



ภัยคุกคามที่อาจเกิดขึ้นจาก
การจัดส่งและเผยแพร่ข้อมูล
เอกสารราชการ
ผ่านสื่อสังคมออนไลน์ต่าง ๆ

สำนักงานพัฒนารัฐกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ภาพรวมเนื้อหา

- รูปแบบการจัดส่งและเผยแพร่เอกสารราชการในปัจจุบัน
- ข้อดี/ข้อเสีย ของการรับส่งเอกสารราชการผ่านอินเทอร์เน็ต
- ตัวอย่างกรณีศึกษาปัญหาที่พบ
- ข้อควรระวังในการใช้งาน

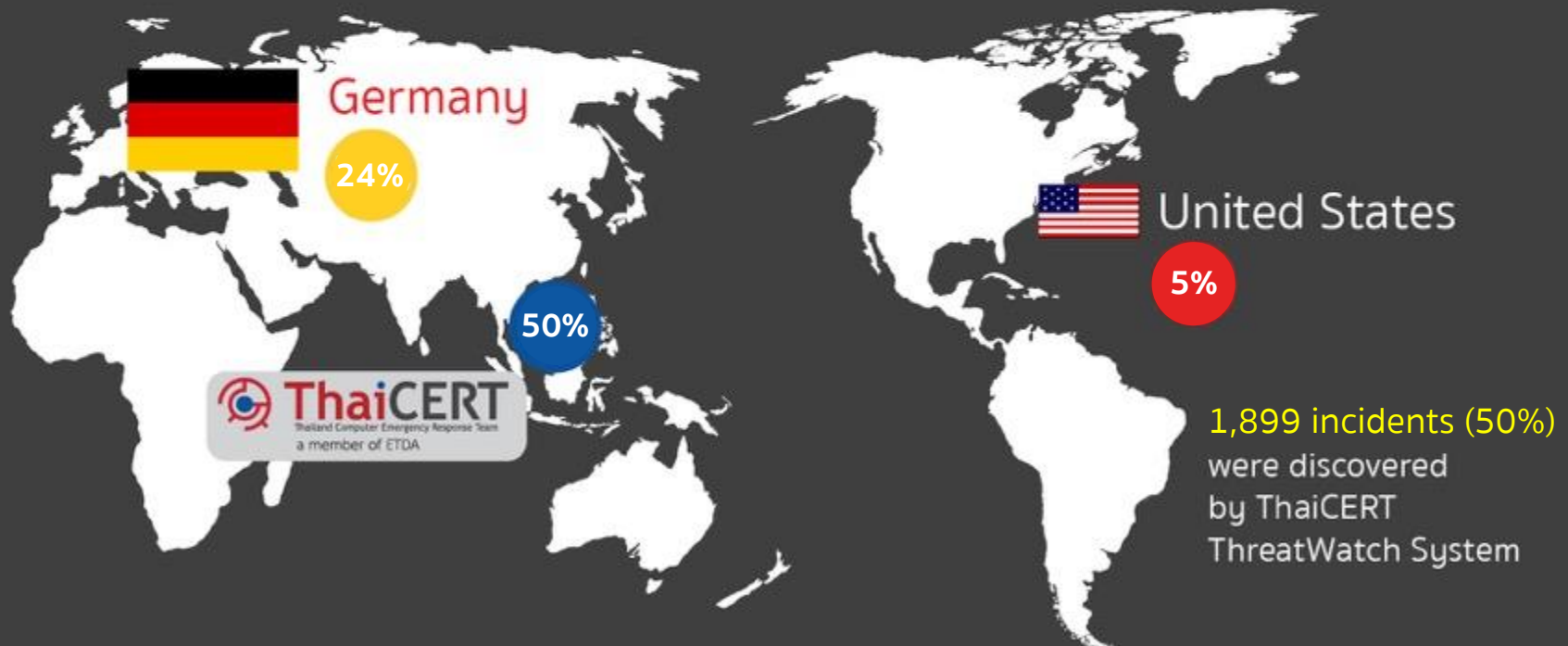


สถิติภัยคุกคามไซเบอร์ ในปี 2559

สถิติภัยคุกคาม
3 อันดับแรก

- 🟡 Intrusion
- 🟡 Malicious Code
- 🟡 Fraud (Phishing)

ThaiCERT handled
3,797 incidents.



หมายเหตุ: ข้อมูลจากระบบ ThreatWatch ของไทยเซิร์ต ตั้งแต่ 1 ม.ค. 2559 - 31 ธ.ค. 2559

การรับส่งเอกสารราชการในรูปแบบเดิม



พิมพ์เอกสารเป็นกระดาษ ส่งเซ็นตามลำดับชั้น ส่งเอกสารทางไปรษณีย์

การรับส่งเอกสารราชการในปัจจุบัน



รับส่งเอกสารราชการและติดต่อประสานงานผ่านอินเทอร์เน็ต

ข้อดี ข้อเสีย ของการส่งเอกสารราชการผ่านอินเทอร์เน็ต

ข้อดี

- มีความรวดเร็ว
- ป้องกันปัญหาหนังสือสูญหาย
- มีบันทึกวันเวลาส่งเอกสารที่ชัดเจน
- ลดปริมาณการใช้กระดาษ

ข้อเสีย

- อาจขาดความน่าเชื่อถือและการตรวจสอบยืนยันความถูกต้อง
- อาจมีประเด็นเรื่องการใช้อ้างอิงเป็นคำสั่งราชการ
- อาจไม่สะดวกหากต้องการสืบค้นข้อมูลย้อนหลัง
- อาจมีการนำบัญชีส่วนตัวมาใช้งานที่เป็นความลับของราชการ

ความเสี่ยงด้านความมั่นคงปลอดภัย

- ข้อมูลรั่วไหล
- การแอบอ้างสวมรอยบัญชี
- การปลอมแปลงเอกสาร



ความเสี่ยงเรื่องข้อมูลรั่วไหล

- การเผยแพร่หรือส่งต่อเอกสารที่มีระดับชั้นความลับ
 - การนำเอกสารที่มีระดับชั้นความลับไปเก็บไว้ที่ผู้ให้บริการเอกชนหรือผู้ให้บริการต่างประเทศ
- การขโมยข้อมูล
 - อุปกรณ์ที่ใช้งานติดมัลแวร์
 - เซิร์ฟเวอร์ที่เก็บข้อมูลเอกสารราชการถูกเจาะระบบ
- การทำลายเอกสาร
 - ไฟล์เอกสารอาจยังคงอยู่ในเซิร์ฟเวอร์ของผู้ให้บริการ ถึงแม้ผู้ใช้จะสั่งให้ลบไฟล์ออกไปแล้ว

