



# ระวังภัยออนไลน์

คำแนะนำในการรักษาความปลอดภัย  
ของบัญชี Payoneer

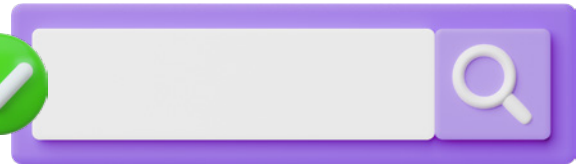




การหลอกลวงข้อมูลทางอินเทอร์เน็ต อาจมาในรูปแบบของอีเมลที่น่าเชื่อถือ ข้อความ SMS หรือเว็บไซต์ที่หลอกลวงโดยมีลักษณะเหมือนกับ Payoneer อย่างมีนัยสำคัญ โดยมีเป้าหมายที่จะหลอกลวงคุณให้แจ้งรายละเอียดส่วนตัวเกี่ยวกับบัญชี หมายเลขบัตร รหัสผ่าน หรือ OTP ของคุณ เพื่อป้องกันไม่ให้พลาดพลัง เราขอเสนอเคล็ดลับเหล่านี้เพื่อความปลอดภัยในการใช้งานบัญชีของคุณ

## การรักษาความปลอดภัยของบัญชี Payoneer

ระวัง URL อันตรายที่แอบอ้างแสดงตัวเป็นเว็บไซต์ทางการ และอาจถูกเพิ่มเข้าไปในผลการค้นหาของ Google เพื่อหลอกลวงคุณให้แบ่งปันรายละเอียดโดยที่คุณไม่รู้ตัว



### ข้อควรระวังเพื่อป้องกันบัญชีของคุณจาก URL ปลอม

- ตรวจสอบความผิดพลาดในการสะกดคำ

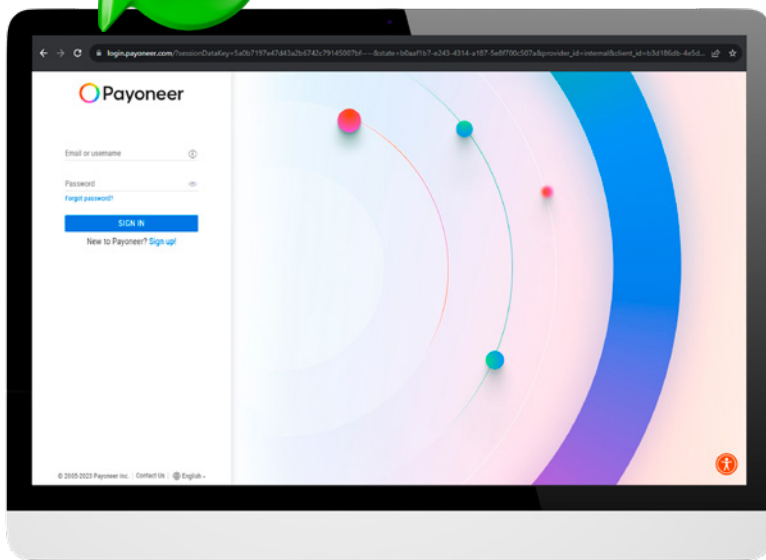
หากพบว่ามี ความผิดพลาดในการสะกดคำหรือคำที่ไม่คุ้นเคยใน URL ของ Payoneer ให้ออกจากเว็บไซต์ทันที เช่น

www.payoneen.com  
www.payqneer.com  
www.PayoneerIsAlwaysTheBest.com  
www.radiostation4payoneer.co.uk



- ตรวจสอบสัญลักษณ์ลึกลับ

สัญลักษณ์ลึกลับที่ปรากฏในแถบที่อยู่ URL จะช่วยบ่งชี้ว่าเว็บไซต์ที่คุณกำลังเยี่ยมชมเป็นปลอดภัย



- เลี่ยงการคลิกลิงก์บน Google เพื่อเข้าบัญชี

บุคมาค์เว็บไซต์หน้าเข้าสู่ระบบ Payoneer หรือใช้แอป Payoneer เพื่อเข้าสู่บัญชีโดยตรง เพื่อให้มั่นใจว่าลิงก์ที่เข้าไปเป็นลิงก์ที่ถูกต้อง โดยเฉพาะเมื่อเข้าระบบทางมือถือ เพราะไม่สามารถเห็น URL ได้ครบถ้วน

