

[ออกแบบมาเพื่อความปลอดภัยยิ่งขึ้น](#) > [เคล็ดลับความปลอดภัย](#)



เคล็ดลับและเครื่องมือ ที่จะช่วยให้คุณปลอดภัยบนโลก ออนไลน์อยู่เสมอ

นอกจากการป้องกันอัตโนมัติที่มีอยู่ในผลิตภัณฑ์ของเราแล้ว ต่อไปนี้
คือเคล็ดลับเพิ่มเติมที่จะช่วยให้คุณหลีกเลี่ยงการหลอกลวงทาง
ออนไลน์และลงชื่อเข้าใช้แอปและอุปกรณ์ได้อย่างปลอดภัย

การหลีกเลี่ยงการหลอกลวง

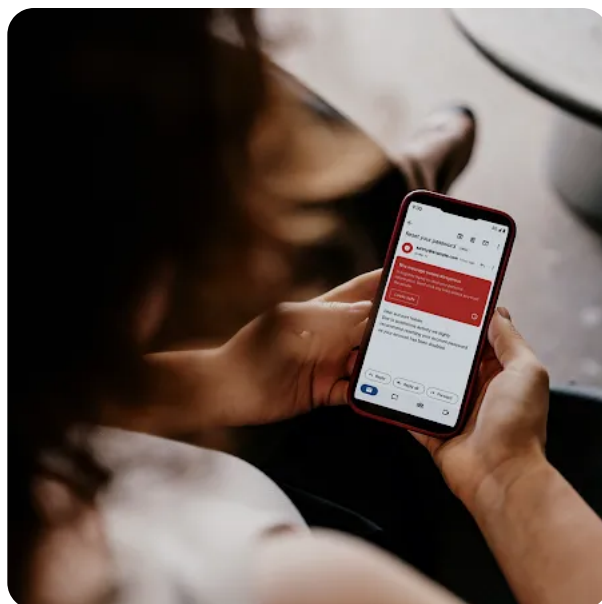
เคล็ดลับการลงชื่อเข้าใช้

ความปลอดภัยของอุปกรณ์

ความปลอดภัยบนเว็บ

หลีกเลี่ยงการหลอกลวงทางออนไลน์ และการพยายามฟิชชิง

การหลอกลวงทางออนไลน์และความพยายามในการฟิชชิงออกแบบมาเพื่อหลอกลวงให้ผู้ใช้ที่หลงเชื่อเปิดเผยข้อมูลส่วนบุคคลหรือข้อมูลทางการเงิน ซึ่งนับวันจะเพิ่มจำนวนขึ้นเรื่อยๆ หนึ่งในปรการด้านแรกที่ดีที่สุดคือการรู้ว่าต้องมองหาอะไร



การสังเกตการหลอกลวงทางอีเมล

วิธีที่ง่ายที่สุดในการหลีกเลี่ยงการหลอกลวงทางอีเมลคือการใช้ระบบป้องกันที่มีอยู่ใน Gmail แต่ไม่ว่าคุณจะใช้แพลตฟอร์มไหน นี่คือสิ่งที่คุณควรระวังเมื่อได้รับอีเมล

1. ระวังอีเมลจากคนแปลกหน้า
2. คิดให้รอบคอบก่อนทำตามคำขอเร่งด่วน
3. ตรวจสอบอีเมลของผู้ส่ง
4. ตรวจสอบโดเมนที่คล้ายกัน
5. เลื่อนเคอร์เซอร์วางเหนือลิงก์ก่อนคลิก
6. ไม่ดำเนินการใดๆ กับการรีเชิตรหัสผ่านที่คุณไม่ได้ส่ง

