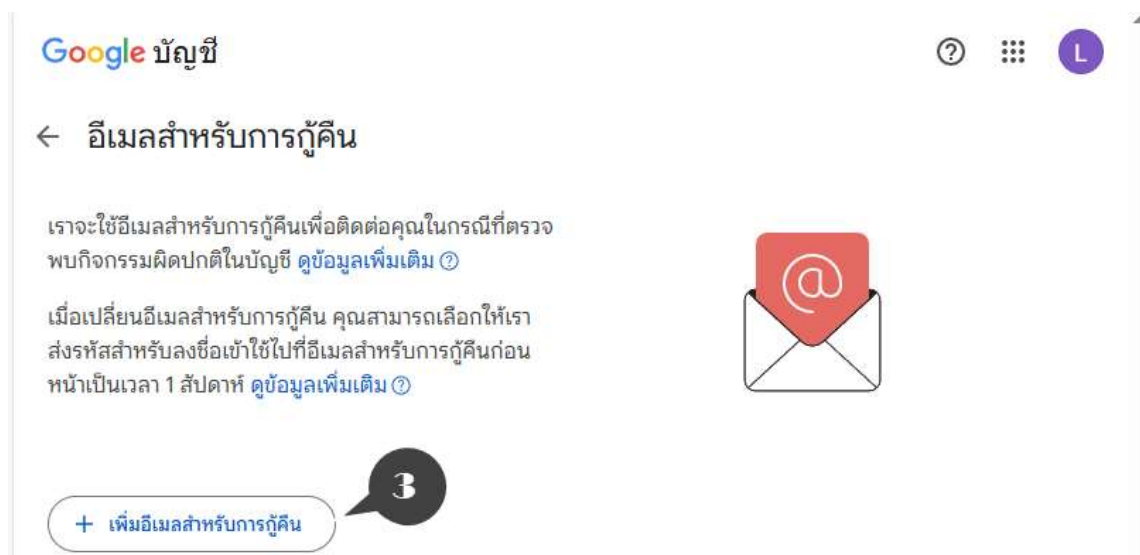


ส่วนที่ 3 การเพิ่มอีเมลส่วนตัวสำหรับการกู้คืน

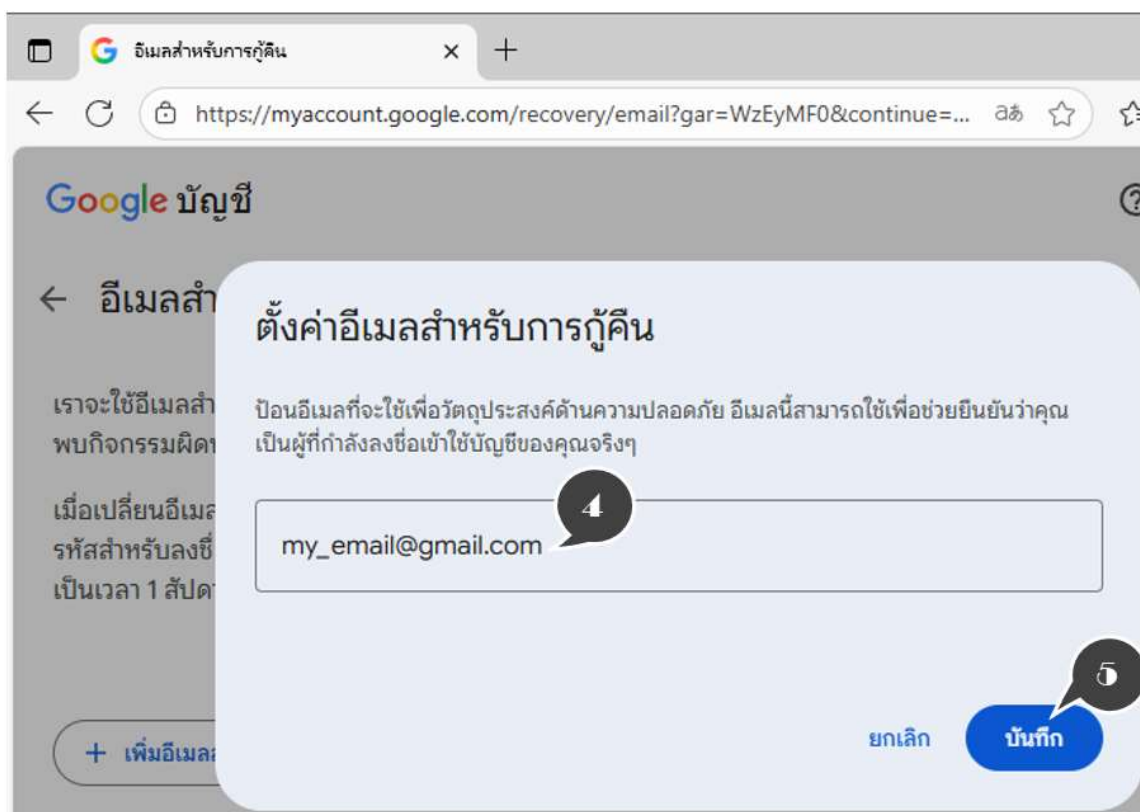
- ต่อไปจะเป็นการใช้อีเมลส่วนตัวของผู้ใช้ในการตั้งค่า 2FA ให้คลิกที่ “รูปโปรไฟล์” มุมบนขวา คลิกที่ “จัดการบัญชี Google” คลิกที่เมนู “ความปลอดภัย” แล้วคลิกที่ “เพิ่มที่อยู่อีเมล”