ความเสี่ยงเรื่องการแอบอ้างสวมรอย บัญชี

- เจ้าหน้าที่ถูกแฮกบัญชีที่ใช้ติดต่อประสานงาน
 - ตั้งรหัสผ่านที่คาดเดาได้ง่าย
 - ตกเป็นเหยื่อเว็บไซต์ Phishing
 - ถูกดักขโมยข้อมูลจากการเชื่อมต่อ Wi-Fi สาธารณะ
- มีบุคคลอื่นสมัครบัญชีที่มีชื่อคล้ายกันเพื่อแอบอ้างสวมรอย
 - การสนทนาผ่านโปรแกรมแชทอาจตรวจสอบข้อมูลผู้ติดต่อได้ยากกว่าอีเมล

ข้อเสนอแนะเพื่อการรักษาความมั่นคงปลอดภัย

การรักษาความมั่นคงปลอดภัยอุปกรณ์

- คอมพิวเตอร์และโทรศัพท์มือถือ

การรักษาความมั่นคงปลอดภัยบัญชี

- อีเมล
- สื่อสังคมออนไลน์
- โปรแกรมสนทนา

การรักษาความมั่นคงปลอดภัย อุปกรณ์

- ตั้งรหัสล็อกหน้าจอ
- อัปเดตระบบปฏิบัติการและซอฟต์แวร์ให้ทันสมัย
- ติดตั้งแอนติไวรัส

