

# Cyber Safety

คุณมีรูเท่ากันมิจาชีพและวิธี  
ป้องกันตัวในโลกออนไลน์

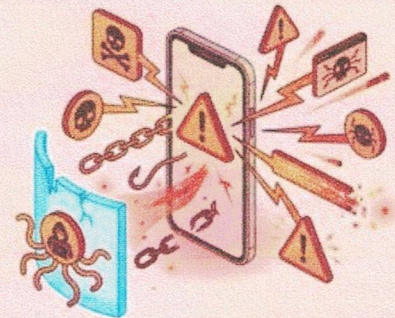
เช็กให้ชัวร์ กลัวให้เป็น  
ปลอดภัยบนโลกไซเบอร์



ฟอ.ส. นก.อก. นร.ตชช.

© NotebookLM

ภัยเงียบในมือคุณ: มิจาชีพไม่ได้มาเคาะประตูบ้านอีกต่อไป



**การโจมตีรูปแบบใหม่**

แฝงตัวมาในรูปแบบของข้อความ  
ส.า.ไกรศัพท์ หรือสิ่งกัที่ดูเหมือนจริงที่สุด

**เป้าหมายคือทุกคน**

ไม่ใช่แค่ผู้สูงอายุ  
แต่วัยทำงานและเยาวชนก็ตกเป็นเหยื่อ  
ความเสียหายพุ่งสูงขึ้นทุกปี

**เป้าหมายของคุณนี่**

เพื่อเป็นเกราะป้องกันให้คุณและ  
ครอบครัวไม่ตกเป็นเหยื่อรายต่อไป

© NotebookLM

## 5 รูปแบบกลโกงยอดฮิตของมิจฉาชีพ



## โจมตีด้วย ความกลัว ให้คุณขาดสติ



## ล่อลวงด้วย ความโลภและความรัก



### Investment Scam (หลอกลงทุน)

ชวนลงทุนคริปโตหรือหุ้น ชูจุดขาย  
รวดเร็ว ง่ายง่าย ได้เงินจริง  
ผลตอบแทนสูงเกินจริง



### Romance Scam (หลอกรักออนไลน์)

สร้างโปรไฟล์ปลอมเป็นฝรั่งหน้าตาดี/  
ทหาร/หมอ หลอกให้รักแล้วขอให้โอนเงิน  
ค่าธรรมเนียมพิสด



### Shopping Scam (หลอกขายสินค้า)

ตั้งราคาสินค้าถูกผิดปกติ  
โอนเงินแล้วไม่ส่งของ  
หรือส่งของไม่ตรงปก

#N NotebookLM

## ถอดรหัสกลโกง: คู่มือวิเคราะห์ภัยไซเบอร์

รูปแบบภัย	อารมณ์ที่เป็นเป้าหมาย	สัญญาณเตือนหลัก
Phishing	● ความกลัว	ลิงก์แบบใน SMS, อ้างว่าบัญชีมีปัญหา
Call Center	● ความกลัว	ข่มขู่ด้วยกฎหมาย, อ้างเป็นเจ้าหน้าที่รัฐ
หลอกลงทุน	● ความโลภ	การันตีผลตอบแทนสูง, ได้เงินเร็วเกินจริง
Romance Scam	● ความรัก/ความหลง	โปรไฟล์ดูดีเกินจริง, ขอให้ช่วยจ่ายค่าธรรมเนียม
หลอกขายสินค้า	● ความโลภ	ราคาถูกกว่าตลาดมาก, เร่งให้รีบโอน

#N NotebookLM

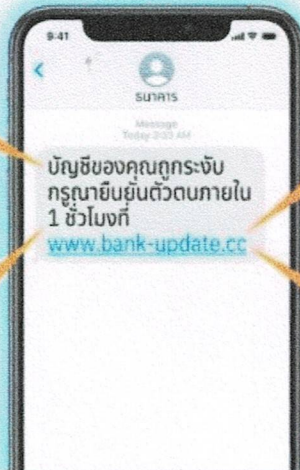
## สแกน พิรุณ ก่อนคลิก: สัญญาณเตือนที่คุณต้องรู้

### สร้างความตกใจ:

มักเริ่มด้วยบัญชีของคุณถูกระงับ หรือคุณถูกหมายเรียก เพื่อให้เราขาดสติ

### สะกดผิด/ภาษาแปลก:

ใช้คำสะกดผิด หรือภาษาทางการที่ดูแปลกคล้ายใช้โปรแกรมแปลภาษา



### ลิงก์แปลกปลอม:

URL ไม่ใช่เว็บไซต์ทางการ มักลงท้ายด้วย .cc, .top หรือชื่อเลียนแบบ

### เร่งรีบ:

ต้องดำเนินการภายใน 1 ชั่วโมง เพื่อบังให้เราไม่ทันได้คิดหรือปรึกษาใคร

# NotebookLM

## กฎเหล็ก 3 ไม่: ด้านป้องกันภัยส่วนบุคคล

ไม่เชื่อ

อย่าหลงเชื่อตัวเลขผลตอบแทนที่สูงเกินจริง หรือคำโปรยที่สร้างความตื่นตระหนก

ไม่คลิก

อย่ากดลิงก์จาก SMS หรือช่องทางแยกจากคนแปลกหน้าเด็ดขาด

ไม่โอน

ตรวจสอบชื่อบัญชีปลายทางผ่านแอปฯ หรือเว็บไซต์ตรวจสอบรายชื่อคนโกงก่อนโอนเสมอ

# NotebookLM

# ตั้งค่าอุปกรณ์ให้เป็นป้อมปราการ



## เปิดใช้งาน 2FA

เปิดใช้งาน Two-Factor Authentication ในทุกแอปพลิเคชันที่รองรับ เพื่อการยืนยันตัวตนสองชั้น