- เปิดใช้งาน Multi-Factor Authentication (MFA)

ระบบความปลอดภัยเพิ่มเติมมีส่วนช่วยป้องกันการหลอกลวงข้อมูลทางอินเทอร์เน็ต

- จัดการรหัสผ่านของคุณ

เปลี่ยนรหัสผ่านเป็นประจำทุก 6 เดือน และหลีกเลี่ยงการใช้รหัสเดียวกันในหลายแพลตฟอร์ม



# การหลอกลวงข้อมูลทางอินเทอร์เน็ตผ่านอีเมลและ SMS

การโจรกรรมออนไลน์อาจมาในรูปแบบของอีเมลหรือ SMS มาดูวิธีการตรวจสอบเบื้องต้นเพื่อรักษาความปลอดภัยบัญชี

- **ตรวจสอบอีเมลของผู้ส่งว่าถูกต้องหรือไม่**

ตรวจสอบว่าผู้ส่งมาจาก "@payoneer.com" เท่านั้น และต้องสะกดอย่างถูกต้อง

- **ตรวจสอบการหักทวงและรูปแบบคำขิ้นต้น**

การติดต่อของ Payoneer เราจะหักทวงคุณด้วยชื่อ ตามที่ระบุ "ไว้ในระบบ แทนที่จะเป็นการหักทวงโดยรวม เช่น "เรียน คุณลูกค้า"

- **สำรวจข้อผิดพลาดทางไวยากรณ์หรือการสะกดคำผิด**

การติดต่อที่ถูกต้องจาก Payoneer จะมีการตรวจสอบอย่างเคร่งครัด นั้นหมายความว่าข้อผิดพลาดทางไวยากรณ์มักจะไม่มีเกิดขึ้น

- **อย่ารีบคลิกในกรณีพบลิงก์ที่น่าสงสัย**

ให้นำเมาส์ไปวางที่ลิงก์ก่อนที่จะคลิกเพื่อตรวจสอบ URL ปลายทางของพวกเขา

- **อย่าเปิดเผยข้อมูลที่เป็นสาระสำคัญ**

อย่าแจ้งรายละเอียดที่สำคัญ เช่น หมายเลขบัตร หรือรหัสผ่านของคุณ ให้กับบุคคลอื่น

- **ระวังการเปิดไฟล์แนบ**

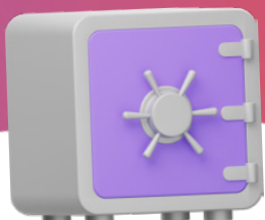
เปิดเฉพาะไฟล์แนบที่คุณคาดหวังเพื่อหลีกเลี่ยง Spyware หรือไวรัส



## ควรทำอย่างไรหากคุณพบการหลอกลวงข้อมูลทางอินเทอร์เน็ต?

หากคุณสงสัยว่าคุณพบการพยายามหลอกลวงข้อมูล

- 1 อย่าเข้าสู่ระบบ และห้ามคลิกเปิดลิงก์หรือไฟล์แนบ
- 2 ถ่ายรูปหน้าจอให้เห็นเว็บไซต์หรือข้อความ แล้วส่งมาที่ [reportaproblem@payoneer.com](mailto:reportaproblem@payoneer.com)
- 3 ปิดแท็บที่มี URL ที่เป็นอันตรายหรือลบอีเมล/ SMS ที่น่าสงสัย



# หากคุณสงสัยว่าบัญชีของคุณถูกโจรกรรม

ติดต่อฝ่ายบริการลูกค้าให้เร็วที่สุดเพื่อระงับการใช้งาน ป้องกันความเสียหาย  
ที่ทีมงานของเราจะแนะนำขั้นตอนที่จำเป็นเพื่อรักษาความปลอดภัยบัญชี

## ศูนย์บริการลูกค้า



<https://paynr.co/387D8M4>

## เบอร์โทรติดต่อ

060-003-5396

02-026-8178

ภาษาอังกฤษให้บริการตลอด 24 ชั่วโมง

ภาษาไทยให้บริการในวันทำการ จ - ศ 9.00 -16.00น.