การรักษาความมั่นคงปลอดภัย Android

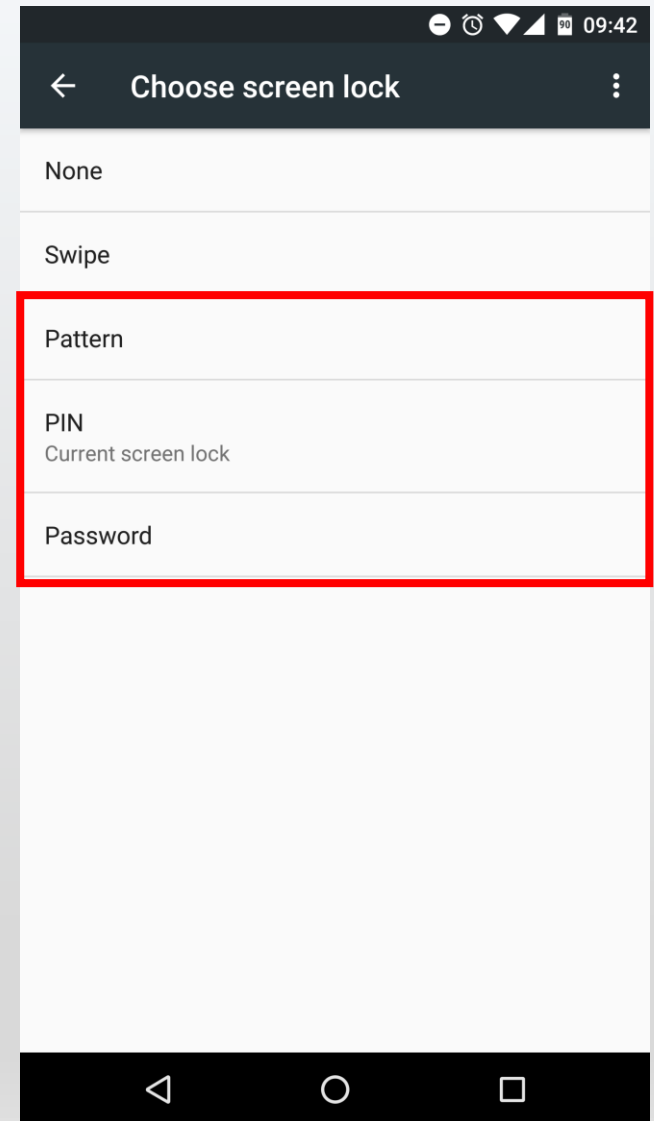


ดกคโรว

การตั้งรหัสล็อกหน้าจอ

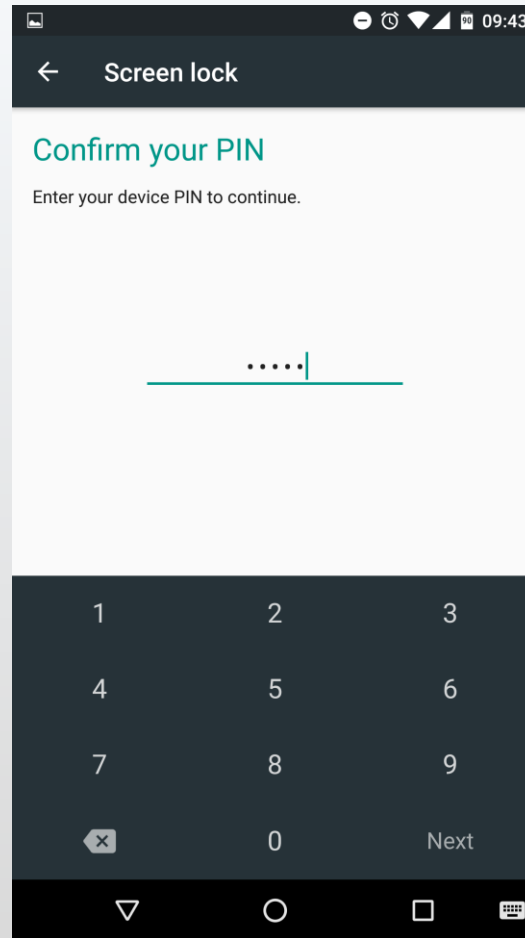
1. Settings
2. Security
3. Screen lock

สามารถตั้งรหัสล็อกหน้าจอได้
3 รูปแบบ คือ Pattern, PIN และ
Password

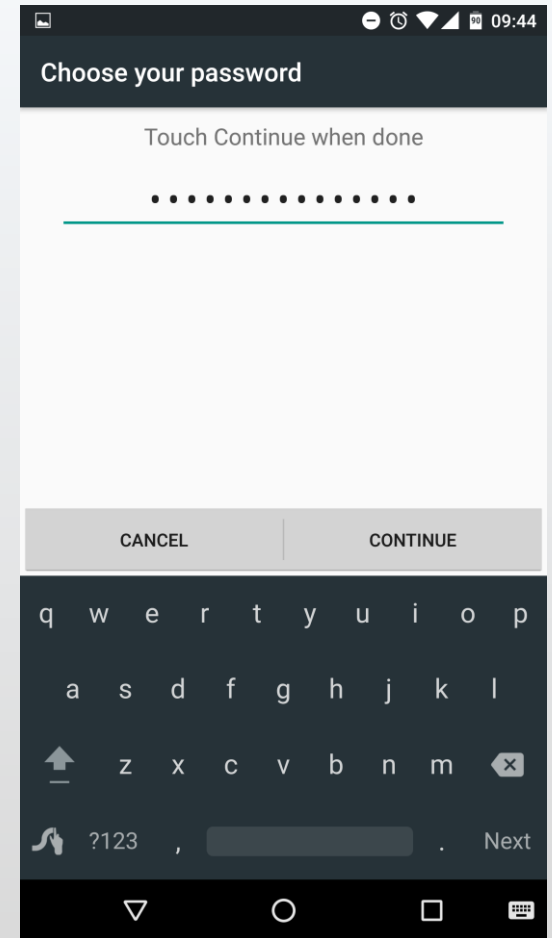




Pattern



PIN

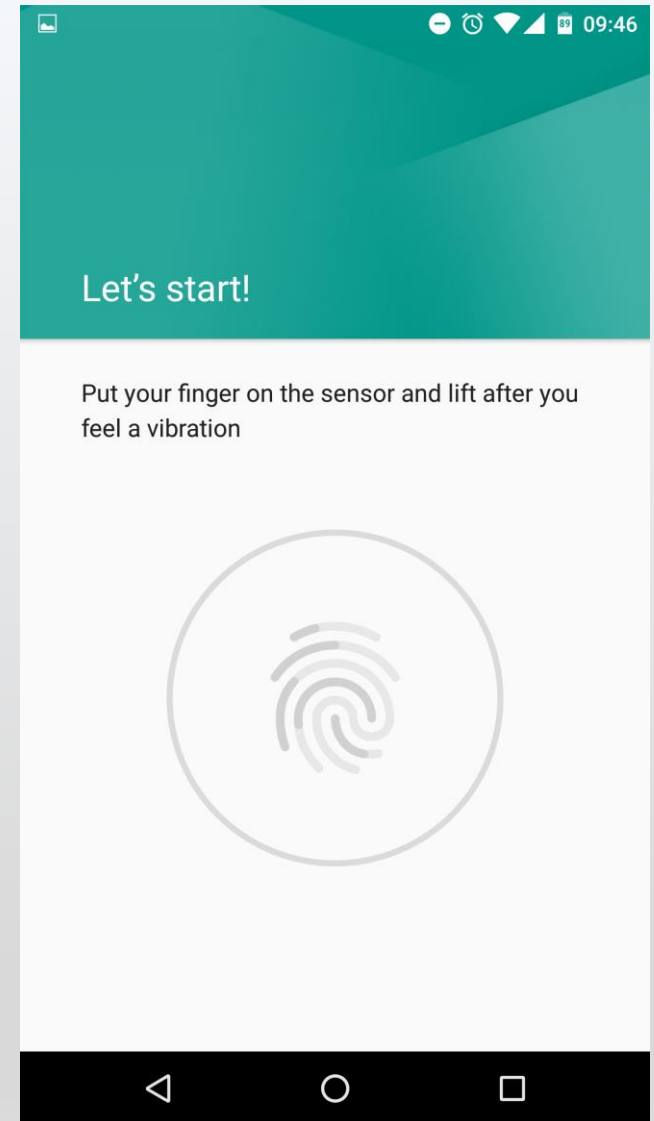


Password

การตั้งค่าให้ปลดล็อกหน้าจอ ด้วยลายนิ้วมือ

1. Settings
2. Security
3. Fingerprint

เมนูการตั้งค่าลายนิ้วมืออาจแตกต่างกัน
ไปในแต่ละเครื่อง ขึ้นอยู่กับผู้ผลิต



ข้อแนะนำในการตั้งรหัสล็อกหน้าจอ

- ระดับความปลอดภัย
 - Password > PIN > Pattern
- ไม่ควรตั้งรหัสผ่านที่สั้นเกินไปหรือคาดเดาได้ง่าย เช่น 1234 หรือ password
- การตั้งค่าให้ปลดล็อกหน้าจอด้วยลายนิ้วมืออาจมีความเสี่ยงที่จะถูกปลอมลายนิ้วมือเพื่อปลดล็อก

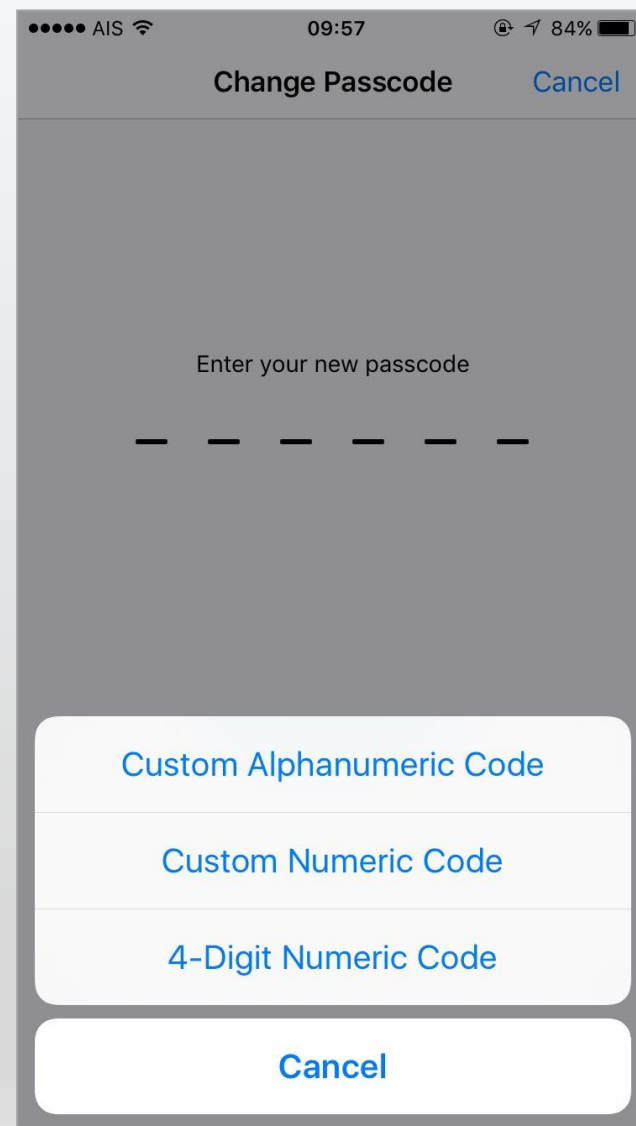
การรักษาความมั่นคงปลอดภัย iOS

iOS

การตั้งรหัสล็อกหน้าจอ

1. Settings
2. Passcode
3. Change Passcode
4. Passcode Options

เลือกรูปแบบการตั้งค่าล็อกหน้าจอได้หลัก ๆ 2 รูปแบบ คือ Alphanumeric (Password) และ Numeric (PIN)