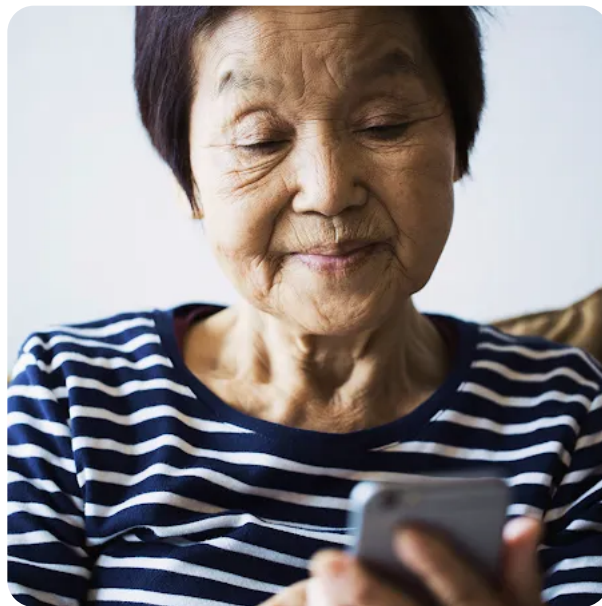
ดูข้อมูลเพิ่มเติม



การสังเกตการหลอกลวงทางโทรศัพท์และข้อความ

คนจำนวนมากขึ้นได้รับสายและ SMS ไม่พึงประสงค์ที่ขอข้อมูลส่วนบุคคลของตน โปรดจำไว้เสมอว่า Google จะไม่มีทางโทรหาคุณเรื่องบัญชี

1. ถามคำถามจำนวนมาก
2. อย่าคลิกลิงก์ที่ส่งผ่านข้อความ
3. อย่าแชร์ข้อมูลเข้าสู่ระบบชั่วคราว
4. หลีกเลี่ยงคำขอเร่งด่วนจากผู้โทร
5. ฟังคำเตือนจากระบบป้องกันที่มีให้



การสังเกตการหลอกลวงบนเว็บ

ในการรักษาความปลอดภัยให้คุณบน Search เรามี [นโยบายที่เข้มงวด](#) และระบบการต่อสู้กับสแปมขั้นสูงที่ช่วยให้ Search ปลอดภัยได้ถึง 99% และช่วยต่อสู้กับความพยายามของสแกมเมอร์ที่จะหลอกลวงผู้คน สำหรับโฆษณา เราจะใช้ AI เพื่อปกป้อง [ผู้ใช้จากการฉ้อโกง](#) และเพื่อตรวจจับอาชญากรไซเบอร์และ [สแกมเมอร์](#) ต่อไปนี้คือเคล็ดลับเพิ่มเติม 6 ข้อเพื่อความปลอดภัย

1. หากไม่แน่ใจ ให้ดูข้อมูลเพิ่มเติมเกี่ยวกับโฆษณาและผู้สร้างโฆษณา
2. ตรวจสอบ URL ก่อนคลิกลิงก์ที่ไม่คุ้นเคย
3. [จับภาพหน้าจอ](#) ข้อความที่น่าสงสัยและอัปโหลดไปยัง Google Search ผ่าน Lens หรือพีเจอาร์ลิงก์เพื่อค้นหาเพื่อวิเคราะห์
4. รวบรวมข้อมูลเชิงลึกเกี่ยวกับหน้าเว็บ ร้านค้า หรือธุรกิจโดยใช้ [เครื่องมือ "เกี่ยวกับผลการค้นหา"](#)
5. มองหาแหล่งข้อมูลที่เป็นทางการและระวังการจัดรูปแบบที่ผิดปกติ
6. หากคุณเป็นธุรกิจ ให้ [แสดงช่องทางการสนับสนุนลูกค้าให้ชัดเจน](#) บน Search โดยตรง

การหลอกลวง 6 รูปแบบที่พบบ่อย และวิธี ป้องกันตัวเองจากการหลอกลวงเหล่านี้

การหลอกลวงทางออนไลน์มีจำนวนมากขึ้นและซับซ้อนขึ้น ทีมความน่าเชื่อถือและความปลอดภัย (T&S) ของ Google มีหน้าที่ติดตามและต่อสู้กับการหลอกลวง รวมถึงแฮกซ์ข้อสังเกตและข้อมูลที่เรารวบรวมมาเพื่อช่วยให้คุณปลอดภัยยิ่งขึ้น ทำความคุ้นเคยกับการหลอกลวงเหล่านี้เพื่อหลีกเลี่ยงไม่ให้ตกเป็นเหยื่อ

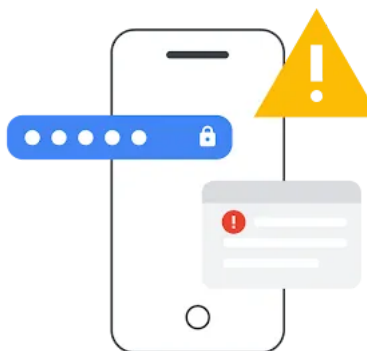
1. การแสวงหาประโยชน์จากเหตุการณ์สำคัญๆ

เคล็ดลับด้านความปลอดภัย: ในช่วงเหตุการณ์สำคัญ ให้ซื้อหรือบริจาคผ่านแพลตฟอร์มที่เชื่อถือได้และผู้จัดงานอย่างเป็นทางการเท่านั้น