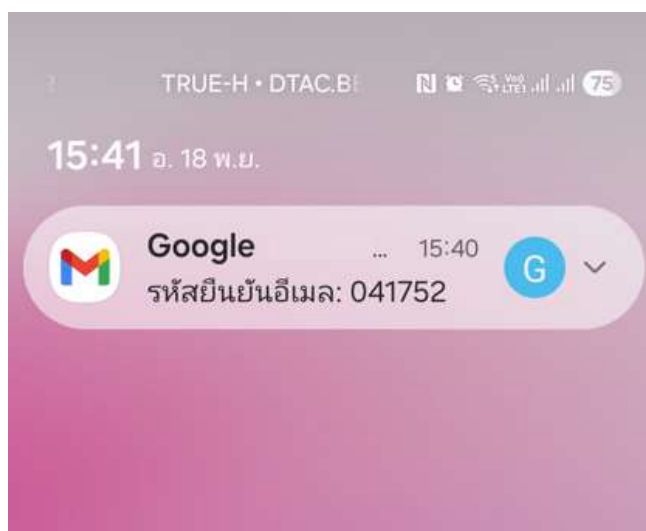
- คลิกที่ “เพิ่มอีเมลสำหรับการกู้คืน”



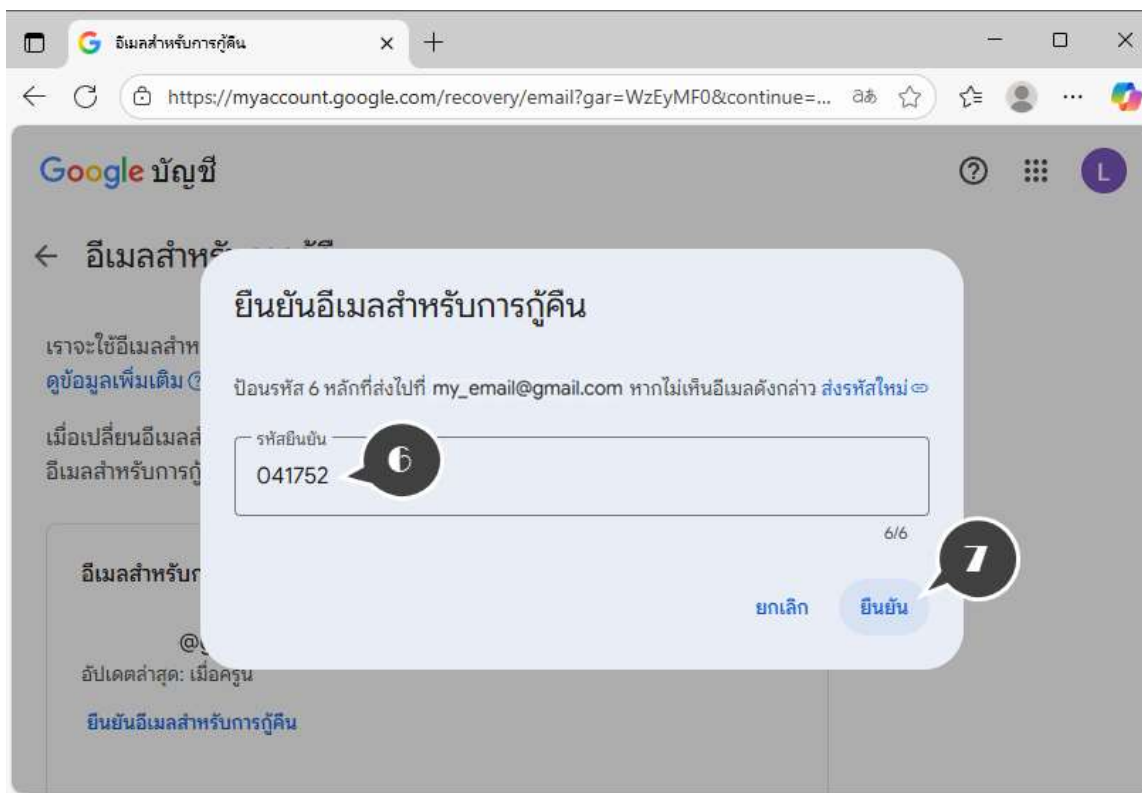
3. กรอกอีเมลส่วนตัว (เช่น อีเมลส่วนตัวที่ใช้สำหรับโทรศัพท์มือถือส่วนตัว) แล้วคลิกที่ “บันทึก”



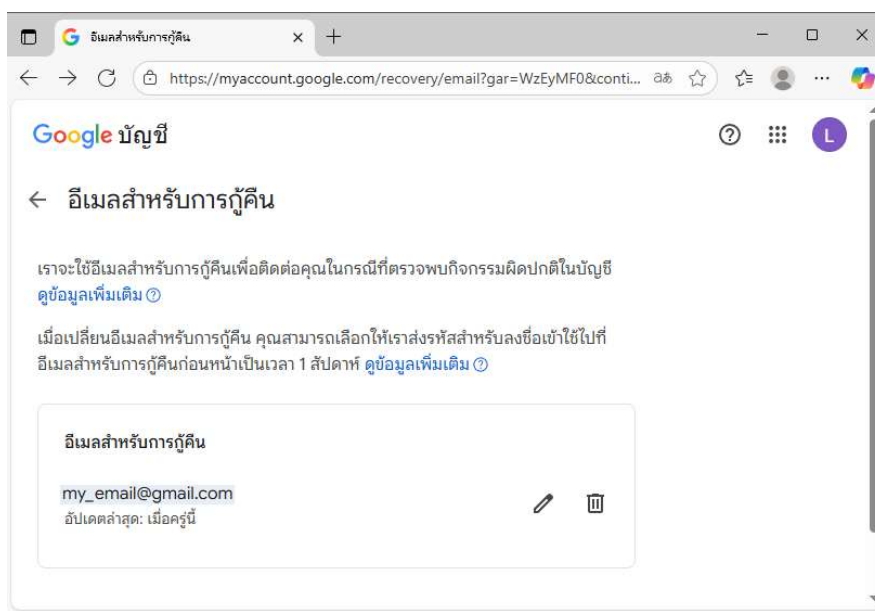
4. จะมีรหัส 6 ส่งถึงผู้ใช้ทางอีเมลส่วนตัวที่ได้ระบุไว้



5. นำรหัส 6 หลักที่ได้รับจากอีเมลมารอกในช่อง “รหัสยืนยัน” แล้วคลิก “ยืนยัน”



6. ระบบจะแสดงข้อมูลการตั้งค่าอีเมลสำหรับการกู้คืนที่ได้กำหนดไว้



7. ภายหลังการตั้งค่า 2FA ครบทั้ง 3 ส่วน เมื่อผู้ใช้คลิกไปที่เมนู “ความปลอดภัย” จะมีสัญลักษณ์ความปลอดภัยปรากฏขึ้นและมีข้อความ “บัญชีของคุณได้รับการปกป้องแล้ว”