••••• AIS 09:58 83%

Cancel Change Passcode Next

Enter your new passcode

|

Passcode Options

q	w	e	r	t	y	u	i	o	p
a	s	d	f	g	h	j	k	l	
↶	z	x	c	v	b	n	m	✖	
123	🌐	space	return						

Passcode

••••• AIS 09:57 84%

Change Passcode Cancel

Enter your new passcode

— — — — —

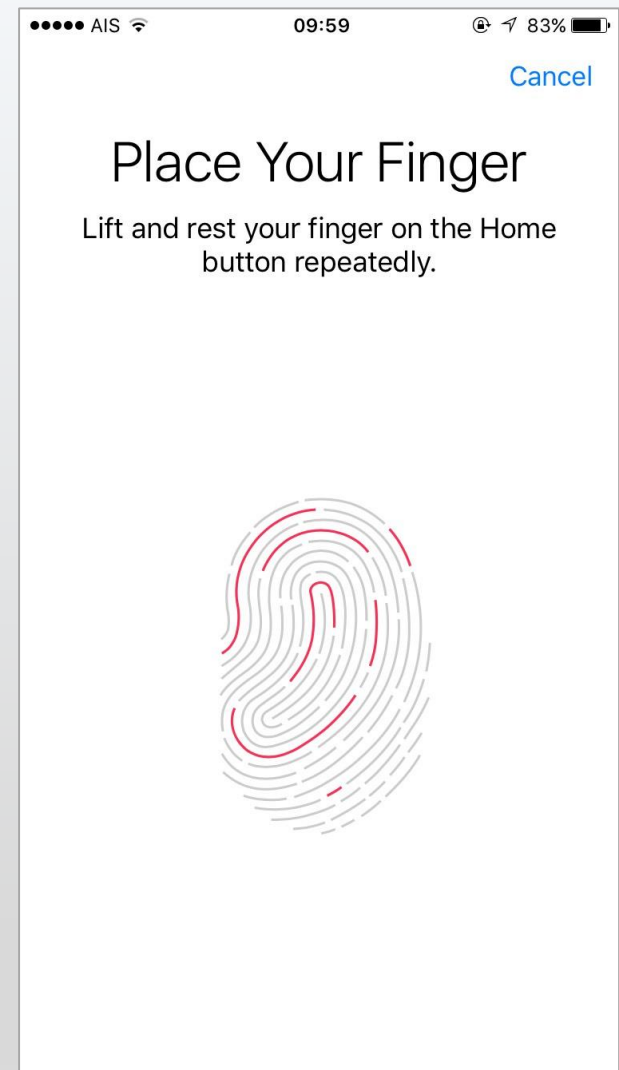
Passcode Options

1	2 ABC	3 DEF
4 GHI	5 JKL	6 MNO
7 PQRS	8 TUV	9 WXYZ
	0	✖

PIN

การตั้งให้ปลดล็อก หน้าจอด้วยลายนิ้วมือ

1. Settings
2. Passcode
3. Change Passcode
4. Passcode Options
5. Fingerprint



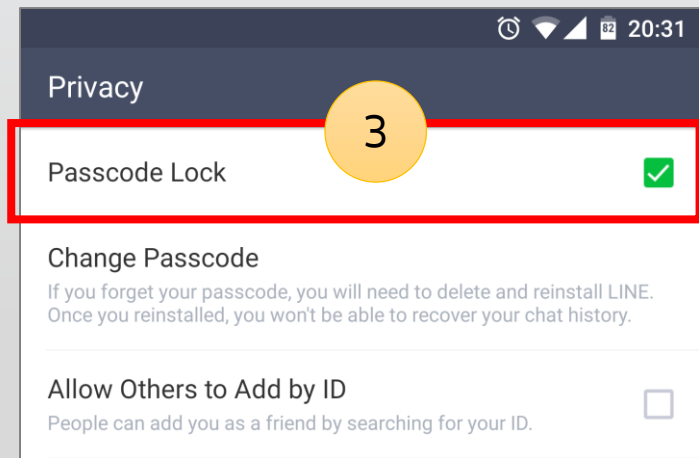
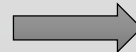
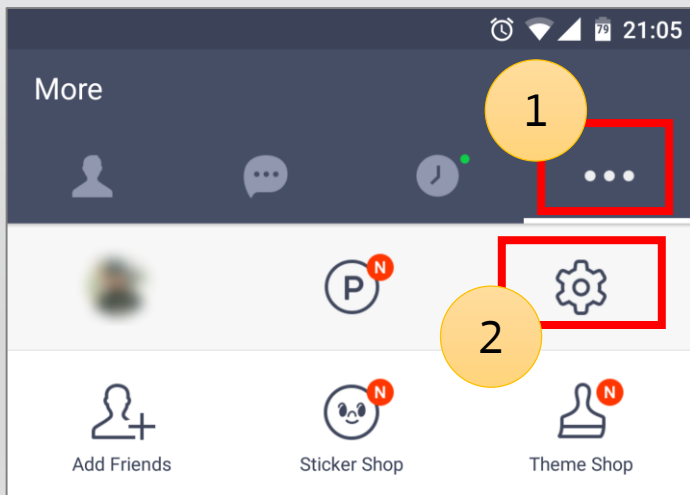
การตั้งค่าความมั่นคงปลอดภัย ในการใช้งาน LINE



การตั้งค่าความมั่นคงปลอดภัยบัญชี LINE (1)

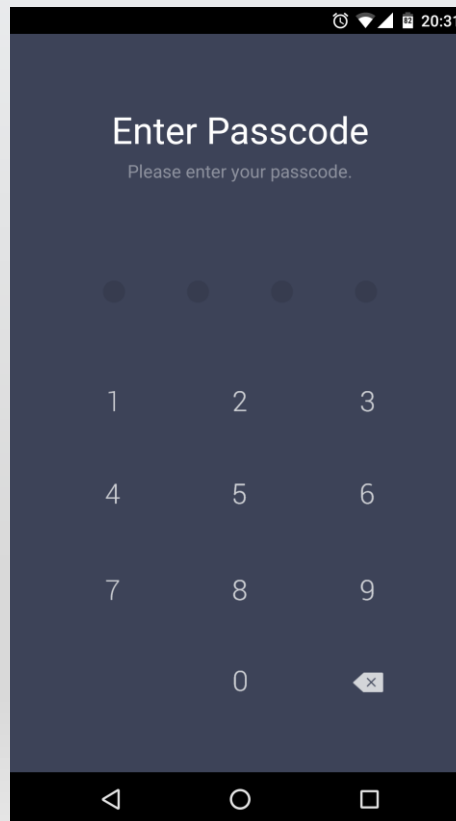
ตั้งค่าให้ใช้รหัสผ่านเพื่อเข้าใช้งานโปรแกรม