การผสมผสานเทคโนโลยีใหม่และเทคโนโลยีที่กำลังมาแรงเข้ากับเทคนิคการหลอกลวงแบบดั้งเดิมทำให้ผู้ไม่ประสงค์ดีสามารถตอบสนองต่อข่าวฉ้อโกงและเหตุการณ์สำคัญได้อย่างรวดเร็ว ทำให้แผนการของตนดูน่าเชื่อถือมากขึ้น

มีงานวิจัยในช่วงเกิดเหตุการณ์สำคัญ ผู้คนมักรู้สึกกดดันให้ต้องรีบดำเนินการ ไม่ว่าจะเป็นการจองตั๋วเครื่องบินที่ได้รับความนิยมสูง การซื้อสินค้าจำนวนจำกัด หรือการช่วยเหลือผู้ประสบภัย และมีงานวิจัยที่ใช้ความรู้เชิงแรงกดดันนี้ให้เป็นประโยชน์

Google มีนโยบายเกี่ยวกับเหตุการณ์ที่ละเอียดอ่อนโดยเฉพาะ ซึ่งรวมถึง [โฆษณา](#) และ [Shopping](#) การสร้างรายได้ใน [YouTube](#) และ [Google Play](#) นโยบายเหล่านี้ห้ามสินค้าหรือบริการที่แสวงหาประโยชน์ ละเลย หรือสนับสนุนเหตุการณ์ที่มีความละเอียดอ่อน และใช้การตรวจสอบที่เข้มงวดขึ้นเพื่อช่วยให้คุณปลอดภัยยิ่งขึ้นในช่วงเหตุการณ์สำคัญ



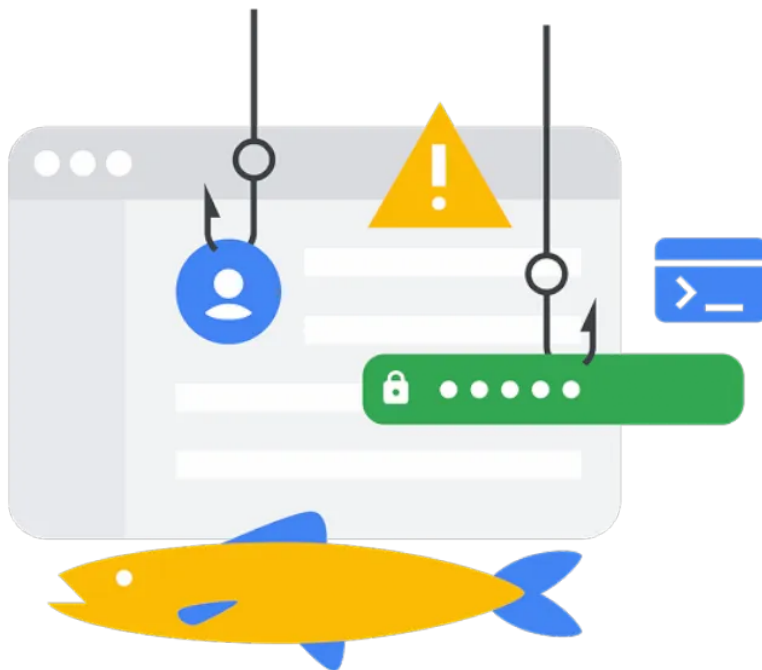
2. การหลอกลวงให้ลงทุนโดยใช้คนที่ AI สร้างขึ้น

3. การหลอกลวงด้านการท่องเที่ยวและอีคอมเมิร์ซปลอม

4. การประพฤติมิชอบโดยแอบอ้างเป็นฝ่ายสนับสนุนด้านเทคนิคเกี่ยวกับการเข้าถึงระยะไกล

5. การหลอกลวงเรื่องงาน

6. แอปพลิเคชันที่แสวงหาประโยชน์จากผู้อื่น



ทดสอบทักษะการสังเกตการหลอกลวงทางอินเทอร์เน็ต

AI กำลังทำให้การโจมตีแบบฟิชชิงซับซ้อน ปรับเปลี่ยนเฉพาะบุคคล และเกิดบ่อยขึ้น ดังนั้น การสังเกตว่าอะไรจริงอะไรปลอมจึงไม่ใช่เรื่องง่ายอย่างที่เห็นเสมอไป คุณสามารถทดสอบความรู้เรื่องการสังเกตการหลอกลวงทางอินเทอร์เน็ตได้ด้วยแบบทดสอบความรู้เท่าทันอีเมลฟิชชิงที่พัฒนาโดย [Jigsaw](#) ซึ่งเป็นหน่วยงานหนึ่งของ Google แครแบบทดสอบนี้กับเพื่อนๆ และครอบครัวเพื่อช่วยให้พวกเขาปลอดภัยยิ่งขึ้นบนโลกออนไลน์