## รหัสผ่านซับซ้อนและไม่ซ้ำ

ตั้งรหัสผ่านที่ซับซ้อน และที่สำคัญคือต้องไม่ซ้ำกันในแต่ละบัญชี



## ปิดกั้น Accessibility Service

ไม่อนุญาตให้แอปแปลกๆ เข้าถึงการควบคุมเครื่อง เพื่อป้องกันการถูกรับขโมย

© NotebookLM

# ตกเป็นเหยื่อแล้ว ต้องทำอะไร?



## 1. ติดต่อธนาคารทันที

โทรหา Hotline ศูนย์แจ้งเหตุภัยทางการเงิน (เปิด 24 ชม.) เพื่ออายัดบัญชีชั่วคราว



## 2. รวบรวมหลักฐาน

เก็บข้อมูลทุกอย่างก่อนที่บิตจะหายไป



## 3. แจ้งความออนไลน์

ดำเนินการผ่านเว็บไซต์ [www.thaipoliceonline.go.th](http://www.thaipoliceonline.go.th) เท่านั้น (ระวังเว็บปลอม!)

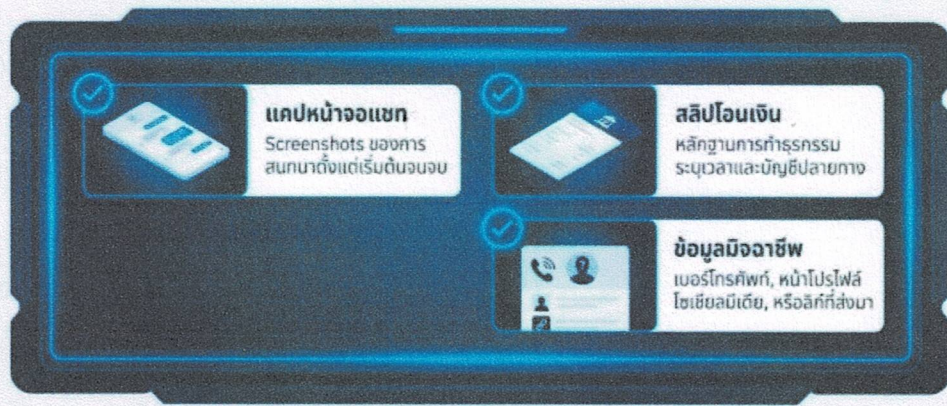


## 4. เปลี่ยนรหัสผ่าน

รีบเปลี่ยน Password ของแอปพลิเคชันธนาคารและอีเมลหลักทั้งหมด

© NotebookLM

## เพิ่มหลักฐาน: สิ่งที่ต้องรวบรวมก่อนไปแจ้งความ



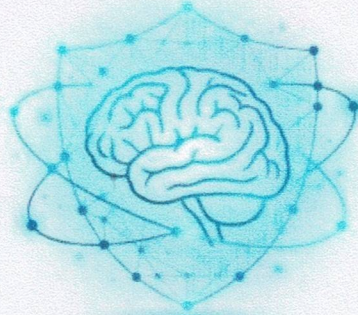
© NotebookLM

## สายด่วนและแหล่งข้อมูลฉุกเฉิน



© NotebookLM

# สติ คือเกราะป้องกันที่ดีที่สุดในโลกออนไลน์



เทคโนโลยีเปลี่ยนแปลงตลอดเวลา

แต่วิธีการของมิจฉาชีพยังคงวนเวียนอยู่กับการหลอกลวงอารมณ์ของมนุษย์

หากคุณ หยุดคิดสักนิดก่อนคลิก คุณจะปลอดภัยจากภัยไซเบอร์ได้ถึง 99%



© NotebookLM

# ส่งต่อความปลอดภัยให้คนที่คุณรัก



มิจฉาชีพไม่เคยหยุดพัก

แต่เราสามารถช่วยกันสร้างสังคมออนไลน์ที่ปลอดภัยยิ่งขึ้นได้

แชร์คู่มือนี้ให้ครอบครัวและเพื่อนของคุณ  
เพื่อเป็นเกราะป้องกันให้พวกเขาในโลกดิจิทัล



© ส.ช.ค.ค.บ.๒๕๖๖

© NotebookLM

## ส่งต่อความปลอดภัยให้คนที่คุณรัก



มีจาชีฟไม่เคยหยุดพัก  
แต่เราสามารถช่วยกันสร้างสังคมออนไลน์ที่ปลอดภัยยิ่งขึ้นได้  
แชร์คู่มือนี้ให้ครอบครัวและเพื่อนของคุณ  
เพื่อเป็นเกราะป้องกันให้พวกเขาในโลกดิจิทัล