1. Settings (กด ... แล้วเลือกรูปฟันเฟือง)
2. Privacy
3. Passcode Lock

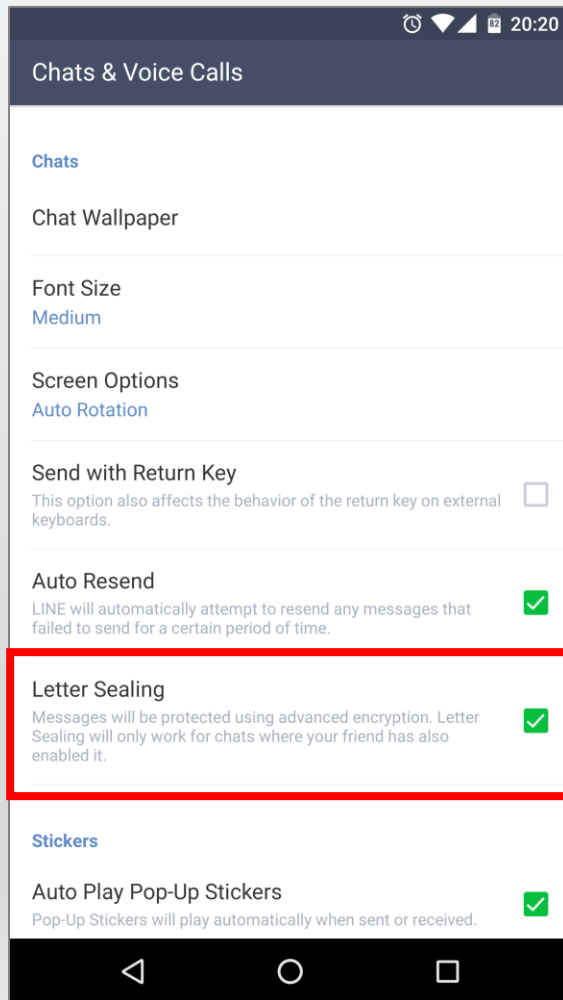


การตั้งค่าความมั่นคงปลอดภัยบัญชี LINE (2)

ข้อควรระวัง: หากลืมหุ้สผ่าน จะไม่สามารถเข้าใช้งาน LINE ได้ ต้องลบแอปพลิเคชันแล้วติดตั้งใหม่ ประวัติข้อความที่เคยสนทนาจะหายไป



การตั้งค่าความมั่นคงปลอดภัยบัญชี LINE (3)

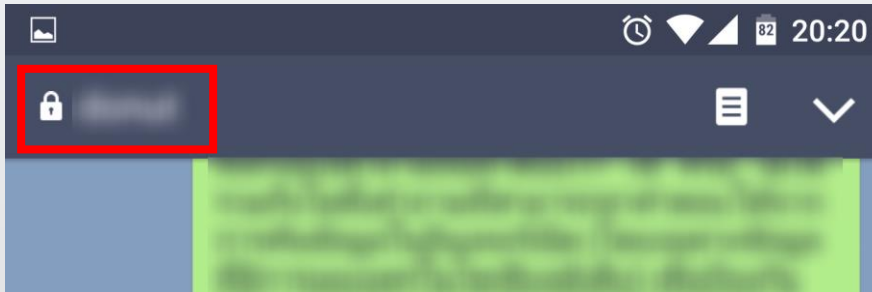


Letter Sealing
ช่วยปกป้องข้อความสนทนาใน LINE
จากการถูกดักจับข้อมูลระหว่างทาง

(มีใน LINE เวอร์ชัน 5.3.0 ขึ้นไป)

1. Setting
2. Chats & Calls
3. Letter Sealing

การตั้งค่าความมั่นคงปลอดภัยบัญชี LINE (4)



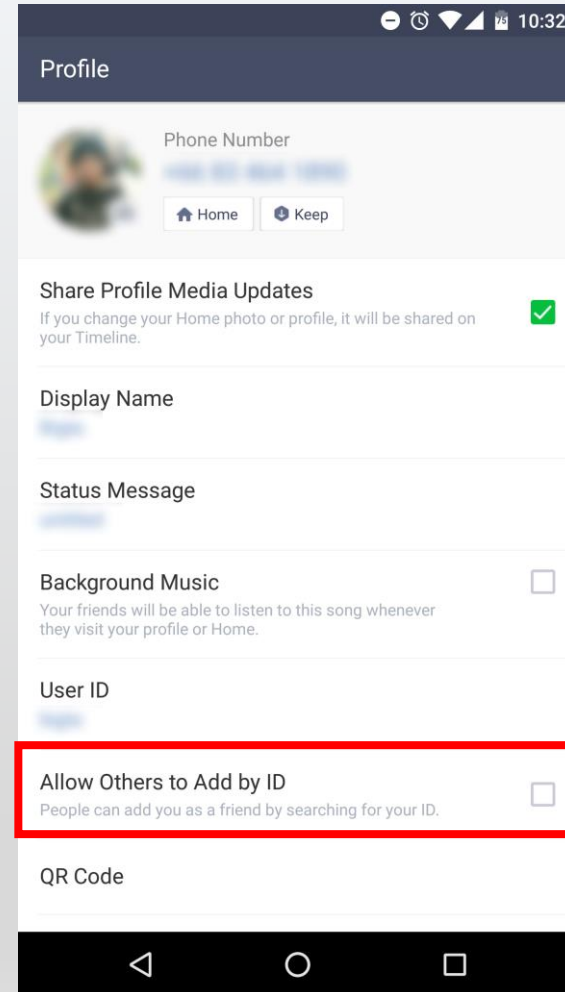
การใช้งาน Letter Sealing ทั้งสอง
ฝ่ายต้องเปิดใช้งานทั้งคู่

หากเปิดใช้งานแล้ว ข้อความที่ส่ง
ด้วย Letter Sealing จะมี
เครื่องหมายกุญแจล้อมรอบข้อความ
สนทนา

การตั้งค่าความมั่นคงปลอดภัยบัญชี LINE (5)

ปิดตัวเลือก Allow Others to Add by ID เพื่อป้องกันไม่ให้ถูกบุคคลที่ไม่รู้จักเพิ่มในรายชื่อผู้ติดต่อโดยการเดาชื่อ ID (ต้องเพิ่มผ่าน QR)

1. Settings
2. Edit Profiles
3. Allow Others to Add by ID



การตั้งค่าความมั่นคงปลอดภัยบัญชี LINE (6)