ทำแบบทดสอบ

ต่อสู้กับการหลอกลวงและการประพฤติมิชอบทุกวัน

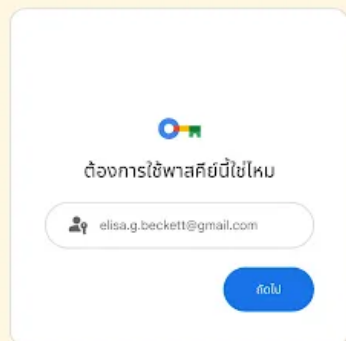
ดูรายละเอียดเกี่ยวกับวิธีที่ระบบรักษาความปลอดภัยในตัวของเราปกป้องคุณจากการหลอกลวงและการประพฤติมิชอบทางออนไลน์

ไปที่การหลอกลวงและการประพฤติมิชอบ

วิธีทำให้ การลงชื่อเข้าใช้ปลอดภัยยิ่งขึ้น

การลงชื่อเข้าใช้บัญชีออนไลน์เป็นหนึ่งในความเสี่ยงด้านความปลอดภัยที่สำคัญที่สุดในปัจจุบัน โดยมีรหัสผ่านเป็นล้านรายการที่ถูกเปิดเผยจากการละเมิดข้อมูลในทุกๆ วัน เครื่องมือการตรวจสอบสิทธิ์และรหัสผ่านของเราออกแบบมาเพื่อช่วยให้คุณลงชื่อเข้าใช้ในแอปและบริการที่ชื่นชอบได้อย่างรวดเร็วและปลอดภัย

ดูข้อมูลเพิ่มเติมเกี่ยวกับการตรวจสอบสิทธิ์



การลงชื่อเข้าใช้ที่ง่ายและปลอดภัยโดยไม่ต้องกรอกรหัสผ่าน

[พาสคีย์](#) มอบวิธีการลงชื่อเข้าใช้ที่ง่ายและปลอดภัยที่สุด โดยใช้การล็อกหน้าจอของอุปกรณ์ เพียงแค่คุณมองโทรศัพท์หรือสแกนลายนิ้วมือ ก็ลงชื่อเข้าใช้ได้เลย พาสคีย์ใช้โปรโตคอลวิทยาการเข้ารหัสคีย์สาธารณะแบบเดียวกับที่ใช้ในอุปกรณ์เพื่อความปลอดภัยตามมาตรฐานของ FIDO Alliance และ W3C จึงทำให้สามารถรับมือกับฟิชซิง การสวมข้อมูลเข้าสู่ระบบ และการโจมตีระยะไกลรูปแบบอื่นๆ ได้

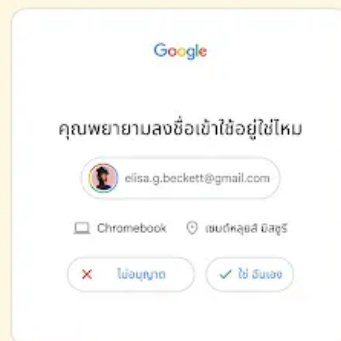
[ดูข้อมูลเพิ่มเติม](#)



ลงชื่อเข้าใช้น้อยครั้งลง บัญชีปลอดภัยยิ่งขึ้น

วิธีการลงชื่อเข้าใช้ผ่านโซเชียล เช่น [พีเจอาร์](#) [ลงชื่อเข้าใช้ด้วย Google](#) ช่วยให้คุณลงชื่อสมัครใช้และลงชื่อเข้าใช้แอปและเว็บไซต์หลายพันรายการได้โดยไม่ต้องใช้ชื่อผู้ใช้และรหัสผ่านที่ไม่ซ้ำกัน คุณจึงมีข้อมูลเข้าสู่ระบบที่จัดเก็บไว้ทางออนไลน์น้อยลงและข้อมูลของคุณจะปลอดภัยยิ่งขึ้น

[ดูข้อมูลเพิ่มเติม](#)



ป้องกันตัวเองจากแฮกเกอร์ด้วยการยืนยันแบบ 2 ขั้นตอน

[การยืนยันแบบ 2 ขั้นตอน](#) ช่วยปกป้องบัญชีของคุณจากการใช้งานของบุคคลที่ไม่มีสิทธิ์ โดยกำหนดให้คุณใช้กระบวนการตรวจสอบสิทธิ์ที่ 2 นอกเหนือจากชื่อผู้ใช้และรหัสผ่านในการลงชื่อเข้าใช้บัญชีของคุณ

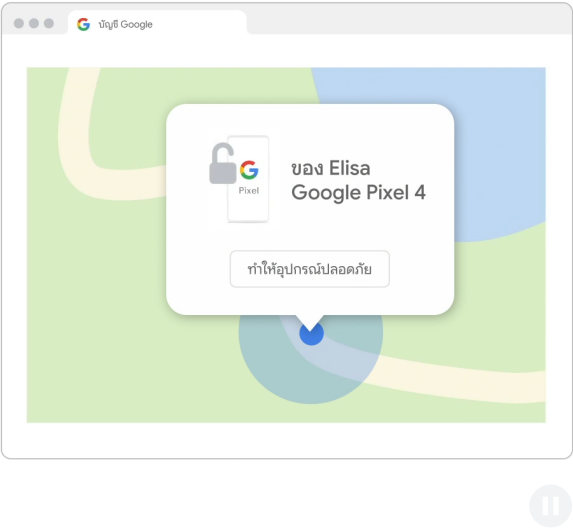
[ดูข้อมูลเพิ่มเติม](#)



ทำให้ อุปกรณ์ของคุณปลอดภัยอยู่เสมอ



หากโทรศัพท์สูญหายหรือถูกขโมย ให้เข้าไปที่บัญชี Google ของคุณ แล้วเลือก "หาโทรศัพท์ของคุณ" เพื่อปกป้องข้อมูลในไม่กี่ขั้นตอน ไม่ว่าจะใช้อุปกรณ์ Android หรือ iOS คุณก็ค้นหาและล็อกโทรศัพท์จากระยะไกลได้เพื่อไม่ให้ผู้อื่นใช้โทรศัพท์หรือเข้าถึงข้อมูลส่วนบุคคลของคุณ



ดูแลให้ซอฟต์แวร์อัปเดตอยู่เสมอ



บล็อกแอปที่อาจเป็นอันตรายในโทรศัพท์



ใช้ล็อกหน้าจอ



ท่องเว็บ อย่างปลอดภัย

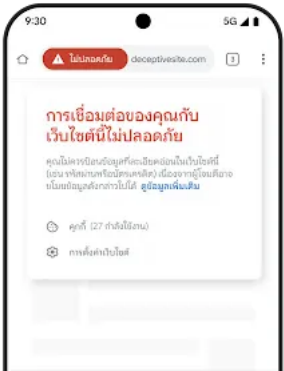
ขยายทั้งหมด

ใช้เครือข่ายที่ปลอดภัย



ระวังเรื่องการใช้ Wi-Fi สาธารณะหรือ Wi-Fi ฟรีแม้จะต้องใช้รหัสผ่าน เครือข่ายเหล่านี้อาจไม่มีการเข้ารหัส ดังนั้น เมื่อคุณเชื่อมต่อกับเครือข่ายสาธารณะบุคคลในบริเวณใกล้เคียงอาจติดตามดูกิจกรรมในอินเทอร์เน็ตของคุณได้ รวมถึงเว็บไซต์ที่คุณเข้าชมและข้อมูลที่คุณพิมพ์ในนั้นด้วย หากจำเป็นต้องใช้ Wi-Fi สาธารณะหรือ Wi-Fi ฟรี โปรดดูแถบที่อยู่ของเบราว์เซอร์ Chrome ซึ่งจะแจ้งหากการเชื่อมต่อเว็บไซต์นั้นไม่ปลอดภัย

[รับชมวิดีโอ](#) เพื่อข้อมูลเพิ่มเติมเกี่ยวกับความสำคัญของการใช้การเชื่อมต่อ Wi-Fi ที่ปลอดภัย และเคล็ดลับสำหรับวิธีทำให้เครือข่าย Wi-Fi ของคุณปลอดภัย



[ตรวจสอบว่าการเชื่อมต่อที่ปลอดภัยก่อนจะป้อนข้อมูลที่ละเอียดอ่อน](#)

[ความแม่นยำของตำแหน่งของ Google](#)

ดูวิธีอื่นๆ ที่จะช่วยทำให้บัญชีของคุณปลอดภัยอยู่เสมอ

ไปที่การตั้งค่าความปลอดภัย

ติดตามเรา     

ไซต์ที่เกี่ยวข้อง

ครอบครัว

ศูนย์ความปลอดภัย