1. Settings
2. Account

Authorized Apps

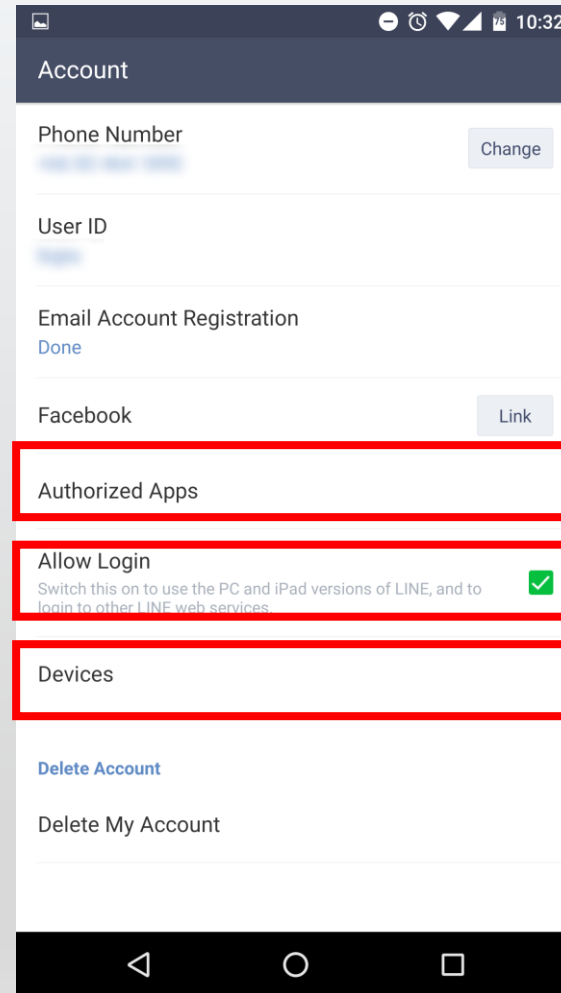
- ตรวจสอบว่ามีแอปพลิเคชันใดบ้างที่ผูกกับบัญชีนี้

Allow Login

- อนุญาตให้ล็อกอินผ่าน LINE บนอุปกรณ์อื่น

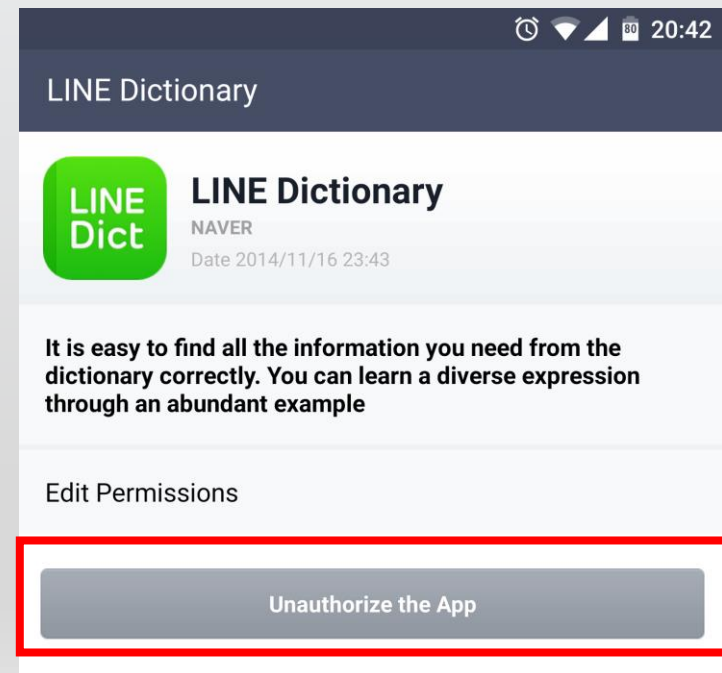
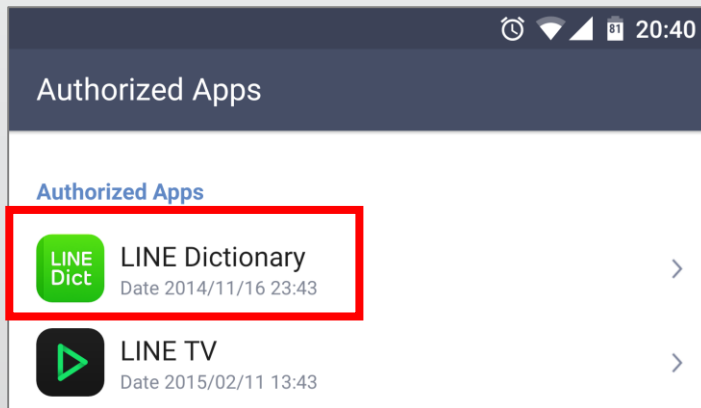
Devices

- ดูว่ามีอุปกรณ์ใดบ้างที่ล็อกอินบัญชีนี้อยู่



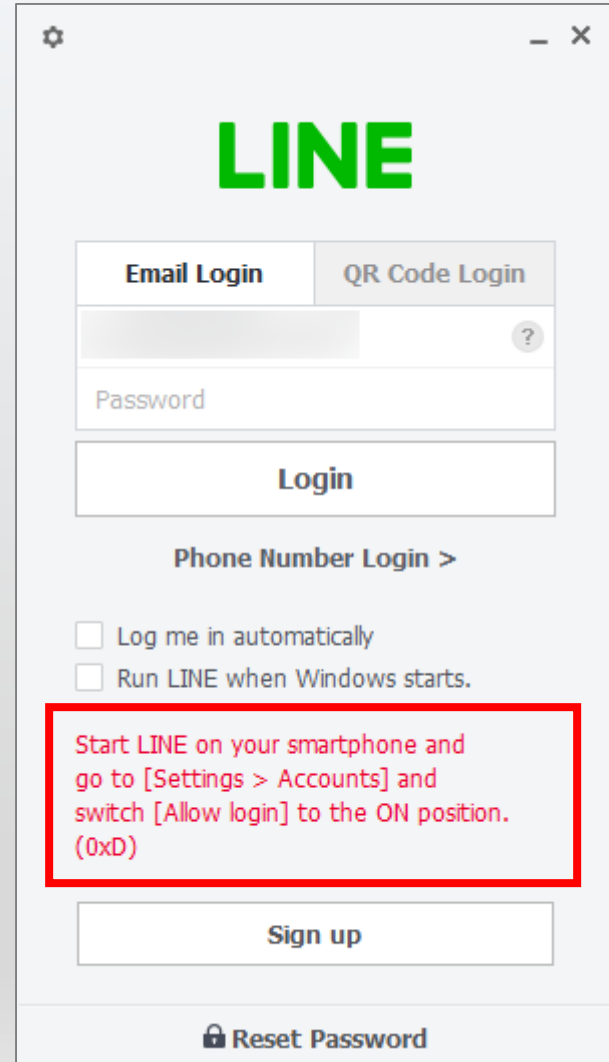
การตั้งค่าความมั่นคงปลอดภัยบัญชี LINE (7)

หากเลือกเมนู Authorized Apps จะสามารถตรวจสอบรายชื่อแอปพลิเคชันที่ล็อกอินโดยใช้บัญชี LINE ได้ หากต้องการยกเลิกให้กดที่ชื่อแอปพลิเคชันแล้วเลือก Unauthorize the App



การตั้งค่าความมั่นคงปลอดภัยบัญชี LINE (8)

หากปิดตัวเลือก Allow Login
จะไม่สามารถล็อกอินเข้าใช้งาน
LINE จากอุปกรณ์อื่นได้ (เช่น
PC)



LINE

Email Login QR Code Login

?

Password

Login

Phone Number Login >

☐ Log me in automatically

☐ Run LINE when Windows starts.

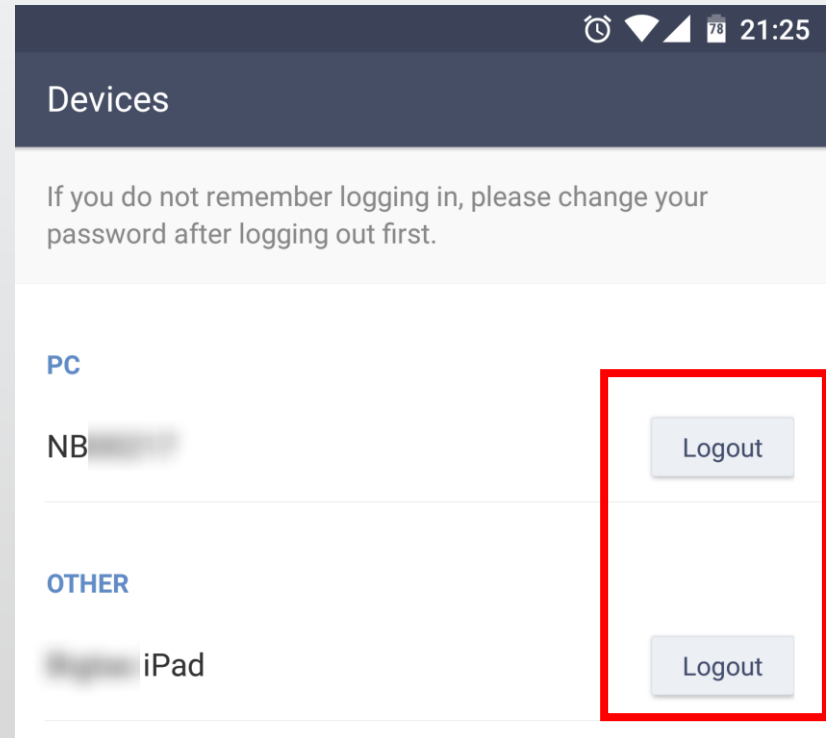
Start LINE on your smartphone and go to [Settings > Accounts] and switch [Allow login] to the ON position. (0xD)

Sign up

Reset Password

การตั้งค่าความมั่นคงปลอดภัยบัญชี LINE (9)

เมนู Devices สามารถ
ตรวจสอบรายชื่ออุปกรณ์
ที่ล็อกอินบัญชี LINE ได้
หากไม่ต้องการให้
อุปกรณ์ใดใช้งานได้ให้กด
ปุ่ม Logout

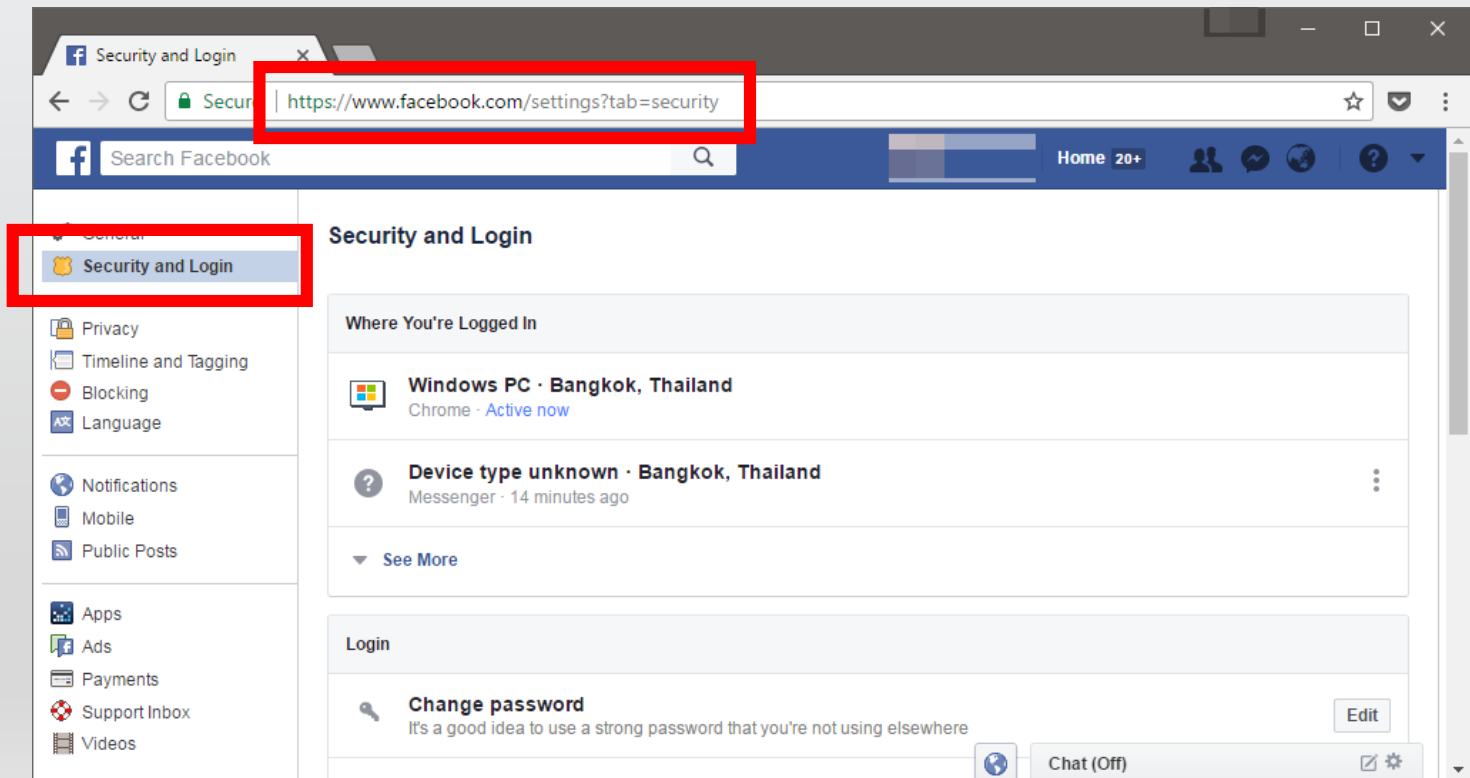


การตั้งค่าความมั่นคงปลอดภัยในการ ใช้งาน Facebook



การตั้งค่าความมั่นคงปลอดภัยบัญชี Facebook (1)





<https://www.facebook.com/settings?tab=security>



การตั้งค่าความมั่นคงปลอดภัยบัญชี Facebook (2)

ตรวจสอบว่าเคยมีการล็อกอินบัญชีนี้จากอุปกรณ์ใดบ้าง

Where You're Logged In


	Windows PC · Bangkok, Thailand Chrome · Active now	
	Device type unknown · Bangkok, Thailand Messenger · 19 minutes ago	⋮
	iPhone · Bangkok, Thailand Mobile Safari · 16 hours ago	⋮
	Huawei Nexus 6P · Bangkok, Thailand Groups · September 14, 2016	⋮

[▲ See Less](#)[Log Out Of All Sessions](#)

การตั้งค่าความมั่นคงปลอดภัยบัญชี Facebook (3)


ตั้งค่าให้มีการแจ้งเตือนเมื่อมีการล็อกอินบัญชี โดยแจ้งเตือนทั้งผ่านแอปพลิเคชันและอีเมล

Setting Up Extra Security


**Get alerts about unrecognized logins**Close

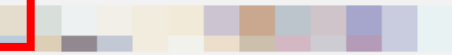
On • We'll let you know if anyone logs in from a device or browser you don't usually use

Get an alert when anyone logs into your account from an unrecognized device or browser.


 **Notifications**

☒ Get notifications
☐ Don't get notifications

 **Email**

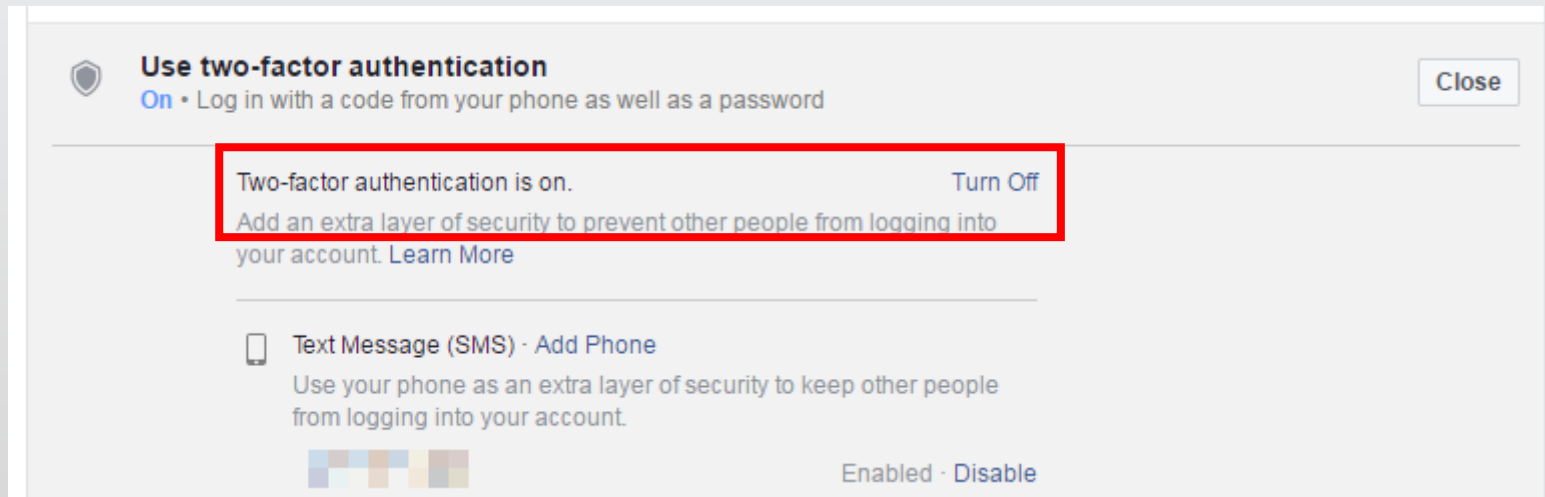
☒ Email login alerts to 
☐ Don't get email alerts

Add another email or mobile number



การตั้งค่าความมั่นคงปลอดภัยบัญชี Facebook (4)

ตั้งค่าให้มีการใส่รหัสยืนยันอีกชั้นหนึ่งก่อนล็อกอิน



การรักษาความมั่นคงปลอดภัยบัญชี

- ควรใช้บัญชีอีเมลของหน่วยงาน เพื่อป้องกันข้อมูลรั่วไหล
- ตั้งรหัสผ่านให้มีความปลอดภัย
- หากเป็นไปได้ควรเปิดใช้งานการยืนยันตัวตนแบบ 2 ขั้นตอน

* * * * *

Make sure that your

PASSWORD IS HARD TO GUESS

– at least 8 characters long
with mixed-case letters,
numbers and symbols

Aa

123

!@#



PASSWORD MUST BE CHANGED

at least every 3 months
for important systems,
and every 6 months
for others

* * * * *



DO NOT ENABLE
THE 'REMEMBER PASSWORD'
option if prompted

SECURITY AWARENESS

DO NOT



DO NOT REVEAL
YOUR PASSWORD
with anyone.



DO NOT WRITE YOUR
PASSWORDS DOWN
and leave them lying around.



* * * * *

• BANK
• E-MAIL
• ON-LINE
TRADING A/C

SOCIAL
MEDIA

THE **DO NOT USE**
SAME PASSWORD FOR
WORK AND PERSONAL
ACTIVITIES

ติดตามข้อมูลข่าวสารเพิ่มเติม

www.etda.or.th และ www.thaicert.or.th



ThaiCERT ETDA
Thailand Computer Emergency Response Team
a member of ETDA
www.etda.or.th

แจ้งเหตุภัยคุกคาม กิจกรรม แจ้งเตือนและข้อแนะนำ เอกสารเผยแพร่ บริการ เว็บไซต์ที่เกี่ยวข้อง เกี่ยวกับไทยเซิร์ต

เตือนภัย มัลแวร์เรียกค่าไถ่ WannaCry

ThaiCERT

เอกสารเผยแพร่ล่าสุด
2017-04-19
วิธีตรวจสอบและป้องกันการถูกแฮก

ThaiCERT Annual Report

Thumbnail	Report Title	Version
	ThaiCERT Annual report	2015 Thai version
	ThaiCERT Annual report	2013 Thai version
	ThaiCERT Annual report	2013 English version
	ThaiCERT Annual report	2012 Thai version
	ThaiCERT Annual report	2012 English version

Cyber Security Articles & Alerts

Thumbnail	Article Title	Year
	Cyber Threat Alerts & Articles	2015
	Cyber Threat Alerts & Articles	2014
	Cyber Threat Alerts & Articles	2013
	Cyber Security Articles	2012
	Cyber Threat Alerts	2012



SECURITY AWARENESS

Make sure that your **PASSWORD IS HARD TO GUESS**
— at least 8 characters long
with mixed-case letters,
numbers and symbols

3 6
PASSWORD MUST BE CHANGED
at least every 3 months
for important systems,
and every 6 months
for others

DO NOT REUSE THE SAME PASSWORD FOR DIFFERENT SERVICES

จะเกิดอะไรขึ้น? ...
ถ้า รหัสผ่านอีเมลส่วนตัว
ตกอยู่ในมือผู้ไม่หวังดี

พฤติกรรมเสี่ยงใช้งาน LINE
ที่ช่วยต่อการลบรอยนิ้วมือ

Accounts

สัญญาณเตือนว่า กำลังมีใครใช้งานบัญชีของคุณอยู่



Q & A



Thank You